Cryptologic Quarterly

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

2014-01 • Vol. 33

Center for Cryptologic History

Cryptologic Quarterly

Publisher: Center for Cryptologic History
Executive Editor: Pamela F. Murray
Managing Editor: Laura Redcay
Associate Editor: Jennie Reinhardt

Editorial Policy. *Cryptologic Quarterly* is the professional journal for the National Security Agency/Central Security Service. Its mission is to advance knowledge of all aspects of cryptology by serving as a forum for issues related to cryptologic theory, doctrine, operations, management, and history. The primary audience for *Cryptologic Quarterly* is NSA/CSS professionals, but *CQ* is also distributed to personnel in other United States intelligence organizations as well as cleared personnel in other federal agencies and departments.

Cryptologic Quarterly is published by the Center for Cryptologic History, NSA. The publication is designed as a working aid and is not subject to receipt, control, or accountability.

Contacts. Please feel free to address questions or comments to Editor, *CQ*, at history@nsa.gov.

Disclaimer. All opinions expressed in *Cryptologic Quarterly* are those of the authors. They do not necessarily reflect the official views of the National Security Agency.

Copies of *Cryptologic Quarterly* can be obtained by sending an email to history@nsa.gov.

Cover: Monument to Marian Rejewski in Bydgoszcz, Poland, with sculpture of the ENIGMA machine he reconstructed; see article on page 56.

Contents

2014-01 • Volume 33

Articles

Renaissance Cryptography, Occultism, and the Jewish Cabala

Erin Higgins

Several minor but historically interesting cipher systems expounded upon by Renaissance cryptographers have their origin in the Jewish mystical system Cabala. The link between cryptography and Cabala is a book by Cornelius Agrippa, which reproduced and expounded upon several cabalistic systems of rearranging words. These systems were picked up and elaborated upon by the later cryptographers Giambattista della Porta and Blaise de Vigenère. We consider here the Tables of Ziruf, something Agrippa learned from the Cabalists and which appear to be the ancestor of the Reciprocal Ciphers of Giovan Battista Bellaso, Porta, and Vigenère.

Introduction

During the Renaissance, manual cryptography, such as was used until very recently, was just beginning to flower. Particularly in Italy and the Papal states, with the advent of resident ambassadors and what we would even now recognize as modern-style diplomacy, powerful players recognized the need for communication more secure than a Caesar-shift cipher and an underpaid messenger. The early developers of Renaissance-era ciphers and codes were focused in Italy but popped up throughout Europe: Leon Battista Alberti, inventor of the cipher wheel; and Johannes Trithemius, who publicized and elaborated on the wheel, and introduced steganography, for which he is most widely remembered. Then later, Bellaso developed mixed keying for polyalphabetic ciphers;[1] Porta recommended layering ciphers to prevent cryptanalysis, an art on which he wrote extensively; and Vigenère, the French diplomat and Cabalist, collated and expanded upon the works of these men and pioneered the concept of auto-keying, showing what was, by 1586,[2] the state of the art in cryptography.

Our concern here is to establish the connection among these men, the cryptographers, and Heinrich Cornelius Agrippa von Nettesheim (hereafter Agrippa), who is nearly exclusively remembered as a superstitious magician and occasionally as an early modern skeptic. The tremendous dissonance between these two labels should immediately rouse the suspicions of the reader: what has he done that history can name him equally superstitious and skeptical? An explanation lies in Agrippa's relationship with the cryptographer Trithemius, who, likewise, was widely regarded as a magician, though we know differently today.

HENRICUS CORNELIUS AGRIPPA Med. & IC. EQU.
Naſcitur Colon. Agrip. 1486
Obijt Anno 1538.
Stemmate natus Eques, Medicus, Magus atq; peritu

Heinrich Cornelius Agrippa von Nettesheim (Wikimedia)

Up until 1996, Trithemius scholarship was split into two camps: those who thought the books he wrote were strictly about cryptography, and those who thought that some of his writings dealt in magic. With Thomas Ernst's and James Reeds'[3] independent solutions of the remaining ciphers in Book III of *Steganographia*, history knows Trithemius as strictly a cryptographer, who used magical-sounding verbiage only as cover text.

Agrippa entered the story in 1509, shortly after the Benedictine monk Trithemius had left his first abbey in Sponheim, Germany, having been ordered to Wurzburg. Agrippa had read something of Trithemius' work—though only in manuscript, since *Steganographia* was not published until nearly a century later, and *Polygraphia*, Trithemius's overt book of ciphers, was not yet written. Agrippa, returning from what seems to have been a diplomatic mission on behalf of the Holy Roman Emperor,[4] stopped by the abbey at Wurzburg. Our record of the meeting is a pair of letters the men exchanged afterward. In early 1510, Agrippa sent Trithemius a manuscript of a book he had been writing; the personal letter he sent with it referenced their meeting and discussions of Cabala and magic. Trithemius is said to have detained the messenger so he could read the manuscript immediately and compose a response that very hour. The reply letter, which Agrippa later had printed along with his letter to Trithemius as a sort of preface to *De Occulta Philosophia Libri Tres*, praises Agrippa's accomplishment this far, urging him to continue, but with caution.[5]

Trithemius, in writing *Steganographia*, evidently thought it the height of cleverness to compose a book of ciphers disguised as magic, and was shocked when there was outcry against it and he was called “magician.”[6] Agrippa, soon after, sent him this manuscript which was full of what scholars of the time called “natural magic”—a sort of bastard mix of early science, late superstition, and folk medicine. There was nothing obviously identifiable as ciphers or cipher text in the initial draft; if there are ciphers, they are more cleverly hidden than in *Steganographia*.

Agrippa could be highly rationalist, especially in his later years. While the publication of *De Occulta Philosophia* is his most remembered bit of civil disobedience today, at the time he landed himself in worse trouble for a book he published several years earlier, in 1530: *De incertitudine et vanitate scientiarum atque artium declamatio invectivo*.[7] This book, an example of Pyrrhonic skepticism similar to that which Descartes would espouse a few years later, attacks all the arts and sciences. In it—and in a section of the book reprinted and included as an epilogue in *Occulta Philosophia* three years later—Agrippa appears to recant his early magical experimentations as the foolishness of youth, accounting for nothing.[8] In *De Vanitate*,[9] after he is finished declaiming magic, sorcery, and his own *De Occulta Philosophia*, he goes on to forswear mathematics, astronomy and astrology, chemistry and alchemy, painting, printing, the monastic system (likely the source of the Church’s displeasure), and, to our great disappointment, cryptography and cryptographers.

Once we understand the framework in which Agrippa’s scholarship rests, we can examine his sources. Agrippa, like most of his contemporaries,[10] rarely cited sources except when quoting from classical “Auctoritas.”[11] His sources, however, are vast, and he states from the outset that *Occulta Philosophia* is written to be survey and summa[12] of all nondiabolical occult sciences.

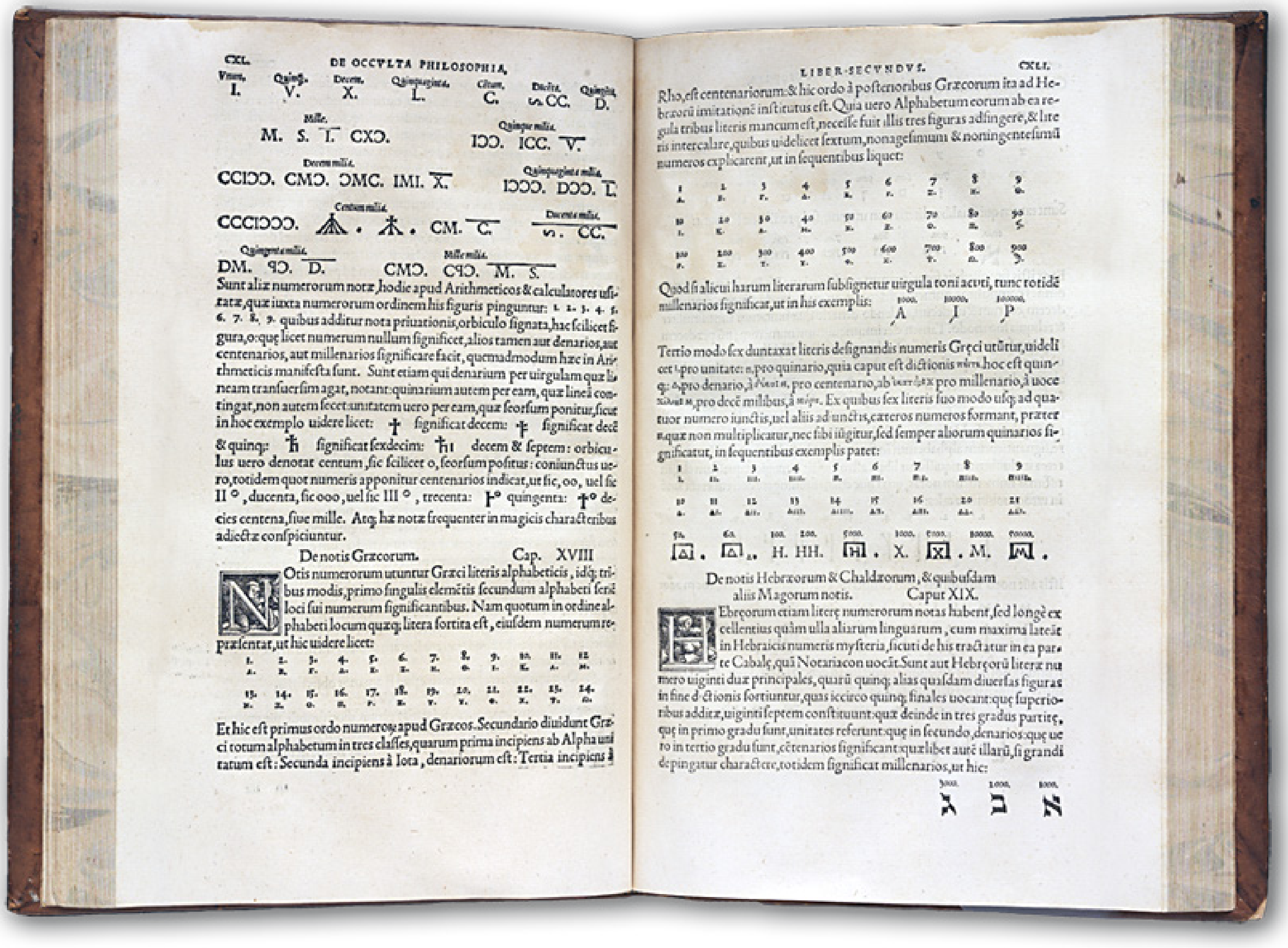
Background on Ciphers and Cabala

Cabala is probably unfamiliar to most readers; there is room here only for explanation of the elements which pertain to Agrippa and cryptography. An important book in traditional Jewish cabalism[13] is the *Sefer Yetzirah.* It had circulated in one of four manuscript versions for generations,[14] though it was not translated into Latin before Agrippa’s death.[15] The book, the name of which translates as “The Book of Formation” or “The Book of Creation,” poetically describes the creation of the universe as an analogy to the creation of the Hebrew alphabet.

The *Sefer Yetzirah* is the source of a system of cipher alphabets, called “Ziruf” (צירוף, literally “refinement”) by Johannes Reuchlin,[16] Agrippa,[17] and Vigenère,[18] but called “the 231 gates” by Aryeh Kaplan in his commentary to the *Sefer Yetzirah*. There are no Ziruf in the *Sefer Yetzirah* itself; they originated probably in early medieval and Renaissance commentaries.[19] This system of Temurah (תמורה), or “change,” is itself the source for the famous AThBaSh and ALBaM biblical ciphers.[20]

Traditional Cabala concerns itself, in addition to the Temurah, with other letter and word manipulations. *Gematria* is the practice of equating words on the basis of the numeric value of their letters.[21] *Notarikon* is shorthand, acrostic, or initialism: a new word is formed from the initial, middle, or last letters of each word in an important phrase, and the new word is considered to mean the same as, or even have the same power as, the original phrase.[22] Obviously, neither of these is as conducive to the development of substitution cipher systems as Temurah is.

Vigenère was quite sold on the whole academic discipline of Cabala, at least the version of it he encountered. He makes the bold claim that not only is the cipher he is at that time describing (the Ziruf, or Bellaso cipher), but *all* ciphers, are at root borrowed from the Hebrews, particularly the Cabalists and



CXL. DE OCCVLTA PHILOSOPHIA.

Vnum.	Quinq;.	Decem.	Quinquaginta.	Centum.	Ducẽta.	Quingẽta.
I.	V.	X.	L.	C.	ɅCC.	D.

Mille. M. S. T̄. CXƆ. Quinque milia. IƆƆ. ICC. V̄.

Decem milia. CCIƆƆ. CMƆ. ƆMC. IMI. X̄. Quinquaginta milia. IƆƆƆ. DƆƆ. L̄.

Centum milia. CCCIƆƆƆ. ⩚. ⩚. CM. C̄. Ducenta milia. Ʌ. C̄C̄.

Quingenta milia. DM. ꟼƆ. D̄. Mille milia. CMƆ. CꟼƆ. M̄. S̄.

Sunt aliæ numerorum notæ, hodie apud Arithmeticos & calculatores uſitatæ, quæ iuxta numerorum ordinem his figuris pinguntur: 1. 2. 3. 4. 5. 6. 7. 8. 9. quibus additur nota priuationis, orbiculo ſignata, hac ſcilicet figura, o: quę licet numerum nullum ſignificet, alios tamen aut denarios, aut centenarios, aut millenarios ſignificare facit, quemadmodum hæc in Arithmeticis manifeſta ſunt. Sunt etiam qui denarium per uirgulam quæ lineam tranſuerſim agat, notant: quinarium autem per eam, quæ lineã contingat, non autem ſecet: unitatem uero per eam, quæ ſeorſum ponitur, ſicut in hoc exemplo uidere licet: † ſignificat decem: † ſignificat decẽ & quinq;: † ſignificat ſexdecim: †I decem & ſeptem: orbiculus uero denotat centum, ſic ſcilicet o, ſeorſum poſitus: coniunctus uero, totidem quot numeris apponitur centenarios indicat, ut ſic, oo, uel ſic II°, ducenta, ſic ooo, uel ſic III°, trecenta: †° quingenta: †° decies centena, ſiue mille. Atq; hæ notæ frequenter in magicis characteribus adiectæ conſpiciuntur.

De notis Græcorum. Cap. XVIII

NOtis numerorum utuntur Græci literis alphabeticis, idq; tribus modis, primo ſingulis elemẽtis ſecundum alphabeti ſeriẽ loci ſui numerum ſignificantibus. Nam quotum in ordine alphabeti locum quæq; litera ſortita eſt, eiuſdem numerum repræſentat, ut hic uidere licet:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
Α.	Β.	Γ.	Δ.	Ε.	Ζ.	Η.	Θ.	Ι.	Κ.	Λ.	Μ.
13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.
Ν.	Ξ.	Ο.	Π.	Ρ.	Σ.	Τ.	Υ.	Φ.	Χ.	Ψ.	Ω.

Et hic eſt primus ordo numerorũ apud Græcos. Secundario diuidunt Græci totum alphabetum in tres claſſes, quarum prima incipiens ab Alpha unitatum eſt: Secunda incipiens à Iota, denariorum eſt: Tertia incipiens à

LIBER SECVNDVS. CXLI.

Rho, eſt centenariorum: & hic ordo à poſterioribus Græcorum ita ad Hebræorũ imitationẽ inſtitutus eſt. Quia uero Alphabetum eorum ab ea regula tribus literis mancum eſt, neceſſe fuit illis tres figuras adfingere, & literis intercalare, quibus uidelicet ſextum, nonageſimum & noningenteſimũ numeros explicarent, ut in ſequentibus liquet:

1	2	3	4	5	6	7	8	9
α.	β.	γ.	δ.	ε.	ϛ.	ζ.	η.	θ.
10	20	30	40	50	60	70	80	90
ι.	κ.	λ.	μ.	ν.	ξ.	ο.	π.	ϟ.
100	200	300	400	500	600	700	800	900
ρ.	σ.	τ.	υ.	φ.	χ.	ψ.	ω.	ϡ.

Quod ſi alicui harum literarum ſubſignetur uirgula toni acuti, tunc totidẽ millenarios ſignificat, ut in his exemplis: 1000. ͵Α 10000. ͵Ι 100000. ͵Ρ

Tertio modo ſex duntaxat literis deſignandis numeris Gręci utũtur, uidelicet Ι pro unitate: Π pro quinario, quia caput eſt dictionis πέντε hoc eſt quinq;: Δ pro denario, à δέκα: Η, pro centenario, ab ἑκατὸν: Χ pro millenario, à uoce χίλιοι: Μ, pro decẽ milibus, à μυρίοι. Ex quibus ſex literis ſuo modo uſq; ad quatuor numero iunctis, uel aliis adiunctis, cæteros numeros formant, præter Π quæ non multiplicatur, nec ſibi iũgitur, ſed ſemper aliorum quinarios ſignificatur, in ſequentibus exemplis patet:

1	2	3	4	5	6	7	8	9
Ι.	ΙΙ.	ΙΙΙ.	ΙΙΙΙ.	Π.	ΠΙ.	ΠΙΙ.	ΠΙΙΙ.	ΠΙΙΙΙ.
10	11	12	13	14	15	16	20	21
Δ.	ΔΙ.	ΔΙΙ.	ΔΙΙΙ.	ΔΙΙΙΙ.	ΔΠ.	ΔΠΙ.	ΔΔ.	ΔΔΙ.

50.	60.	100.	200.	500.	1000.	5000.	10000.	50000.
⌈Δ⌉.	⌈Δ⌉Δ.	Η.	ΗΗ.	⌈Η⌉.	Χ.	⌈Χ⌉.	Μ.	⌈Μ⌉.

De notis Hebræorum & Chaldæorum, & quibuſdam aliis Magorum notis. Caput XIX.

HEbręorum etiam literę numerorum notas habent, ſed longẽ excellentius quàm ulla aliarum linguarum, cum maxima lateãt in Hebraicis numeris myſteria, ſicuti de his tractatur in ea parte Cabalę, quã Notariacon uocãt. Sunt aũt Hebręorũ literæ numero uiginti duæ principales, quarũ quinq; alias quaſdam diuerſas figuras in fine dictionis ſortiuntur, quas iccirco quinq; finales uocant: quę ſuperioribus additæ, uiginti ſeptem conſtituunt: quæ deinde in tres gradus partitę, quę in primo gradu ſunt, unitates referunt: quę in ſecundo, denarios: quę uero in tertio gradu ſunt, cẽtenarios ſignificant: quælibet autẽ illarũ, ſi grandi depingatur charactere, totidem ſignificat millenarios, ut hic:

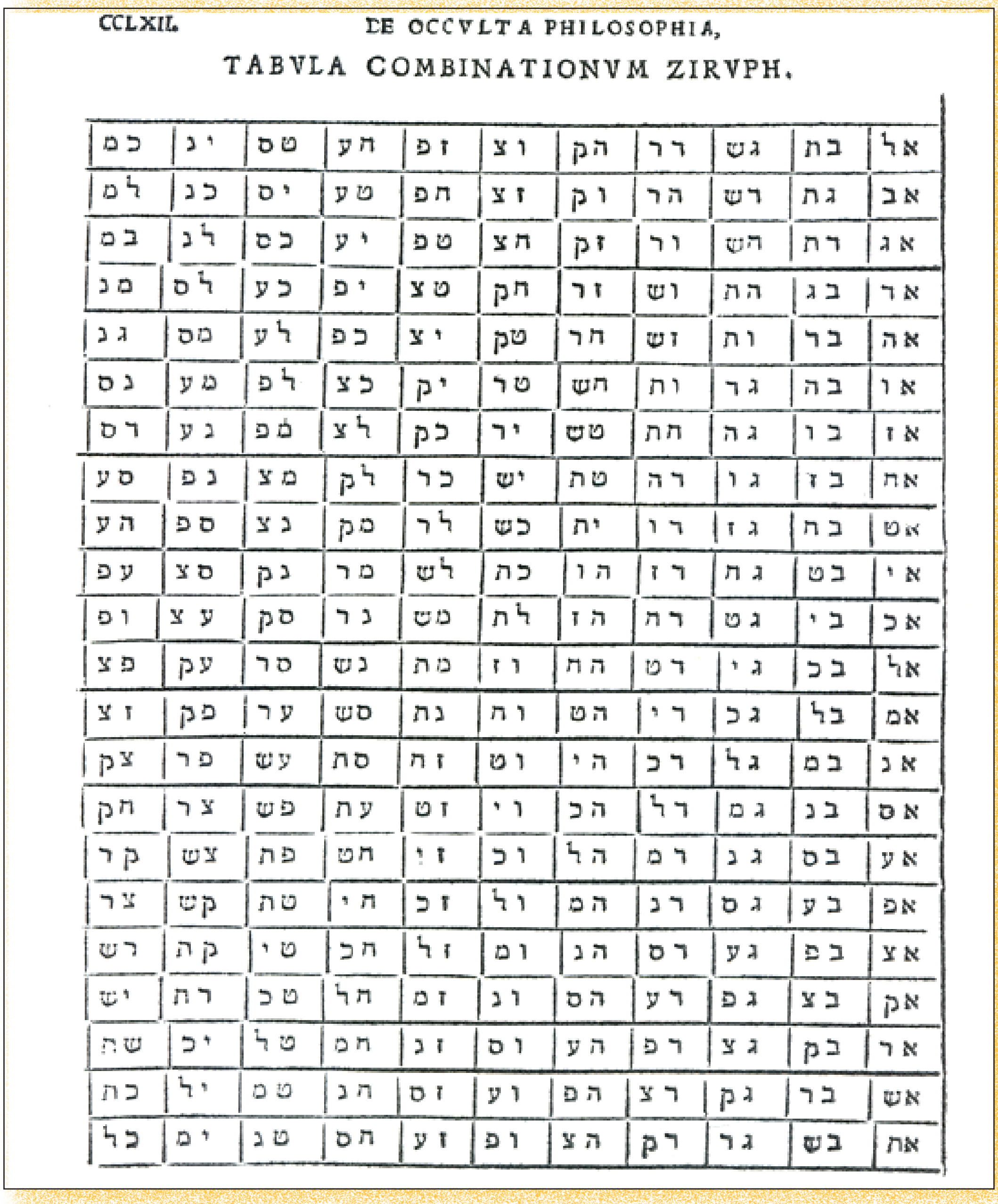
3000.	2000.	1000.
ג	ב	א

De Occulta Philosophia Libri Tres, 1533, by Heinrich Cornelius Agrippa von Nettesheim.
(National Library of Medicine, National Institutes of Health, Bethesda, MD)

their various systems of number and word manipulations.[23] Charles Mendelsohn, in his masterful but brief 1940 paper on the "Chiffre Carré" is dismissive, and bemoans the bulk of fluffy mysticism in Vigenère's *Traicte des Chiffres*.[24] I contend to the contrary that Agrippa the magician helps demonstrate to us the veracity of Vigenère's claim.

Ziruf: Cipher Alphabets

The two Ziruf Tables, as Agrippa calls them, represent the transmission of a critical idea which triggered a leap forward in Renaissance cryptography: the mixed polyalphabet. Alberti's polyalphabet, the same as carried forward by Trithemius, uses only shifts, without permutation of the letters within each alphabet. These Ziruf tables require a user not only to change alphabets every word or character but also to mix the various alphabets, something which could not be managed with a simple cipher wheel such as Alberti created. Agrippa and the Christian cabalists he studied do not show a clear understanding of the potential secular use of these polyalphabets. Possible descendants of Agrippa's Ziruf, conversely, are presented by three later authors, two of whom (Vige-



CCLXII. DE OCCVLTA PHILOSOPHIA,

TABVLA COMBINATIONVM ZIRVPH.

אל	בת	גש	דר	הק	וצ	זפ	חע	טס	ינ	כמ
אב	גת	דש	הר	וק	זצ	חפ	טע	יס	כנ	למ
אג	דת	הש	ור	זק	חצ	טפ	יע	כס	לנ	במ
אד	בג	הת	וש	זר	חק	טצ	יפ	כע	לס	מנ
אה	בד	ות	זש	חר	טק	יצ	כפ	לע	מס	גנ
או	בה	גד	ות	חש	טר	יק	כצ	לפ	מע	נס
אז	בו	גה	חת	טש	יר	כק	לצ	מפ	נע	דס
אח	בז	גו	דה	טת	יש	כר	לק	מצ	נפ	סע
אט	בח	גז	דו	ית	כש	לר	מק	נצ	ספ	הע
אי	בט	גח	דז	הו	כת	לש	מר	נק	סצ	עפ
אכ	בי	גט	דח	הז	לת	מש	נר	סק	עצ	ופ
אל	בכ	גי	דט	הח	וז	מת	נש	סר	עק	פצ
אמ	בל	גכ	די	הט	וח	נת	סש	ער	פק	זצ
אנ	במ	גל	דכ	הי	וט	זח	סת	עש	פר	צק
אס	בנ	גמ	דל	הכ	וי	זט	עת	פש	צר	חק
אע	בס	גנ	דמ	הל	וכ	זי	חט	פת	צש	קר
אפ	בע	גס	דנ	המ	ול	זכ	חי	טת	קש	צר
אצ	בפ	גע	דס	הנ	ומ	זל	חכ	טי	קת	רש
אק	בצ	גפ	דע	הס	ונ	זמ	חל	טכ	רת	יש
אר	בק	גצ	דפ	הע	וס	זנ	חמ	טל	יכ	שת
אש	בר	גק	דצ	הפ	וע	זס	חנ	טמ	יל	כת
את	בש	גר	דק	הצ	ופ	זע	חס	טנ	ימ	כל

Fig. 1. Agrippa's "standard" Ziruf table

nère[25] and Porta[26]) read and borrowed from Agrippa but, unlike him, understood and clearly conveyed the practical uses to which these ciphers could be applied.

Reuchlin[27] may be the first printed author to present what I will call the "standard" Ziruf table,[28] the first of the two tables that Agrippa describes (Figure 1). The second Ziruf table, which Agrippa calls Rationalis (Figure 3, following discussion), is similarly constructed, but with a mixing algorithm evidently created by Agrippa himself. Neither of Agrippa's algorithms is identical to the traditional method of generating tables, described by Aryeh Kaplan, though both of Agrippa's Ziruf tables and the later Zirufs and Ziruf-like ciphers presented by Bellaso and Porta hearken back to this original numerical technique.

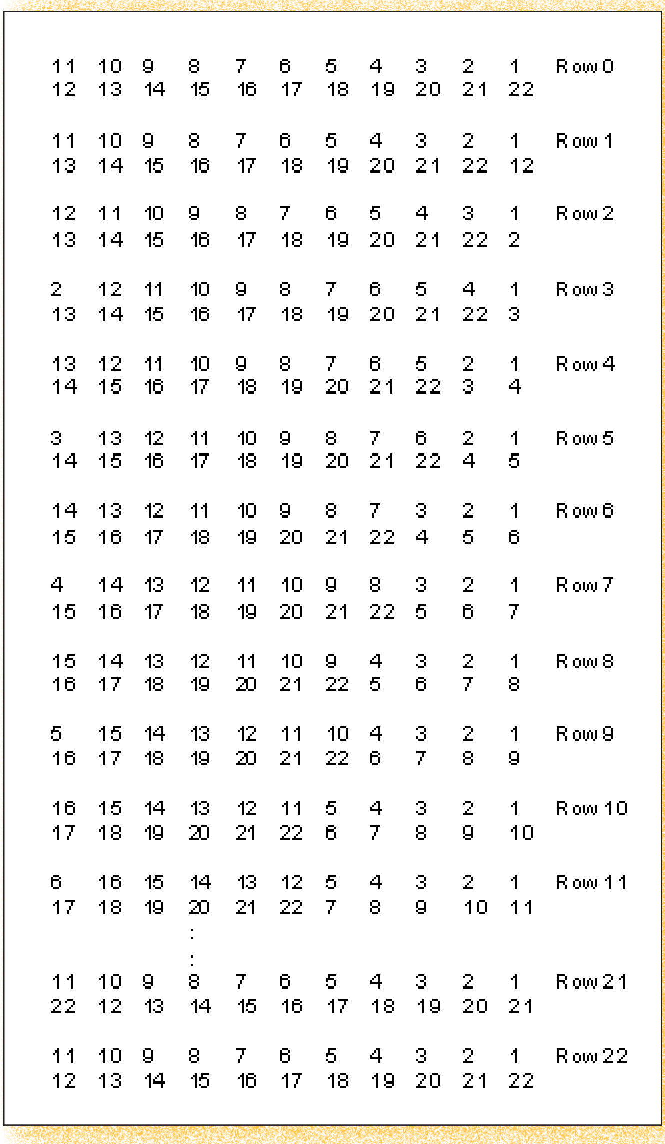
Kaplan calls these tables the 231 Gates, after a phrase in the *Sefer Yetzirah*;[29] this appears to be standard usage among Cabala scholars. There are several ways to present the tables, though they all—at least those predating the Renaissance—are constructed in the same basic way. These are an exercise in combinatorics. Given the twenty-two letters of the Hebrew alphabet, there are 22-choose-2 ways to pair them uniquely, unordered, and without pairing a letter to itself. This gives a total of 231 pairs, which may be represented in an 11×21 table of pairs, which is the usual size of traditional 231 Gates tables.

The traditional construction as described by Kaplan[30] actually is meant to create twenty-two tables of twenty-one rows each. The first table will use the Hebrew alphabet in lexicographic order; the second rotates the ordinary alphabet by one place, so beginning with *bet* and ending with *alef*; the third table shifts two places, beginning with *dalet* and ending with *bet*; and so on. Each table, then, will contain twenty-one rows, though Kaplan implies that only the 11th row of each table is important. The first row of the first table, for example, takes the full alphabet beginning with *alef*. If we treat this row as a cipher in itself, pairing letters as Agrippa does, we have the ABGaD cipher: a traditional Hebrew one, where ב <=> א, and ד <=> ג, and so on—each odd letter pairs with the one following it, each even letter with the one before.

Within a 231 Gates table, each successive row after the first takes every second, third, fourth (and so on) letters from the alphabet, omitting the remainder and cycling through until there are twenty-two pairs filled in. Since we have twenty-two characters, the 11th row, which takes the first and twelfth characters,[31] will oscillate between *alef* and *lamed*, exclusively. If, for our second table, we shift our alphabet by one, starting with *bet* this time, the 11th row will have *bet* and *mem* (the second and thirteenth letters); our third table will give us *dalet* and *nun* (3 and 14), and so on. This pairing of letters, essentially an eleven-long Caesar shift, is the Hebrew cipher ALBaM. This series of twenty-two tables will eventually give all possible pairs of Hebrew characters—though with more work involved than is strictly necessary.

Leon Battista Alberti, inventor of the cipher wheel (School of Florence, Uffizi Gallery)

Agrippa,[32] Reuchlin,[33] and Abraham Abulafia[34] before them built a different sort of table following the same general premise—which we are here calling the "standard" Ziruf. The greater difference between it and the 231 Gates algorithm is that only one table will produce all possible combinations (rather than one row from each of twenty-one tables). Interestingly, the "standard" Ziruf, as Reuchlin has, does not do so in the most efficient way possible, although Agrippa's Rationalis Ziruf does (at least, it generates



11	10	9	8	7	6	5	4	3	2	1	Row 0
12	13	14	15	16	17	18	19	20	21	22	
11	10	9	8	7	6	5	4	3	2	1	Row 1
13	14	15	16	17	18	19	20	21	22	12	
12	11	10	9	8	7	6	5	4	3	1	Row 2
13	14	15	16	17	18	19	20	21	22	2	
2	12	11	10	9	8	7	6	5	4	1	Row 3
13	14	15	16	17	18	19	20	21	22	3	
13	12	11	10	9	8	7	6	5	2	1	Row 4
14	15	16	17	18	19	20	21	22	3	4	
3	13	12	11	10	9	8	7	6	2	1	Row 5
14	15	16	17	18	19	20	21	22	4	5	
14	13	12	11	10	9	8	7	3	2	1	Row 6
15	16	17	18	19	20	21	22	4	5	6	
4	14	13	12	11	10	9	8	3	2	1	Row 7
15	16	17	18	19	20	21	22	5	6	7	
15	14	13	12	11	10	9	4	3	2	1	Row 8
16	17	18	19	20	21	22	5	6	7	8	
5	15	14	13	12	11	10	4	3	2	1	Row 9
16	17	18	19	20	21	22	6	7	8	9	
16	15	14	13	12	11	5	4	3	2	1	Row 10
17	18	19	20	21	22	6	7	8	9	10	
6	16	15	14	13	12	5	4	3	2	1	Row 11
17	18	19	20	21	22	7	8	9	10	11	
			:								
			:								
11	10	9	8	7	6	5	4	3	2	1	Row 21
22	12	13	14	15	16	17	18	19	20	21	
11	10	9	8	7	6	5	4	3	2	1	Row 22
12	13	14	15	16	17	18	19	20	21	22	

Fig. 2. Numerical representation of the standard Ziruf

all possible pairs in the minimum of twenty-one sets of eleven pairings; there are other means of doing so minimally, all of which are equally "efficient"). The standard Ziruf, due to a weakness in the algorithm, must add a 22nd row to be sure to account for all pairs. The Rationalis Ziruf also adds a 22nd row, but this appears to be either for conformity or to include another useful alphabet that is not constructable by the Rationalis algorithm.

The premise of the standard Ziruf is this: each row in the table holds a copy of the complete Hebrew alphabet, folded in half, so that, on the first row, for example, א (*alef*) enciphers to ת (*tov*), and ת enciphers back to א. The naïve, unmixed version of the folded alphabet is the AThBaSh cipher, one of the simpler and better-known Hebrew biblical ciphers. We can think of the unmixed AThBaSh alphabet as an unseen row 0, since it informs the basic structure which is mixed further with each successive row. (It will also reappear at the end of the tables—as that added 22nd row necessary to generate all 231 possible pairs or in the 21st row in the Rationalis—because both algorithms are cyclic.)

It will be easier for non-Hebrew readers to see the pattern developing if we replace the Hebrew letters with numbers—not those which the letters ordinarily represent, because that might cause more confusion, but only the number corresponding to their place in the alphabet. So that א (*alef*) = 1, ב (*bet*) = 2, and so on, then ל (*lamed*) =12, through ת (*tov*) = 22. We have also written each pair of letters in a box one above the other, rather than side-by-side. Beginning with the conjectured row 0, which is AthBaSh, the first few rows and last few proceed as in Figure 2.

The algorithm for mixing rows in the standard Ziruf is contingent on the row number being constructed. Hebrew is written from right to left; and the major characteristic of the simple substitution system AthBaSh is that it folds the alphabet in half, such that the bottom half is written backwards, or left to right. The algorithm for standard Ziruf attempts to maintain this structure, only adapting it so that *alef* (1) is paired with a different letter on each row. Which letter further depends on which row—such that row two pairs *alef* with the second letter, *bet*, row three with the third letter, *dalet*, and so on. The rules for the algorithm are these:

```
Row = $x$
Fill in cells, in order, up to value $floor(x/2)$
IF row is odd-numbered
    write value $ceiling(x/2)$ in top left cell
Write value $ceiling(x/2) + 1$ in cell directly underneath the cell for $floor(x/2)$
Fill in values $> ceiling(x/2) + 1$ on the bottom row, to the right
When you hit the edge, return to the first free gap on the top row, and proceed.
```

For example, if we want to create row 12, first write numbers up to floor(12/2) = 6:

					6	5	4	3	2	1

Then, drop the bottom row, and continue writing with ceil(12/2) + 1 = 7:

					6	5	4	3	2	1
					7	8	9	10	11	12

So, 12 (which will correspond to the letter ל [*lamed*] and is the identifying characteristic of this row) is paired with 1, or א. Then, we return to the top row and fill in the rest—right to left until the cells run out, then left to right across the bottom, as is standard in AthBaSh:

17	16	15	14	13	6	5	4	3	2	1
18	19	20	21	22	7	8	9	10	11	12

To do the next row, number 13, we first start the table going only up to six, since 6 = floor(13/2), and then we stick 7 = ceil(13/2) into the far left:

7					6	5	4	3	2	1

We continue filling in starting with 8 = ceil(13/2) + 1, again, going right to left since this is the bottom half of the row:

7					6	5	4	3	2	1
					8	9	10	11	12	13

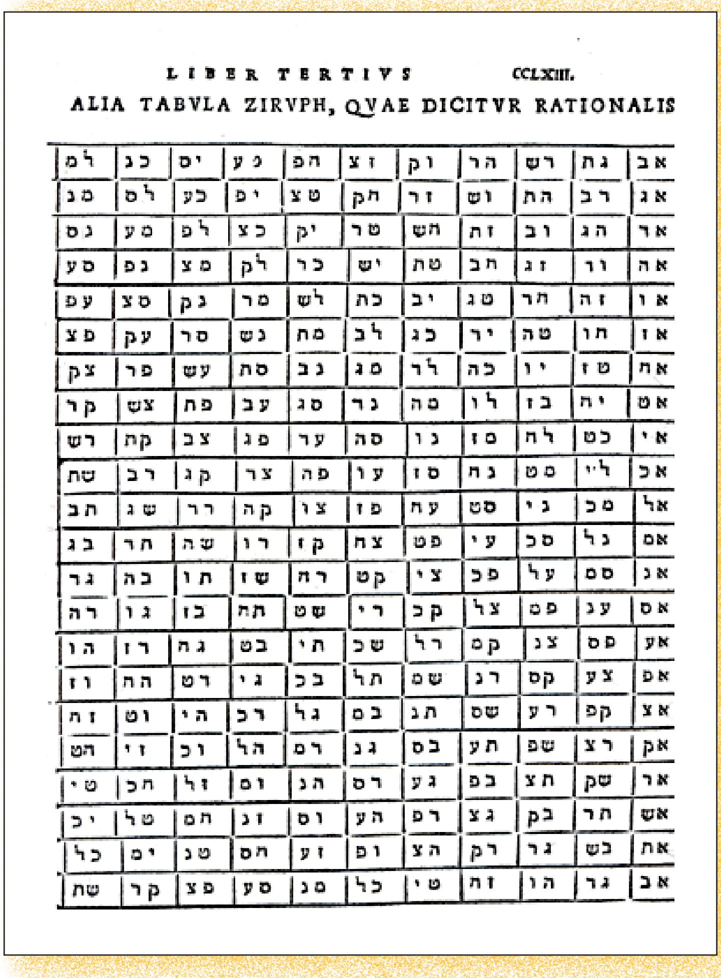
Then we can fill in the remaining spots, starting to the left of the floor() value in the top cells, and hopping over the ceil() value when we get to it:

7	17	16	15	14	6	5	4	3	2	1
18	19	20	21	22	8	9	10	11	12	13

Looking at the table in Figure 2, we'll spot that Row x = 1 is something of an anomaly. Since, clearly, we can never pair *alef* with itself, we replace 1 with its mod 11 equivalent (counting from 1), which is 12.[35]

The flaw in the algorithm should be immediately obvious from taking into account this special case for x = 1. If we substitute x = 12 mod 11 for x = 1, we've just duplicated the pairing of 1 and 12 (א and ל) that would normally occur in row 12. Because of this we would need at least one more row (hence the use of 22 instead of 21) for an exhaustive set of all 231 possible pairs. The algorithm, in fact, forces one repeat for each of 10 pairs—1:12, 2:13, 3:14, 4:15, 5:16, 6:17, 7:18, 8:19, 9:20, and 10:21—nearly a whole row's worth! In fact, this pattern should be familiar as the 11-shift Caesar cipher ALBaM, but missing a pair. Adding ALBaM to the table introduces a repeat in one more pair, 11:22, thus, technically, giving us ALBaM twice: once explicitly and once invisibly in the set of all repeated pairs.

Of all the Ziruf and Ziruf-like tables,[36] the "standard" version uses the most complicated



LIBER TERTIVS CCLXIII.

ALIA TABVLA ZIRVPH, QVAE DICITVR RATIONALIS

למ	כנ	יס	טע	חפ	זצ	וק	הר	רש	גת	אב
מנ	לס	כע	יפ	טצ	חק	זר	וש	הת	רב	אג
נס	מע	לפ	כצ	יק	טר	חש	זת	וב	הג	אד
סע	נפ	מצ	לק	כר	יש	טת	חב	זג	ור	אה
עפ	סצ	נק	מר	לש	כת	יב	טג	חד	זה	או
פצ	עק	סר	נש	מת	לב	כג	יד	טה	חו	אז
צק	פר	עש	סת	נב	מג	לד	כה	יו	טז	אח
קר	צש	פת	עב	סג	נד	מה	לו	כז	יח	אט
רש	קת	צב	פג	עד	סה	נו	מז	לח	כט	אי
שת	רב	קג	צד	פה	עו	סז	נח	מט	לי	אכ
תב	שג	רד	קה	צו	פז	עח	סט	ני	מכ	אל
בג	תד	שה	רו	קז	צח	פט	עי	סכ	נל	אמ
גד	בה	תו	שז	רח	קט	צי	פכ	על	סמ	אנ
דה	גו	בז	תח	שט	רי	קכ	צל	פמ	ענ	אס
הו	דז	גח	בט	תי	שכ	רל	קמ	צנ	פס	אע
וז	הח	דט	גי	בכ	תל	שמ	רנ	קס	צע	אפ
זח	וט	הי	דכ	גל	במ	תנ	שס	רע	קפ	אצ
חט	זי	וכ	הל	דמ	גנ	בס	תע	שפ	רצ	אק
טי	חכ	זל	ומ	הנ	דס	גע	בפ	תצ	שק	אר
יכ	טל	חמ	זנ	וס	הע	דפ	גצ	בק	תר	אש
כל	ימ	טנ	חס	זע	ופ	הצ	דק	גר	בש	את
שת	קר	פצ	סע	מנ	כל	טי	זח	הו	גד	אב

Fig. 3. Agrippa's Rationalis Ziruf

mixing algorithm. Reuchlin, in *De Arte Cabalistica*,[37] does not put the alphabets in clear columns, but rather just packs the letters, in pairs, as close together as was convenient for his typesetter, with no indication of the relationships down columns, or even that there are columns. This could mean Reuchlin was not sure how the Ziruf was used ... or only that his printer was not. In any case, it is easy to overlook the table in *De Arte* since it doesn't look like a table at all to a non-Hebrew reader,[38] and there is understandably little cause for historians of cryptography to seek out primary sources amongst mystics and occultists.

Agrippa's version of the table identifies the letters which will encipher to each other by enclosing each pair in a single cell in his table. Vigenère reprinted Agrippa's standard Ziruf, likewise enclosed in a grid and with the addition of both alphabetic and numerical keys at the top and side of the table.[39] We know Vigenère read Agrippa and Reuchlin (both are cited by name). Vigenère could have learned the standard Ziruf from either, though his formatting is closer to Agrippa's. Vigenère, Porta, and Bellaso all demonstrate additional tables of polyalphabets which follow this general format of paired half-alphabets, differing only in the mixing algorithm. There is precedence for such pairing in Agrippa: we have already mentioned that in addition to the "standard" Ziruf, Agrippa presented one he apparently created which uses a different mechanism for mixing the alphabets.

The mixing algorithm for the Ziruf Agrippa calls "Rationalis"[40] is simpler, and, as the name implies, rather more rational (Figure 3). Like the standard Ziruf, it begins with AthBaSh implicitly. *Alef* (1) is again pegged to the first spot in each row. Each row is based upon the last, with an update created by popping out whatever letter-number appears to the left of *alef*, rotating the rest of the characters clockwise, and then placing the "popped" character in the now-vacant bottom right cell. In Figure 4 we show the following:

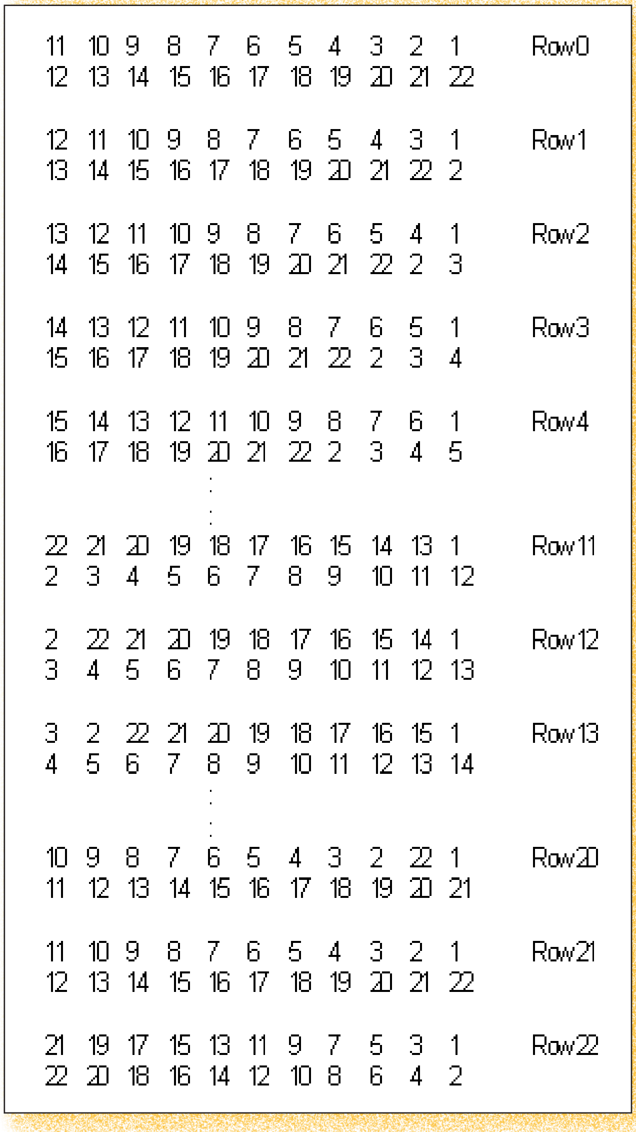
- enough of the first several rows to establish the pattern;
- the middle rows, to establish that the pattern continues as the end of the sequence of popped-and-pushed characters cycles around and wraps to the top half of a row; and
- the last several rows.

Note that the pattern has returned to AThBaSh by row 21. Row 22 is entirely unnecessary if we are exclusively concerned with following the pattern, though Agrippa inserts another traditional Hebrew cipher, ABGaD. We mentioned this cipher earlier, as the first row in the traditional Ziruf explained by Kaplan.

Porta's and Bellaso's versions of Ziruf bear a stronger resemblance to the Rationalis than the "standard" Ziruf. They are rather more similar to one another than to Agrippa's, so we cannot be certain *Occulta Philosophia* was the source for these authors. Bellaso, who has no other apparent connections to either Agrippa or the Cabalists, published his version before Porta (though after Agrippa), and consequently created the concept of a keyed polyalphabet.[41]

Bellaso's earliest table—and he published several versions, each with successively more complicated mixing and keying algorithms—is only eleven rows long, not twenty-two, though he does use a twenty-two-character Latin alphabet. Naturally, since he is working with Latin, the characters are presented left to right, though the bottom half of each row does *not* reverse order—making his unmixed alphabet a simple 11-shift Caesar cipher, like ALBaM. Also, Bellaso mixes only the bottom half of the row; the entire top half of the row is fixed for all alphabets in the system. This is somewhat like Agrippa's Rationalis algorithm, except in the Rationalis only the first character is fixed, and all the rest rotated around it. Bellaso's cipher, again replacing numbers for letters, is as shown (Figure 5).[42]

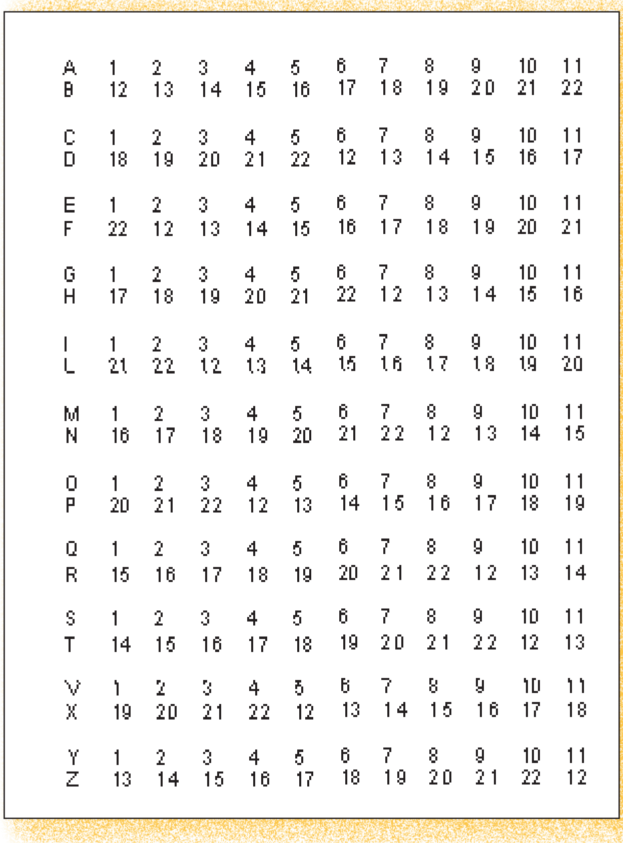
The pattern may be clearer if we note that Bellaso has used a one-step mixing algorithm, in which each new row depends on the one before, but then has disordered the rows within the table. Row A-B in the table is the initial, simple Caesar shift alphabet. E-F would then be the next in logical order, then I-L, O-P, V-X, C-D, G-H, M-N, Q-R, S-T, and Y-Z. If reordered according to the logic of the table, the "key" is the Latin alphabet, beginning with vowels (A, E, I, O, V) followed by consonants (C, G, M ... though using only those key letters from the top line of the pair in each row). Bellaso's table does not include all possible pairs of letters, by definition.



11	10	9	8	7	6	5	4	3	2	1	Row0
12	13	14	15	16	17	18	19	20	21	22	
12	11	10	9	8	7	6	5	4	3	1	Row1
13	14	15	16	17	18	19	20	21	22	2	
13	12	11	10	9	8	7	6	5	4	1	Row2
14	15	16	17	18	19	20	21	22	2	3	
14	13	12	11	10	9	8	7	6	5	1	Row3
15	16	17	18	19	20	21	22	2	3	4	
15	14	13	12	11	10	9	8	7	6	1	Row4
16	17	18	19	20	21	22	2	3	4	5	
				⋮							
22	21	20	19	18	17	16	15	14	13	1	Row11
2	3	4	5	6	7	8	9	10	11	12	
2	22	21	20	19	18	17	16	15	14	1	Row12
3	4	5	6	7	8	9	10	11	12	13	
3	2	22	21	20	19	18	17	16	15	1	Row13
4	5	6	7	8	9	10	11	12	13	14	
				⋮							
10	9	8	7	6	5	4	3	2	22	1	Row20
11	12	13	14	15	16	17	18	19	20	21	
11	10	9	8	7	6	5	4	3	2	1	Row21
12	13	14	15	16	17	18	19	20	21	22	
21	19	17	15	13	11	9	7	5	3	1	Row22
22	20	18	16	14	12	10	8	6	4	2	

Fig. 4. Patterns in the Rationalis Ziruf

Porta's version of the cipher table uses the same mixing algorithm on each row and omits the mixing of the rows within the table.[43] Understandably, since Porta published some years later, Bellaso was rather snippy about Porta's apparent uncredited use of his cipher.[44] Vigenère, in his discussion of the Ziruf, makes note of this disagreement but adds that neither of them is the original author.[45] In his earlier discussion of ciphers and Cabala in general, he makes a



A	1	2	3	4	5	6	7	8	9	10	11
B	12	13	14	15	16	17	18	19	20	21	22
C	1	2	3	4	5	6	7	8	9	10	11
D	18	19	20	21	22	12	13	14	15	16	17
E	1	2	3	4	5	6	7	8	9	10	11
F	22	12	13	14	15	16	17	18	19	20	21
G	1	2	3	4	5	6	7	8	9	10	11
H	17	18	19	20	21	22	12	13	14	15	16
I	1	2	3	4	5	6	7	8	9	10	11
L	21	22	12	13	14	15	16	17	18	19	20
M	1	2	3	4	5	6	7	8	9	10	11
N	16	17	18	19	20	21	22	12	13	14	15
O	1	2	3	4	5	6	7	8	9	10	11
P	20	21	22	12	13	14	15	16	17	18	19
Q	1	2	3	4	5	6	7	8	9	10	11
R	15	16	17	18	19	20	21	22	12	13	14
S	1	2	3	4	5	6	7	8	9	10	11
T	14	15	16	17	18	19	20	21	22	12	13
V	1	2	3	4	5	6	7	8	9	10	11
X	19	20	21	22	12	13	14	15	16	17	18
Y	1	2	3	4	5	6	7	8	9	10	11
Z	13	14	15	16	17	18	19	20	21	22	12

Fig. 5. Bellaso's 1553 version of the reciprocal cipher

stronger claim about the origin of the idea to use a key with a cipher,

> *Ceste table au reste, soit a Belasio, soit a Baptiste Porta, qu'on la vueille attributer, n'est toutes fois a parler au vray de l'un ny de l'autre, ains contretiree sur les Ziruf du Iezirah, de 22 lettres pareillement, combien qu'on se puisse de vingt, pour en faire un chiffre carre.*[46]

So Vigenère, at least, saw the connection between this particular cipher and the Cabalistic Ziruf. He reprints the standard Ziruf [47] in Hebrew, as Agrippa did, several chapters later in the book (after he has introduced his readers to the Hebrew alphabet and Cabala). More immediately after his discussion of the argument between Porta and Bellaso, Vigenère presents a Latin cipher table in this same style[48]—quite like the contested Porta/Bellaso cipher, but with twenty letters instead of twenty-two.[49] The mixing algorithm is exactly the same as Porta and Bellaso's, without Bellaso's disordering of rows within the table. The table takes on a slightly different appearance because of the smaller alphabet (Figure 6). Vigenère also borrows Bellaso's (and Porta's) use of a key phrase to control encryption of a message.

Neither of two later versions of the table[50] uses exactly the same mixing algorithms as either the standard Ziruf or Agrippa's Rationalis Ziruf; and the later cipher alphabets are based on a single Caesar shifted alphabet, not one folded like the Zirufs. However, the overall format of the tables, particularly the pairs of half-alphabets each mixed progressively from the preceding alphabet, mirrors the format of the Ziruf very well. That the reciprocal ciphers, as Bellaso called them, are only half as long as the Zirufs is a result of them being half as mixed; that is, Bellaso's table fixes the top half of the alphabet and mixes only the bottom.

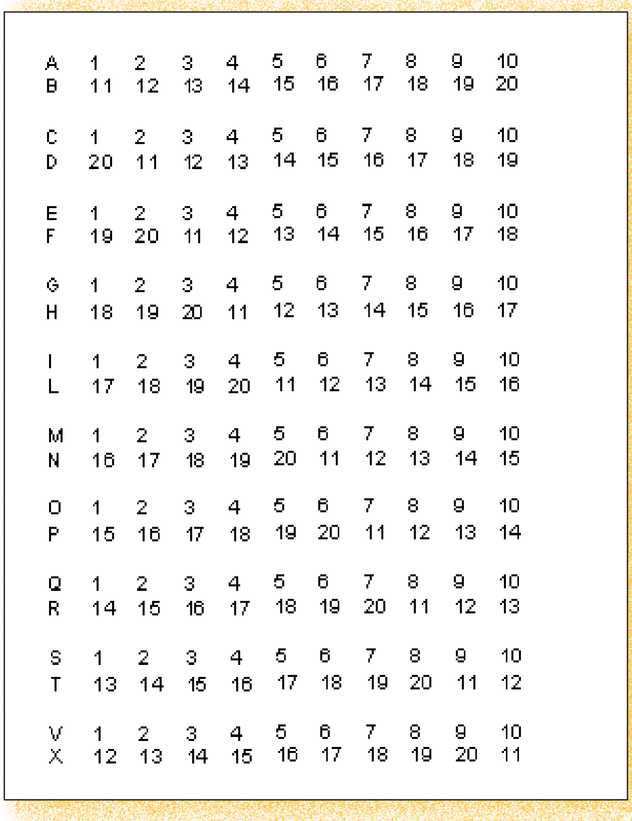
Bellaso went on to produce more complicated versions of this cipher, though we have essentially no record of what he thought or whom he read, only what is printed in his set of short pamphlets.[51] Porta, on the other hand, wrote extensively and reprinted many ideas first laid out by earlier authors, so we have a good idea of what he read. We know he was not a Cabalist; the only references he makes to Cabalists or Cabalism are lifted directly from Agrippa's *Occulta Philosophia*. Vigenère, on the other hand, considered himself a Cabalist and read extensively on the topic. We could explain the appearance of the Ziruf table in Vigenère as a result of his extra-Agrippean readings. But we can't do the same for Porta and Bellaso.

It is accepted in the history of cryptography that Bellaso was the first to present the keyed reciprocal cipher (which we are calling the Ziruf, after Agrippa and Vigenère). However, Agrippa printed his versions of the Ziruf several years before Bellaso began circulating his cipher pamphlets. The timing is appropriate and the similarity between the two cipher systems is striking. *Occulta Philosophia*, being controversial, was widely circulated and printed in at least three editions before 1540. It is possible Bellaso at some point came across a copy of Agrippa; if not Agrippa, then there is enough similarity between his cipher and the Zirufs to imply that Bellaso must have had some exposure to other writings on Cabala.

Summary

If we accept that the Ziruf tables preclude Bellaso's reciprocal cipher, then Bellaso can be credited only with the original invention of a *keyed* polyalphabet of this form (with Vigenère contesting even this). Agrippa, Reuchlin before him, and several generations of Jewish Cabalists even earlier had developed this style of polyalphabet before any appearance of the concept in mainstream Renaissance Europe.

There is too much conflicting data on Agrippa to allow us to make a declaration on whether or not he was an active cryptographer. However, we can establish without doubt that he—or at least his ciphers—had an impact on later cryptography. I can't clear his name of the reputation as a magician, as Ernst and Reeds did for Trithemius. But perhaps this slightly different perspective on the origin, or possible origin, of some familiar ciphers in the misty murk of Renaissance occultism and Cabala, will add a little more color to the history of cryptography.



A	1	2	3	4	5	6	7	8	9	10
B	11	12	13	14	15	16	17	18	19	20
C	1	2	3	4	5	6	7	8	9	10
D	20	11	12	13	14	15	16	17	18	19
E	1	2	3	4	5	6	7	8	9	10
F	19	20	11	12	13	14	15	16	17	18
G	1	2	3	4	5	6	7	8	9	10
H	18	19	20	11	12	13	14	15	16	17
I	1	2	3	4	5	6	7	8	9	10
L	17	18	19	20	11	12	13	14	15	16
M	1	2	3	4	5	6	7	8	9	10
N	16	17	18	19	20	11	12	13	14	15
O	1	2	3	4	5	6	7	8	9	10
P	15	16	17	18	19	20	11	12	13	14
Q	1	2	3	4	5	6	7	8	9	10
R	14	15	16	17	18	19	20	11	12	13
S	1	2	3	4	5	6	7	8	9	10
T	13	14	15	16	17	18	19	20	11	12
V	1	2	3	4	5	6	7	8	9	10
X	12	13	14	15	16	17	18	19	20	11

Fig. 6. Vigenère's version of the reciprocal cipher (first example)

Notes

1. Agusto Buonofalce, "Bellaso's Reciprocal Ciphers," *Cryptologia* 30, no. 1 (2006).
2. Blaise de Vigenère, *Traite des Chiffres* (Paris: L'Angelier, 1586).
3. Thomas Ernst, "Schwarzwieße Magie," *Daphnis* 25, no. 1 (Amsterdam: Rodopi B.V., 1996); Thomas Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," *Cryptologia* 22, no. 4 (1998); James Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia," *Cryptologia* 22, no. 4 (1998).
4. Agrippa von Nettesheim, *Three Books of Occult Philosophy*, ed. Donald Tyson (London: 1651; St. Paul, MN: Llewellyn, 1995), xix; Henry Morley, *The Life of Henry Cornelius Agrippa von Nettesheim*, Vol. I, facsimile (London: Chapman and Hall, 1856; Elibron Classics, 2006), 228-229.
5. Cornelius Agrippa, Epistolae in *Occulta Philosophia.*
6. Noel L. Brann, *Trithemius and Magical Theology*, SUNY Western Esoteric Traditions (Albany, NY: State University of New York Press, 1999), 7.
7. Translated as "On the Uncertainty and Vanity of the Sciences and Arts, An Invective Declamation," and commonly called *De Vanitate*. Agrippa, *De Occulta Philosophia Libri Tres*, ed. Vittoria Perrone Campagni, based largely on the same 1533 Cologne printing, the 1531 printing of Book I only, and the MS copy sent to Trithemius and still housed at University of Wurzburg. In *Studies in the History of Christian Thought*, no. 48 (Leiden, Netherlands: E. J. Brill, 1992), 7-8.

8. Agrippa, Retraction in *Occulta Philosophia*; see also the trio of letters prefacing the retraction, which seem to espouse a sort of ambiguous attack on magic, or those who pursue it.
9. Compagni, page 7 footnote, citing *De Vanitate,* 104.
10. See Wayne Shumaker, *The Occult Sciences in the Renaissance* (Los Angeles: University of California Press, 1972) *passim*, in particular 74-76; and Shumaker, *Renaissance Curiosa* (Tempe, AZ: Arizona Center for Medieval and Renaissance Studies, 2003), 175-176.
11. I give, by way of example, the impressive influence of Francesco Giorgio of Venice, called Zorzi. Compagni (36, 42) has found, aside from the easily dismissed parallels in philosophy, several large sections of text copied outright, though not credited, from Zorzi's *De Harmonia Mundi*, published in Venice, 1525. The name "Zorzi" or "Georgius" never appears in the whole of *Occulta Philosophia*. Agrippa likewise borrows many concepts from the *Corpus Heremeticum* (a book on Pythagorean-like magic supposedly written by an ancient Egyptian and later found to be first or second century CE), though he hadn't apparently read it himself, only Marcilius Ficino's translation (also in Compagni, page 32).
12. "…tres libros de magia compendio brevitatis complexos recentibus his diebus composui et *De occulta philosophia* minus infenso titulo inscripsi" (roughly translated: "these are three books I am writing as a brief compendium on magic and 'On Hidden/Secret Philosophy' is their title"). From the cover letter Agrippa sent along with a draft, manuscript copy in 1510 to Trithemius, reproduced in the 1533 edition, and in Agrippa, *De Occulta Philisophia Libri Tres*, Cologne, 1533. Facsimile ed. Karl Anton Nowotny, Graz, Austria: Akademische Druck u. Verlaganstalt, 1967; Compagni; and Tyson.
13. I distinguish between Jewish cabalism, which has quite a long history, and Christianized or "Hermetic" Cabala, such as what Agrippa and his sources were propounding. Some writers consider the Christianized and Hermetic versions as separate. The Christianized version probably originated with Abraham Abulafia, a 13th-century wandering mystic who added elements which would make Cabala more palatable to Christian audiences in hopes of eventually converting them. He is likely a major source for Reuchlin's Ziruf tables, to be discussed shortly. However, Reuchlin, Zorzi, and the others were all writing shortly after the "rediscovery" of the *Corpus Hermeticum* and around the time of Ficino's translation of it to Latin. All of these Christian cabalists, coming from the Neoplatonic philosophical background characteristic of the humanist movement, were quick to introduce elements of the equally Neoplatonic *Hermeticum* into their version of cabalism—whence the Hermetic flavor of Cabala originated.
14. Aryeh Kaplan, *Sefer Yetzirah: The Book of Creation*, rev. ed. with commentary (San Francisco: Weiser Books, 1997), introduction.
15. Kaplan, appendix IV, 336-337. This means that Agrippa's only contact with the original text or Hebrew commentaries on it (arguably even more valuable than the text) was filtered through his secondary sources, Reuchlin and Zorzi. I am skeptical that Agrippa read Hebrew.
16. Johannes Reuchlin, *De Arte Cabalistica, 1517* (volume bound with *De Verbo Mirifico, 1494*), (Stuttgart-Bad Cannstatt, Germany: Friedrich Frommann Verlag, Gunther Holzboog, 1964), fol. N6r in the Latin version, or 327 in the English translation.
17. Agrippa, Bk III Cap [chapter] XXV.
18. Vigenère, fol. 94r.
19. Kaplan, commentary on 2:4, starting page 109. He uses, in particular, tables of Abulafia and Eliezar (of Worms, Germany) which, as we discussed, are probably the inspiration for Reuchlin's.
20. This is my own conclusion. Kaplan shows how one of the versions of the 231 gates can be used to produce each letter-pair in ALBaM, through 11 iterations of the process (page 117). I find the AThBaSh cipher, and variations of it, as the basis of both Reuchlin's Ziruf (f N6v-r) and in Kaplan's exposition of Abulafia's version of Ziruf (pages 120-123), and as the final line of each table, logically produced as the table is built.
21. Tyson, Appendix VII, 762.
22. Ibid.
23. Vigenère, page 186 primarily, also 32, 94, 182. He further mentions Johannes Reuchlin, 184, and Pico della

Mirandola, 10—two men whose work heavily influenced Agrippa and who are considered among the first proponents of Christianized Cabala, such as Vigenère and Agrippa both espouse, in Europe.

24. Charles Mendelsohn, "Blaise de Vigenère and the 'Chiffre Carré'," *Proceedings of the American Philosophical Society* (March 22, 1940) 82, no. 2, 113, 123.
25. Vigenère, fol. 275v, cites Agrippa directly in reference to the AIQ BeKar, or Pig Pen, cipher.
26. Giambattista (della) Porta, *De Occultis Literarum Notes*, Libri IIII, in the collection of the National Cryptologic Museum (Jacobum Foillet, Expensis, 1593) Bk II, Cap XIV throughout, as a good example, though there are others, discussed in other articles.
27. Compagni, ed., Agrippa, Bk II Cap XXV, 473 of her edition.
28. Kaplan, page 122, describes a whole assortment of Ziruf-like tables attributed to medieval Hebrew cabalists. Most are similar only in shape to Agrippa and Reuchlin's, though one table created by Abraham Abulafia looks to be the same as the "standard." Abulafia, controversially, taught a highly Christianized form of Cabala, in order to broaden the appeal outside the Jewish communities; it is likely enough that Reuchlin got his version of the table either from the writings of Abulafia, or of someone commenting on Abulafia.
29. Kaplan, 122-124.
30. Ibid., this explanation spread over the chapter on the 231 gates.
31. Put another way, each character {x} = 1 mod 11 mod 22. (I use mod 22 to remind us to keep the cycle within the alphabet space.) The mod 11 is the functional operation which selects letters. So, in these terms, each row could be represented by {x} = 1 mod *n* mod 22, where *n* is the row number and {x} is the set of 22 letters, inclusive of repeats, that will fill in the row.
32. Agrippa, Bk II Cap XXV.
33. Reuchlin (*Arte*), Bk III N6r-v.
34. Kaplan, 122.
35. We won't go so far as to say medieval Hebrew scholars were doing modular arithmetic so many generations before Carl Gauss; rather that the Cabalists were using concepts that were novel at the time they were writing (equivalent to Fibonacci and the Chinese Remainder Theorem), and that prefigured modular arithmetic.
36. Including not just Reuchlin's, Agrippa's, and Abulafia's, but the ones created by Bellaso, della Porta, and Vigenère as well, which we will discuss.
37. Morley, 63-66; Christopher I. Lehrich, *The Language of Demons and Angels: Cornelius Agrippa's Occult Philosophy* (Leiden, The Netherlands: Brill, 2003), 26 (possibly from Morley); Agrippa lectured on *De Verbo Mirifico* at the University of Dole (France), not *De Arte*, which had not yet been written. The books were later printed together (and again in a modern edition). Agrippa read both, though could not have incorporated the Ziruf into his books until closer to 1520, nearly ten years after the initial manuscript and his Dole lectures.
38. Reuchlin, Bk III, N6r-v.
39. Vigenère, fol. 95r. Agrippa's version has no key, and therefore would have to be used in strict order, just as his Tables of Commutation (that is, the Tabula Recta or Chiffre Carré) would. Further, on 46, 96v and 97r, Vigenère shows alternate ways to print the standard Ziruf, though he replaces the Hebrew characters with his best guess at a Latin transliteration, and, therefore, he flips from right-to-left printing to left-to-right. In all these examples he calls the tables "Ziruph" and is quick to assign authorship to the "Sepher Ietzirah".
40. Agrippa, Bk III Cap XXV.
41. Buonofalce, *Cryptologia* 30:1, 40.
42. Buonofalce, 41. I have replaced the Latin characters in the alphabets with their equivalent numbers, to make the structure more clear, though I have left the uppercase key letters, on the left, as given.
43. Porta, Bk II Cap XVI.
44. Buonofalce, 50, citing Vigenère, fol. 36r-v.
45. Vigenère, fol. 186.
46. Vigenère, fol. 36v-37r. Loosely translated, this says that no matter whether the cipher is attributed to Porta or Bellaso, the true origins of the table are in the Ziruf of the *Sefer Yetzirah.* Mendelsohn translates this passage more precisely himself, though he interprets it as a reference to the so-called Vigenère Square (also called "*chiffre carré*"). That cipher, however, bears no resemblance to the Ziruf. I have noticed that Vigenère called a number of other ciphers *carré* (see page 100

for an example); he may intend the term *carré* to mean any tabular or box-shaped cipher. Furthermore, this section of the book is a discussion of keys, not of the ciphers themselves. It seems that Vigenère is arguing that the Cabalists originated keying, not just the Ziruf cipher tables, though I find no other proof to support his assertion.

47. Vigenère, fol. 95r.

48. Vigenère, fol. 46r.

49. Vigenère fol. 37r; following the quote given above, he explains his justification for the smaller set of letters (that he wants a couple of spares to use as nulls) which he will use in the cipher he prints and demonstrates the use of several pages later.

50. Vigenère, 96-97.

51 . Buonofalce, 49-50.

The Dawn of American Communications Intelligence: The Spanish-American War and After

David A. Hatch

Shortly after the turn of the twentieth century, many nations of the world, including the United States, began to take advantage of the new medium of wireless telegraphy, soon to be known as radio, to increase the flexibility and speed of government communications. Over time, most of these nations also came to realize that eavesdropping on foreign radio communications constituted an invaluable source of military and civil information.

Radio was a new medium. Transmissions were made in Morse code, and the only existing radio stations with regular broadcasts—and they were still few—were the property of governments, businesses, or interested amateurs. These stations were used to send cables to places telegraph lines did not go, usually transmitting official or business communications, or, occasionally, distributing press items.

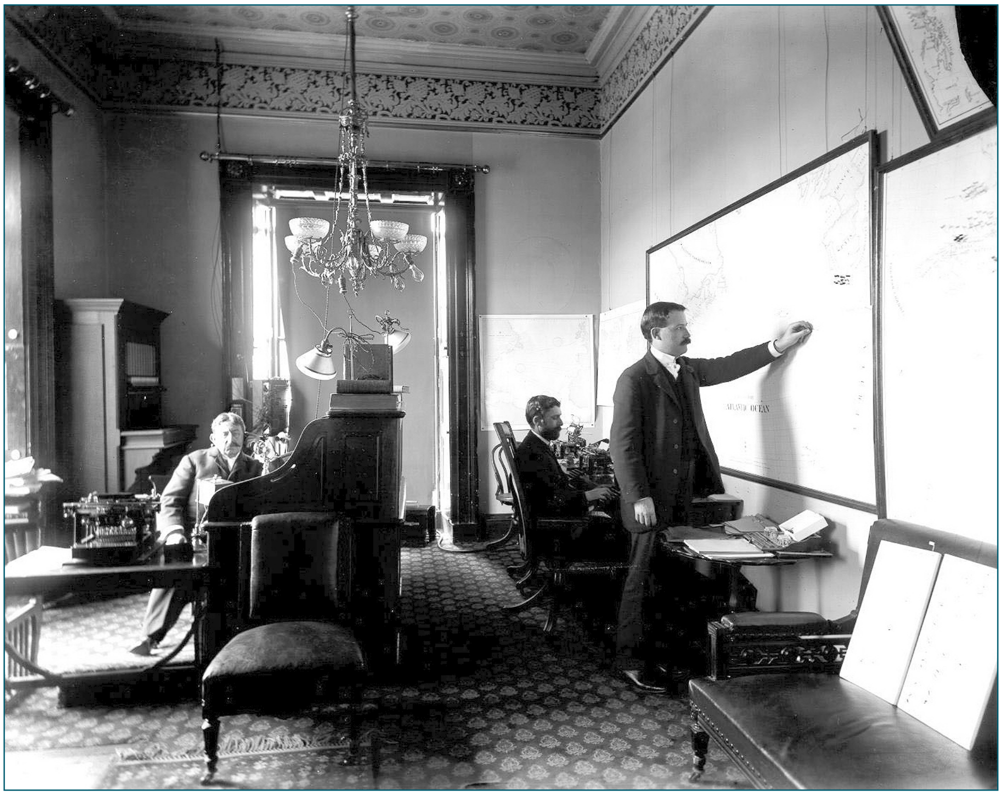
The U.S. Army began using wireless radios for some activities as early as 1903, but began deploying radios regularly for operations around 1910. Even while it was still studying the technology and operational doctrine of radio communications for its own use, it began the practice of intercepting foreign messages, primarily Mexican, for intelligence purposes. Some intercepted messages were enciphered.

This is the story of the origin of U.S. Army signals intelligence, or radio intelligence, as it was called in its infancy. This source was heavily entwined with the development of military intelligence as a profession.

The American Civil War arguably was the world's first information war in the modern sense. Both the Union and Confederacy made extensive and innovative use of the telegraph and tactical signaling on the battlefield for communications and communications intelligence. However, ironically, in the three decades from 1865 to the Spanish-American War, the U.S. government was not itself a heavy user of telegraphic communications, much less engaged in communications intercept.

Neither the U.S. government nor military was much interested in intelligence as an official activity. The only civilian organization engaged in intelligence on behalf of the federal government was the Secret Service. Subordinate to the Treasury Department, agents primarily were concerned with catching counterfeiters.

The U.S. Army and Navy had had intelligence organizations since the 1880s—the Office of Naval Intelligence had been established in March 1882 and the Military Information Division in October 1885—but they served departmental interests exclusively. Moreover, they became repositories of



1898 White House communications room with telegraph operator and wall map (U.S. Army)

military and naval data, but did not do analytic studies or undercover operations.[1] The one truly professional U.S. intelligence capability in 1898 was a network of military attachés assigned in key foreign locations.

The Spanish-American War, as it changed much in U.S. government and military practices, also changed attitudes and activities in regard to communications and intelligence.

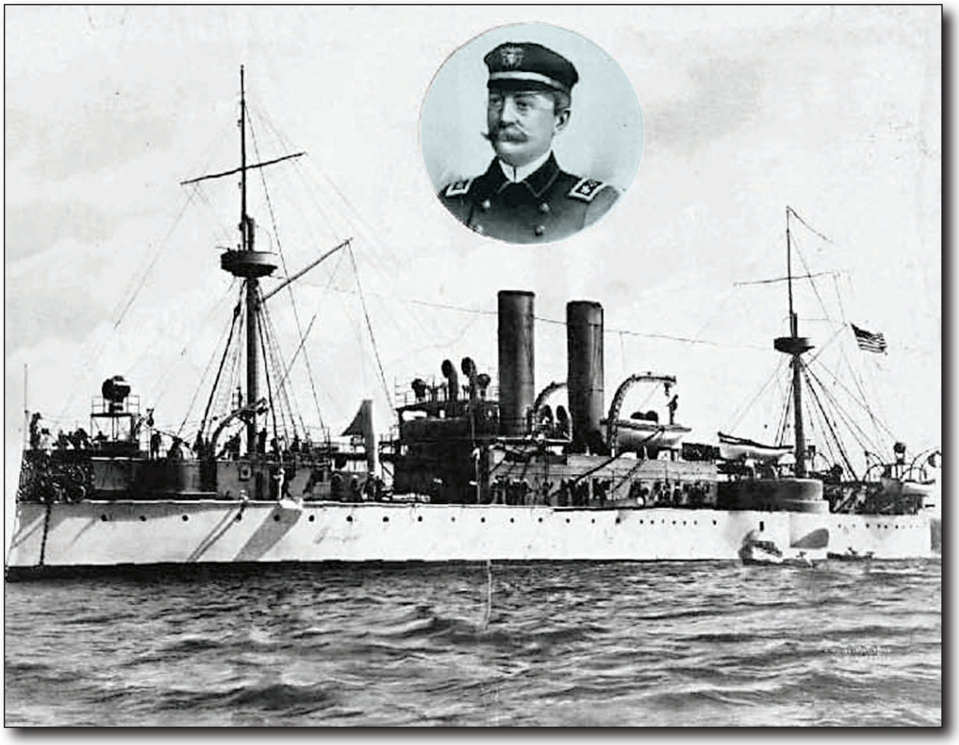
After months of tension between the United States and Spain, primarily over Spanish treatment of its colony, Cuba, exacerbated by a jingoistic press in the U.S., the two countries went to war.

The actual conflict lasted only a few months, essentially the summer of 1898. The inept military campaign has been well told elsewhere; this article is concerned with the development in communications intelligence that affected the war and the effect of the war on the practice of intelligence in the United States.

Martin L. Hellings was a long-time employee of Western Union, and, in 1897, managed its subsidiary, the International Ocean Telegraph Company—which operated the subsea cables from Havana to Key West to mainland Florida.

In December 1897 President McKinley ordered the battleship *Maine* to stand by in Key West, in case it was needed in Havana to protect Americans there. The captain of the *Maine*, Charles D. Sigsbee, was an old friend of Martin Hellings, and asked Hellings to notify him if there were any trouble with the Havana-Key West line that would interfere with reception of warnings sent from Havana.

Hellings went his old friend one or two better. The Havana telegraph office was subordinate



USS *Maine*. Retouched photograph by A. Loeffler, with an inset of her last commanding officer, Captain Charles D. Sigsbee, USN. This print was published as a memento following the ship's loss on February 15, 1898. (U.S. Navy)

to him; its employees would keep him informed of any local developments of interest to the U.S. In addition, there was a branch telegraph office in the Spanish governor general's palace; its employees would now, secretly, give the United States copies of the highest level Havana-Madrid communications.

This "second-hand COMINT" played no part in the subsequent tragic history of the *Maine*, which exploded in Havana harbor on February 15, generating great anger at Spain across the U.S., and putting the country into a situation in which war was near inevitable. The secret source provided usable information only in subsequent events.

The one truly professional U.S. intelligence capability in 1898 was a network of military attachés. Their spies reported the assembly of a large Spanish fleet and preparations for its departure. Part of the fleet under Admiral Pascual Cervera y Topete departed the Cape Verde Islands in late April.

The vital question was Cervera's destination. The Philippines, where his fleet outgunned that of Admiral Dewey? Florida, where his fleet could sink the ragtag collection of transport ships the U.S. Army was using to send an expeditionary force to Cuba? More frightening, the east coast of the United States, where it could shell the great urban areas? There was acute anxiety among residents of these coastal cities.

In reality, Cervera's fleet was in poor fighting condition, and had been ordered to the Caribbean before adequate provisioning had been completed. Cervera barely made it to the Cuban port of Santiago, where he got into harbor unnoticed by the Americans.

His first act upon arrival in Santiago was to telegraph the Spanish governor of the island that he

Admiral Pascual Cervera y Topete

had arrived. The message also was covertly relayed to Martin Hellings in Key West. The Havana-Key West line had continued operation despite the outbreak of war. Hellings had been given a commission in the Volunteer Signal Corps, and the Signal Corps ran his office.

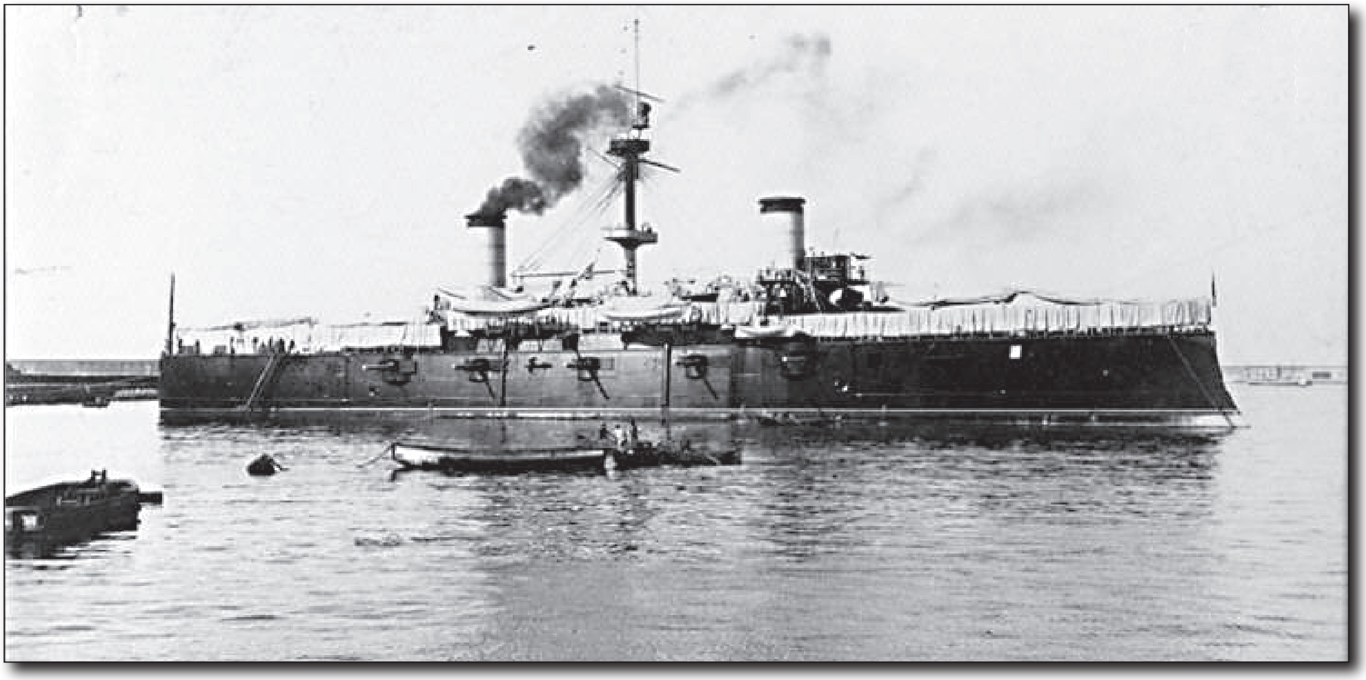
The information about the location of the Spanish fleet was relayed to Washington, where it was sent to the White House—only a short time after its reception in Florida. The result of the rapid transmission of this intelligence was a decision for a naval blockade of Santiago de Cuba. In addition, American war plans were changed to send land forces to attack the port from behind, instead of using them in the Havana region, as originally planned. Thus, ironically, although the United States had no official COMINT capability, "second-hand" COMINT proved important in answering one of the most critical questions of the war and determining the direction of the American campaign in Cuba.[2]

The Spanish-American War in 1898 produced many stirring patriotic images of military action, and the war was won by the valor of the troops. But, to careful observers, the war revealed pervasive American military ineptitude and weakness. From mobilization to transport to equipment to supply to planning to intelligence, the U.S. had done poorly. Some observers claimed that Spain was probably the only European nation the United States could have whipped.

Much of the failure could be attributed to poor top-level organization. The War Department was divided between the secretary, with hide-bound, civilian-controlled bureaus responsible for support activities subordinate to him, and the commanding general of the Army, who controlled troops and issued operational orders. The two halves of the department did not coordinate with each other; there was no formal organization for short- or long-term planning on either side of the department.

The U.S. had no intelligence organization in the modern sense, and little idea what to do with one. While some attempt had been made to collect and disseminate information for combat operations in the Caribbean, the effort was largely a failure. The author of a classic study of American intelligence commented: "Whether the primary fault stemmed from a lack of suitable dissemination procedures or an inability on the part of the individual field commanders themselves to utilize the information properly still remains a moot question."[3]

Because the United States had not fought a foreign war since 1848, and had not conducted war on a large-scale at all since 1865, its military had been able to get along with an inefficient organization. The Army was small, parochial, and structured for border or coastal defense and for suppressing Native Americans. As a result of the Spanish-American War, however, the U.S. had acquired foreign colonial possessions—the Philippines, Guam, Puerto Rico—with the need to defend them; this meant ineffective military organization could no longer be tolerated.



Spanish armored cruiser *Cristobal Colon* photographed in 1897-98. This ship's two ten-inch main battery guns had still not been installed when she was lost in the Battle of Santiago, Cuba, July 3, 1898. (U.S. Navy)

The Origins of Modern Military Intelligence

In 1903, following presidential-level studies generated by the perceptions of poor performance in the war against Spain, Congress approved a general staff for the Army, replacing the commanding general with a chief of staff as the senior soldier in the service. However, this reform did not create planning or intelligence functions, and, as it turned out, the general staff spent much of its time on administrative matters that should have been settled at lower levels.

About the same time, however, the Army created the War College to develop military education, disseminate military data, and coordinate military administration. Despite its name, military education was only one function of the War College, and not the principal one at that. The College was given responsibility for undertaking a number of planning functions on behalf of the General Staff.

Although these reforms represented progress, effective military reorganization and strengthening of the general staff did not occur until the eve of World War I. Real reform was prompted only by a second failure and a serious threat: shortcomings revealed in mobilizations along the Mexican border and with the threat of involvement in the Great War in Europe.

The U.S. Army had little use for military intelligence as a discipline. Although the Military Information Division (MID), subordinate to the Adjutant General's Office, had been founded in 1885, it was small, passive in character, and usually shunned by career-minded officers. If thought of at all by officers, intelligence likely meant scouting or reports sent from overseas by the newly created group of military attachés.

Most data came from open sources. In one example, when asked by a newly assigned commander in the Philippines for information on the islands to support military operations, MID forwarded an article copied from *Encyclopedia Britannica.*

Since the War College was only secondarily an educational institution, and had diverse responsibilities for military planning and staff functions, it made sense to assign the Military Information Division to it. Secrecy was not part of its initial fabric. In 1907 the War College president asked the chief of staff to subordinate MI to the College so that faculty and students could have access to its files.

The Army chief of staff, General Franklin Bell, who disliked the idea of military intelligence on principle, designated the War College as G-2; he divided it into the War College Section and Military Information Section.

For most of the next decade, Army intelligence activities were carried on as the MI Branch of the War College. Its correspondence was headed "War College Division." Despite ostensible intelligence functions, it shared responsibility for such general staff activities as planning, monitoring militia affairs, history, and legislative affairs. In fact, a statement by its chief in 1915 indicated that "current General Staff work" was its primary focus.

In 1915 Major Ralph Van Deman was transferred to the general staff. As Captain Van Deman, he had been assigned to the mapping section of MID before the 1898 war, and subsequently had created a tactical military intelligence organization to support combat operations in the Philippines. He gained a reputation as effective in running intelligence operations.

Although assigned to administrative duties, Van Deman retained an interest in intelligence, and in 1916 petitioned Chief of Staff Hugh Scott to create a permanent Army intelligence organization along European lines. Scott turned down the proposal, but somehow word of it was leaked to the Army's civilian leadership. In early May 1917, Secretary of War Newton Baker issued an order creating the Military Intelligence Division; its chief was Lieutenant Colonel Ralph Van Deman.

It should be noted that in these early days U.S. military personnel referred to "military information." However, the word "intelligence" increasingly replaced the phrase as the U.S. came under British influence in World War I.

Modern American Cryptanalysis

Before the twentieth century the U.S. military had engaged in cryptanalysis as a sustained activity only in times of conflict, notably the American Civil War. In the latter half of the nineteenth century, the army had not trained personnel in the skill nor engaged in intercepting foreign communications. There were no organizations established to do cryptanalysis anywhere in the government.

Until after World War I, when William Friedman coined the term "cryptanalysis," the process of solving an encrypted message was called "translation." (This article will simply use "cryptanalysis" to avoid confusion.)

Because the medium of wireless radio was so new, one major activity for U.S. Army signal units was research into radio technology. As the same types of radios were used both for the military's own communications and for intercept, the Signal Corps required detailed reports about both functions from all radio units on the component equipment used, how and where it was placed, and the results. Since radio was strictly an official business in most countries, there was no central listing of stations, so Army signalers also had to compile reference logs of broadcasting stations.

There were no professional cryptanalysts in the military. In fact, those who engaged in it, either from within the military or civilian volunteers, were autodidacts. They also lagged well behind European military officers in their understanding of cryptologic developments.

In the beginning, some cryptanalysis was done by Colonel Parker Hitt, and some was farmed out. Genevieve Hitt, fascinated by her husband's study of codes, learned cryptanalysis also, and solved some messages for the Army.

Colonel Parker Hitt at Fort Leavenworth. From privately owned collection of Parker Hitt's papers; use is courtesy of David and Evie Moreman and Kevin and Jennifer Mustain

A Shark on Ciphers

Parker Hitt had been born in Indianapolis on August 27, 1878. He studied civil engineering at Purdue University. As the crisis with Spain grew, he enlisted in the Army and served as an enlisted man from July 1898 to May 1899; he was commissioned on September 1, 1899.

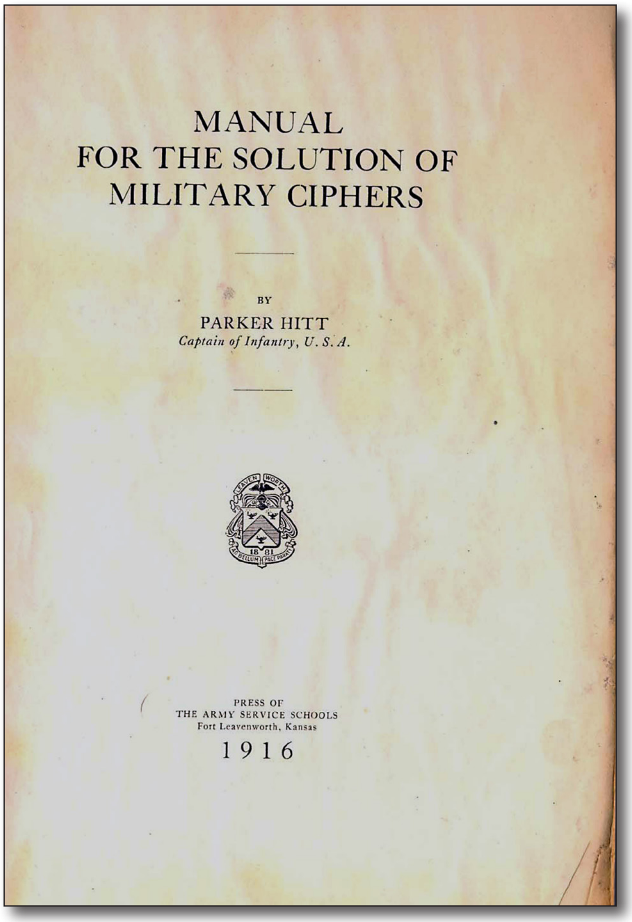
As an officer he served several tours in the Philippines between 1900 and 1906. During that time he was peripherally involved in the acquisition of an encrypted message that allowed the U.S. military to pinpoint the headquarters of Emiliano Aguinaldo, leader of the Philippine resistance. He later wrote an article on this incident, but it is unclear what impression the action made on him at the time. Given his later interest in cryptology, one can speculate that this incident taught Hitt the importance of cryptanalysis.

As a weapons officer in the infantry, he was assigned to Fort Sill, Oklahoma, after his return from the Philippines. While there, in 1910, he was inspired by a conference on communications, and realized the military would require greater expertise in cryptology, both in creating systems and solving them, than it had.

He applied for and received a temporary assignment to the Army Service Schools in Fort Leavenworth, Kansas, in 1911. In the Signal Corps School, he saw the need for and got approval to compose a manual on cryptology for the Army. He had some ability to read French and Spanish, which would abet his work on the manual. From 1915 he served as chief instructor in the Army Signal School and from time to time as acting director of the school.[4]

Lieutenant Colonel Samuel Rebar, acting chief of the U.S. Army Signal Corps, sent Hitt some Mexican messages that the Army had acquired; the messages were sent to New York from Pancho Villa's agent in Ciudad Juarez. One of them had been sent a few days after Villa seized Juarez and captured a number of officials. Rebar said he was sending them because he knew Hitt was a "shark" on ciphers.[5]

In preparing his manual on cryptologic work, Hitt took European texts as one model for his opus. In January 1915 Hitt, in a letter, noted familiarity with a Belgian text on cryptology entitled *Etude sur la Cryptographie*, which appeared in *Revue de L'Armee Belge*; the War College Library had a copy. Hitt told



MANUAL
FOR THE SOLUTION OF
MILITARY CIPHERS

BY
PARKER HITT
Captain of Infantry, U. S. A.

PRESS OF
THE ARMY SERVICE SCHOOLS
Fort Leavenworth, Kansas
1916

Parker Hitt's Army manual title page with seal of the Fort Leavenworth, Kansas, Army Service Schools

Rebar that he hoped to finish the pamphlet before he departed the signal school.[6]

In mid-February 1915, with a month left on his temporary assignment to the Army Signal Corps at Fort Leavenworth, Kansas, Hitt asked the director of the Army Signal School to forward to him copies of any enciphered messages in his possession. Hitt explained that he was preparing a pamphlet on ciphers in English and Spanish, and believed the Army Signal School had a number of enciphered Mexican messages that had passed through the Vera Cruz cable office. Hitt noted that he was not interested in the content of the messages, but merely wanted to have examples of different types of ciphers and show how they could be solved.[7]

The director of the Army Signal School (Wildman) endorsed this request in a memo to the Chief Signal Officer of the Army. Wildman called Hitt the "best cipher expert" in the Army, with "the possible exception of Lt. Maubourgne," and advised taking advantage of Hitt's knowledge, particularly so the Army Signal School could lay a foundation for future cipher experts that might be needed in time of war.[8]

The acting commander of the Signal Corps endorsed Hitt's request and asked that the adjutant general of the Army send the material on, "under such seal of secrecy as may be desired."[9] The adjutant general replied that the Mexican ciphers requested by Captain Hitt were not in the records of the General staff.[10]

The War College Division acknowledged the request for copies of Mexican secret codes, but also said it did not possess any. However, officials believed such materials were held by the Secret Service and the Department of Justice, so the War College Division sent them a memorandum asking for copies.[11]

Eventually, Hitt did receive ciphers from Lieutenant Colonel Reber in Washington. He found, however, that these same cipher messages were also held by the Second Division.[12]

Hitt's work, not only in cryptanalysis but also in cryptography, was acknowledged in practice. An aide to the chief of the Signal Corps wrote Hitt in August 1915: "I am directed by the Chief Signal Officer of the Army to acknowledge with thanks a cipher system for use in the preamble, address, and signature in military radio messages devised by you. This system has been tested with good results by Field Company A, Signal Corps, and the card and instructions covering it are in course of preparation for issue to the Signal Corps at large."[13]

As intercepts became a larger part of the national intelligence effort, the MID in Washington made increasing use of Parker Hitt's skills. For example, on April 21, 1917, Van Deman sent an encrypted message to Hitt, and asked to have the "translation" as soon as practicable. Hitt sent the translation on the 26th. The Mexican message referred to a radio operating near the Arizona border.[14]

Hitt received encrypted messages from many disparate sources. A Signal Corps officer from Kentucky, who had collected a message while deployed along the Mexican border, sent it to Hitt from home. Hitt returned it with the explanation that it was too short to solve at that time, but he would keep it on file against the time when it might be decipherable.[15]

Units deployed along the border often sent intercepts directly to Hitt. In 1916 and 1917, officers in the 19th Infantry and 12th Cavalry did so. In one case a captain in the 12th reported that a solution based on Hitt's principles, presumably from the manual Hitt had authored, had already been tried, but without success. The captain promised Hitt the credit would be his should it be solved.[16]

The subjects contained in the intercepted messages are no longer known, but were not necessarily military: For example, Hitt sent a solution of two out of three messages believed to be in a new cipher used by the Mexican consulate system. In another instance, the encrypted text sent to Hitt was from the Mexican ambassador in Washington to the Mexican consulate in Nogales, Arizona.[17]

Details are now sketchy, but Hitt's wife, Genevieve, also developed an interest in and an expertise in cryptanalysis—and intercepts were sent directly to her for solution. The amount of work she did is unknown, but four examples have survived. In August 1917 an intercepted radiogram sent from San Francisco to Santa Rosalia was forwarded to Mrs. Parker Hitt.[18] An encrypted message was sent from Sergeant Clark, operator in charge, Brownsville, to Mrs. Parker Hitt, Fort Sam Houston, in September 1917.[19] A corporal at Fort Brown sent an encrypted telegram to Mrs. Parker Hitt at Fort Sam Houston in October.[20] In the last extant example, in September 1918 the departmental engineer of the Army's Southern Department forwarded a transposition cipher to Mrs. G. Y. Hitt.[21]

Early in his endeavors, Hitt had expressed surprise to LTC Rebar that Mexican agents used quite simple ciphers, particularly transposition ciphers.[22] He may not have felt the same after several years' experience working on Mexican encrypted messages.

In March 1917, about two years after, Hitt informed Rebar that he and Mrs. Hitt had "done a fair amount of work on [a particular message] and we think we begin to see the system behind it," but it had not been solved. The problem was, cryptanalysis was not his regular duty. Hitt said he was "fairly swamped" with cipher work, but it was done in addition to his regular duty as company commander and instructor in the Army's weaponry school. He said that cipher work required a person's full attention, but he was teaching machine guns to a class of 150 noncommissioned officers from the Army at large, using intensive methods, "which have little consideration for the instructed and none whatever for the instructors."[23]

Later, Hitt served as chief signal officer for the First Army in the AEF; his commanding officer, BG Hugh Drum, recommended him for promotion in his efficiency report.[24] However, Hitt never achieved general officer rank. He was recalled to duty in World War II, but did not work again in the field of communication or cryptology.

The Creation of a Professional Organization

Up through at least mid-1917, still lacking professional cryptanalysts in government employ, Military Intelligence in Washington served as a hub, or a clearinghouse, for encrypted messages. Encrypted intercept was sent by Van Deman—or on his behalf—to a stable of part-time cryptanalysts for solution. This included both Mexican and German encrypted cables. The U.S. was worried that the Germans were using Mexico as a base for espionage or sabatoge.

Military intelligence made arrangements with Riverbank Laboratories, a private think tank near Chicago that had a cryptologic section, to perform cryptanalysis on selected messages. Messages also were worked by a talented amateur, Dr. John Manly, head of the English Department at the University of Chicago.

Van Deman tried to achieve better cooperation within his network of cryptanalytic talent. In May he relayed to Hitt an invitation from Fabyan to visit Riverbank Laboratories. Hitt replied that he could not accept due to the pressure of teaching at the Fort Sill School of Musketry in addition to after-hours cryptologic work.[25]

In early April 1917, Van Deman sent duplicate copies of a German encrypted message to Manly in Chicago and Hitt in Kansas. He said that these were of interest to the Department of Justice. He advised them to keep the messages confidential and under lock and key when not being studied.[26]

Van Deman forwarded information about a German message that had been obtained in San Francisco to Manly in Chicago. He noted that the message also was being worked by Mauborgne at Fort Leavenworth and Parker Hitt at Fort Sill. Manly was given permission to contact either of them about the message. Probably unaware of the considerable interaction between the two, Van Deman also referred Manly to a fellow Chicagoan, George Fabyan, at 160 West Jackson Block, who "seems to know a good deal about cipher work."[27]

In May the State Department gave Van Deman copies of messages that had passed between the Austrian Consul General in New York and the Austrian Minister in Mexico City. Van Deman sent duplicate copies to Hitt, Fabyan, and Mauborgne, with the thought that the messages were in code rather than cipher.[28]

Van Deman also asked to have Hitt detailed to the General Staff in Washington to work in the Military Intelligence Section.[29] However, Hitt was never released from his duties teaching weaponry.

As the Army prepared to deploy troops overseas for the great war in Europe, Riverbank Laboratories endeavored to train selected members of the Army Signal Corps in compiling cryptosystems for its own use, and solving those of others. The training was conducted by two Riverbank employees, William and Elizebeth Friedman. William was shortly to accept a commission and leave for France to support the American Expeditionary Force with his cryptanalytic skills.

As late as August 1917, MI forwarded an encrypted telegram—intercepted at Nogales—to Fabyan in Chicago. Fabyan was asked to furnish a copy of the deciphered message, with the key and keyword, if any. Presumably, Fabyan further delegated the task to the Friedmans at Riverbank.[30]

Dr. Manly also accepted a commission and worked in MI-8 for the duration of the war.

These arrangements continued until June 1917, when a smooth-talking code clerk from the State Department with a flair for cryptanalysis met with Van Deman and convinced him Military Intelligence needed its own organic cryptanalytic service. After further discussions, Van Deman agreed, and arranged a direct commission for the code clerk.

Herbert O. Yardley began his service a month later. Although he had a number of distractions before he began assembling a staff and working messages, increasingly MI began to perform cryptanalysis in-house.[31] The designation MI-8 for this organization became official in December 1917.

This series of steps put Yardley in charge of MI-8, the nation's first modern, sustained military cryptanalytic organization.

It is hard not to view American military intelligence in this period as a child taking its first steps.

The first efforts were shaky, but gradually the child built up strength and confidence to walk on its own. Running had to wait until World War II.

In more realistic terms, U.S. military intelligence emerged from its haphazard existence as it responded to perceived needs. The leadership did the best it could to acquire expertise, and, eventually, a modern organization with committed personnel began to develop.

Author's Note: This is one chapter from an in-progress monograph, *The Dawn of American Cryptology*.

It is hard not to view American military intelligence in this period as a child taking its first steps. … Running had to wait until World War II.

Notes

1. G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly Press, 1991), 177-81.
2. O'Toole, *Honorable Treachery*.
3. Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941* (Frederick, MD: University Publications of America, 1986).
4. Major Leonard D. Wildman, Director Army Signal School, Signal Corps, letter June 18, 1915. David Kahn Collection. Library of the National Cryptologic Museum, Fort Meade, MD.
5. Samuel Rebar, office of the chief signal officer, Washington, confidential letter to Captain Parker Hitt, Fort Leavenworth, January 4, 1915. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."
6. Colonel Samuel Rebar, office of the chief signal officer, Washington, confidential letter to Captain Parker Hitt, Army Signal School, Fort Leavenworth, January 13, 1915. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican." Captain Parker Hitt, Signal Corps, letter to Colonel Samuel Rebar, office of the Chief Signal Officer, Washington, January 15, 1915. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."
7. Parker Hitt, Captain, Army Signal Corps, letter to Director, Army Signal School, "Mexican ciphers," February 19, 1915. David Kahn Collection, National Cryptologic Museum Library; folder: "Manual for Solution of Military Ciphers."
8. Ibid.
9. Samuel Reber, Lieutenant Colonel, acting commandant, Signal Corps, memorandum to Adjutant General, U.S. Army, March 3, 1915. David Kahn Collection, National Cryptologic Museum Library; folder: "Manual for Solution of Military Ciphers."
10. Adjutant General of the U.S. Army, memorandum to the Director, Army Signal School, March 10, 1915. David Kahn Collection, National Cryptologic Museum Library; folder: "Manual for Solution of Military Ciphers."
11. M. M. Macomb, Brigadier General, Chief of War College Division, office of the Chief of Staff, memorandum for the Chief of Staff, subject: "Mexican secret code books," May 16, 1916.
12. Parker Hitt, letter to LTC Samuel Reber, March 16, 1915; David Kahn Collection, National Cryptologic Museum Library; folder: "Manual for Solution of Military Ciphers."
13. 1st Lieutenant John N. Greely, letter to Captain Hitt, August 19, 1915. David Kahn Collection, Library of the National Cryptologic Museum, Fort Meade, MD.

14. Officer in Charge of Military Intelligence, letter to Captain Parker Hitt, 19th Infantry, Ft. Sill, Oklahoma, "Cipher or Code Message," April 21, 1917. Typed response from Hitt on letter, and enclosure. RG 165, Box 2952.

15. Captain Parker Hitt, letter to Captain Otto Holstein, signal officer, Kentucky National Guard, March 25, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."

16. Captain Parker Hitt, 19th infantry, Fort Sill, message to department intelligence officer, southern department, April 23, 1917. David Kahn collection, National Cryptologic Museum; folder: "official cryptanalysis–Mexican area." Fugua (NFI), Camp Stephen Little, Nogales, Arizona, message to Captain Parker Hitt, 19th Infantry, Del Rio Texas, July 1916. David Kahn collection, National Cryptologic Museum Library; folder: "official correspondence–Mexican."

17. Captain, 12th Cavalry, Columbus, New Mexico, to Captain Parker Hitt, 19th Infantry, Fort Sill, March 21, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican." Captain Parker Hitt, 19th Infantry, Fort Sill, message to commanding officer, Fort Sill, November 9, 1916. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."

18. Intelligence officer, 35th Infantry, Nogales, Arizona, memorandum to department intelligence officer, Fort Sam Houston, "Mexican cipher," August 31, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."

19. Sergeant Clark, operator in charge, radio station, Brownsville, Texas, message to Mrs. Parker Hitt, Fort Sam Houston, September 12, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official correspondence–Mexican."

20. Corporal Vale, Fort Brown, Texas, radio station, message to Mrs. Parker Hitt, Fort Sam Houston, October 2, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official correspondence–Mexican."

21. Colonel W. P. Skokey, office of department engineer, headquarters southern department, letter to Mrs. G. Why. Hit [*sic*], c/o department intelligence office, Fort Sam Houston, September 4, 1918. David Kahn collection, National Cryptologic Museum Library; folder: "official cryptanalysis–Mexican."

22. Captain Parker Hitt, Signal Corps, letter to Colonel Samuel Rebar, January 9, 1915. David Kahn collection, National Cryptologic Museum Library; folder: "official correspondence–Mexican."

23. Captain Parker Hitt, Fort Sill, letter to Colonel Samuel Weber, Signal Corps, Chicago, Illinois, March 25, 1917. David Kahn collection, National Cryptologic Museum Library; folder: "official correspondence–Mexican."

24. Efficiency Report for Colonel Parker Hitt, Signal Corps, September 30, 1918. David Kahn Collection, Library of the National Cryptologic Museum, Fort Meade, MD.

25. Parker Hitt, letter to Colonel George Fabyan, May 16, 1917; David Kahn collection, National Cryptologic Museum Library; folder: "Correspondence–Friedman and Official War Department."

26. Major R. H. Van Deman, letter to John Manly, April 5, 1917. Brigadier General Joseph E. Kuhn, letter to commandant, Army service schools, Fort Leavenworth, Kansas, "cipher messages," April 5, 1917. RG 165, box 9140. Handwritten letter, John M. Manly, University of Chicago, Department of English, to Major R. H. Van Deman, War Department, April 9, 1917. RG 265, Box 2952.

27. Major R. H. Van Deman, Officer in Charge of Military Intelligence, letter to Professor John M. Manly, 1312 East 53d Street, Chicago, Illinois, April 12, 1917. RG 165, Box 2952.

28. Major R. H. Van Deman, Chief, Military Intelligence Section, messages to Hitt, Fabyan, and Mauborgne, "Cipher Messages," May 15, 1917. RG 165, Box 2952. Major R. H. Van Deman, Chief, Military Intelligence Section, letter to Leland Harrison, office of the Counselor, Department of State, May 15, 1917. RG 165, box 2952.

29. Major Ralph Van Deman, letter to Captain Parker Hitt, 19th Infantry, Fort Sill, May 12, 1917; David Kahn Collection, National Cryptologic Museum

Library' folder: "Correspondence–Friedman and Official War Department."

30. Lt. Col. R. H. Van Deman, Chief, military intelligence section, letter to Col. George Fabyan, August 11, 1917. RG 165, box 2394.
31. David Kahn, *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking* (New Haven: Yale University Press, 2004), 20-21.

General Sources

Official correspondence between and among Colonel Ralph Van Deman, Colonel Parker Hitt, Colonel Marlborough Churchill, Colonel J. O. Mauborgne, officers of the Southern Department headquarters in San Antonio, Texas, and officers in charge of Radio Tractor Units.

The June 30, 1916, and May 1, 1917, reports of General John J. Pershing to his superiors, and February 6, 1917, final report of the Punitive Expedition's Signal Officer.

Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941* (Frederick, MD: University Publications of America, 1986).

John Patrick Finnegan, *Military Intelligence* (Washington, DC: Center of Military Studies, Army Lineage Series, 1998).

David Kahn, *The Codebreakers* (New York: Macmillan, 1967).

Donald J. Mabry, "Cast of Characters: Birth of the US War Department General Staff, 1898-1916," *Lafayette, We Are Here: The War College Division and American Military Planning for the AEF in World War I* (Historical Text Archive, 2005, historicaltextarchive.com).

Nathan Miller, *Spying for America: The Hidden History of U.S. Intelligence* (New York: Marlow and Company, 1997).

G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* (New York: Atlantic Monthly Press, 1991).

NSA's Senior Technical Development Program Turns Twenty

Nancy Welker and Cathleen L. Civiello

Introduction

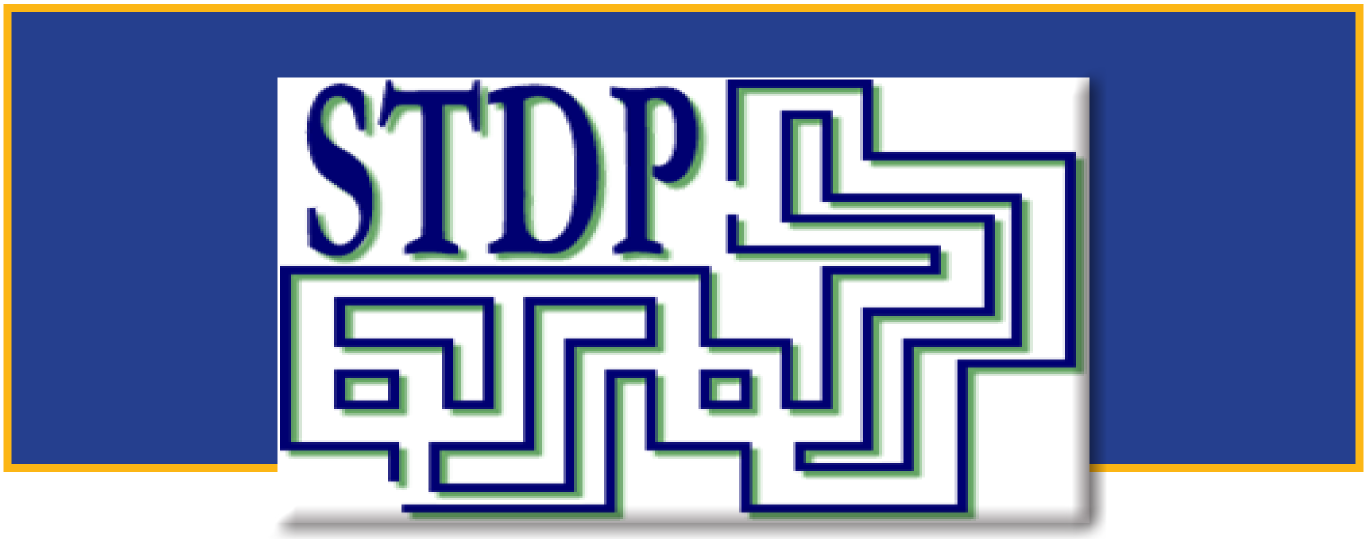
NSA's Senior Technical Development Program (STDP) has proven to be a critical initiative that has unquestionably permitted NSA to maintain parity between its major technical capabilities and evolving mission challenges that dominate its national and tactical cryptologic efforts. Most of the STDP features discussed in this paper have been practiced since the inception of the program and have stood the test of time. Some have been challenged (e.g., the interview process) but have continued, largely because the STDP participants have staunchly supported its structure. The reader may be puzzled that it has proven impossible to *formally* train technical leaders; I submit that is precisely the reason the STDP was created—the program pulls out of its participants, leadership skills that often lie dormant in practice. But the real test of value of this program has been repopulation of the senior technical workforce with world-class experts and leaders in meeting the cryptologic challenges of the nation. This is a challenge without end.

—George R. Cotter, founding Senior Technical Review Panel (STRP) Chair. He was a senior at NSA from 1966 to 2009 and founded the STDP.

No clear definitions of technical leadership are available in either the psychological or leadership literature. Much has been written about assessing and developing managerial and executive leadership skills, but very little has been written about the skills of technical leaders.

Despite a failure to focus on technical leaders, much of what has been written is relevant. A special issue of *The Psychologist-Manager Journal* was dedicated to Douglas Bray, PhD, who in 1956 was asked by AT&T to longitudinally assess the development of managers throughout their careers, specifically focusing on managerial competence. Dr. Bray, along with his wife, Dr. Ann Howard, not only assessed managerial leadership but also laid the groundwork for the science of assessment centers (Rupp, 2006). The impact of such assessment centers has provided much of our understanding of managerial leadership (Howard and Bray, 1988). Such centers, however, were also relevant for assessing technical leaders, to include military officers (Siegfried, 2006). This influence is especially relevant because the very few articles that have been written about technical leadership have primar-

This article is adapted from an article originally published in *The Psychologist-Manager Journal* (Civiello and Welker, 2009).



ily focused on military settings (e.g., Drysdale, 1968; Helme, Willemin, and Grafton, 1975; Hunt, Dodge, and Wong, 1999), although a few have discussed leadership in technical settings and touched on aspects of technical leadership (e.g., Abbey and Dickson, 1983; Birnbrauer and Tyson, 1984; Bowers, Salas, and Jentsh, 2006; Dutta, 2001; Jaques, 2001; Kendra and Taplin, 2004; Mael, Waldman, and Mulqueen, 2001; Robben, 1998). With the increasing pace of business (Hewlett and Luce, 2006) and the pace of technological evolution changing the way individuals in most settings work (Civiello, 1999), technical leadership is no longer relevant just for the military and technology-focused workplaces.

Many authors, too numerous to mention, have informed the well-established field of managerial leadership assessment and development. Several, like Howard and Bray (1988), though, are relevant to technical leadership. These authors include, but are not limited to, Blanchard and Johnson, 1981; Levinson, 1982 (especially the chapter "What the Executive Doesn't See," pp. 74-96); Rath, 2006; Sayles, 1989; Sternberg, 2007; and Wagner and Harter, 2006. In addition, a few authors are beginning to explore wisdom and value-based leadership in executives (e.g., Kilburg, 2006; Kilburg, 2012; Thompson, 2006; Thompson, Grahek, Phillips, and Fay, 2008; and Zaccaro, 2001). Some of their findings are especially relevant to technical leadership. Finally, Hackman and Wageman (2007) in their article for a special issue of *The American Psychologist* discussed the importance of shared leadership. Although they focused on the relationship between leaders and followers, this concept is just as important when addressing the relationship between technical and managerial leaders.

The easiest way to define technical leadership is by describing the context in which technical leaders work. Arthur Freedman (1995) noted the need for organizations to function differently in crises than they do in normal conditions. His article focused on how the behavior of leaders and psychological consultants needs to change when conditions in an organization are not stable or, more relevant for this discussion, when the environmental conditions in which an organization operates are not stable. Freedman describes how technical experts can be critical to the effectiveness of an organization functioning in crises. Specifically, at such times it is critical that specialized technical experts work with consultants (or managerial leaders in the NSA context) to assist with the actual content of the work. The technical leader's proficiency in quickly dealing with complex work patterns enhances the effectiveness of the consultant or managers. Freedman stated that effective experts "push, prod, cajole, and coax unit leaders and members to decide and act" (p. 218). This description, and the reality at NSA, is similar to a description of ideal leadership by Randy Pausch (2008), a Carnegie Mellon professor of computer science and human-computer interaction, in his moving book *The Last Lecture* that captured the messages he wanted to leave for his children. He described how he, like many of his generation, wanted to grow up to be *Star Trek* character Captain James T. Kirk. He stated that one of the attractions of Captain Kirk's leadership style was the interplay between Kirk and the rest of his staff—the technical experts. Like the technical experts described by Freedman, *Star Trek* staff described by Pausch provided the technical information (e.g., medical, engineering) that prodded Captain Kirk to act, but it was Kirk, the managerial leader, who made the final managerial decisions.

This technical-managerial interplay is especially important in our current turbulent times. For example, Freedman drew a parallel between the organizational challenges discussed in his above-described article (Freedman, 1995) and the post-9/11 mission challenges faced by organizations in the U.S. intelligence community (A. M. Freedman, personal communication, October 4, 2008). These organizational challenges drive NSA's managerial and leadership development approaches and initiatives.

Career Paths at NSA

We are an agency with missions that, by their very nature, depend on technology. Technology, especially its pace of change, drives all we do. As a result, our technical personnel are critical to our success. We have twenty-three different skill communities or clusters of professions. Most of these are highly technical, like math, physics, engineering, computer science, language analysis, and intelligence analysis. In addition to the professions that are key to performing our cryptologic missions, we also have communities of professions that are necessary to run any large organization, such as legal, occupational health, and human resources.

About twenty-five years ago, as the pace of technological development began to speed up, NSA found itself losing its technical edge. As in many organizations, for NSA at the time, the career path for our very best and brightest typically involved a move of hands-on technical personnel into managerial roles for which they may or may not have been a good fit. Even worse, those moves left us with a vacuum of technical expertise at the highest levels. Because of the nature of NSA's missions, we cannot directly hire personnel with many of our critical technical skills. For example, if we hire a world-class mathematician (and we regularly do), significant additional training is needed before that mathematician becomes a world-class codemaker or codebreaker. To retain and continue to develop personnel with critical technical skills, we needed a true technical career path for technical leaders as well as a method for technical and managerial leaders to collaborate in mission leadership.

Structure

We created a dual-path career structure (see Figure 1) in which both paths can lead to the senior ranks, although we do have technical leaders at levels throughout the structure. Defense Intelligence Senior Leaders (DISLs) are our senior technical leaders. Those in the Defense Intelligence Senior Executive Service (DISES) are our senior managers. To encourage collaboration between the two types of senior leaders such as that recommended by Freedman (discussed above), we added the responsibility to collaborate to the behavioral anchors for evaluating pay for performance for senior technical and managerial leaders.

Because our mission is so technical, movement back and forth between the paths often occurs; but, because of the complexity of the technical skills, it is far more common to move from the technical path to the managerial path at the highest level. At the lower levels there is movement in both directions.

Technical Positions

Individuals on the technical path hold two general types of positions: technical director and technical expert or subject matter expert. Both types can be most easily understood by thinking of them as embedded consultants in the organization.

Technical director positions. A technical director provides technical guidance for an organization. When she or he consults outside the organization, the consultation is typically related to the mission of the organization for which she or he is technical director.

Technical expert positions. A technical expert is truly a subject matter expert, and we want him or her to stay that way.

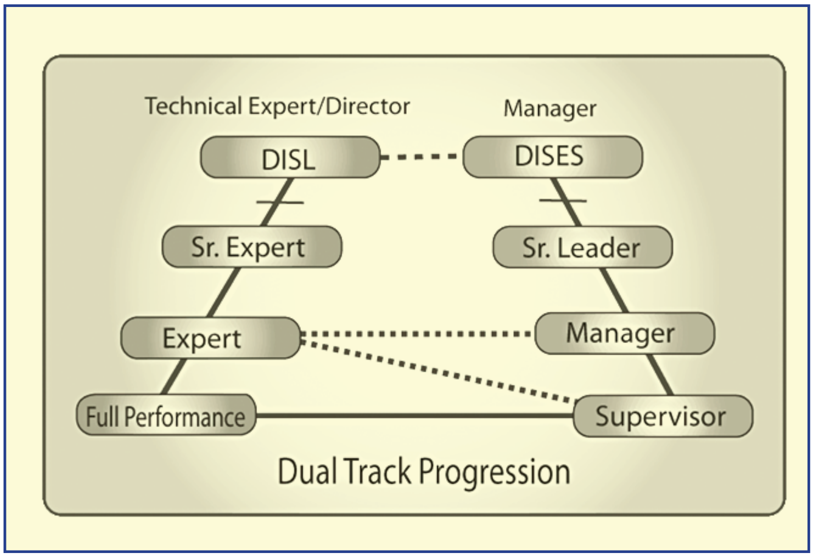


Fig. 1. NSA's dual-path career structure

Performance Expectations

Despite the differences in the positions, NSA has the same performance expectations for technical experts that it has for technical directors. These are the following:

Technical/professional achievements are the core of what we expect of leaders in both types of positions and involve the direct application of technical skills. For example, a psychologist DISL may apply psychology to professional and leadership development activities.

Technical development of others requires the leaders to transfer their knowledge and to develop the next generation of technical personnel and leaders.

Technical leadership and decision-making is the area where embedded consultation skills are the most critical. Technical leaders need to actively identify where they can provide mission value. They often need to proactively help the managers use their technical expertise, a difficult task for a workforce like NSA's whose professions tend to attract introverted individuals. Add to that an environment in which keeping secrets is critical to success as well as a legal requirement, and the personnel who are attracted to this environment tend to be even more introverted than their colleagues in similar professions who work in other settings. This proactive help is a special challenge in technical leadership development.

Continued development or enhancement of technical skills is actually specified as a performance expectation. Because of the fast pace of change in technology, keeping up one's technical skills is a critical job requirement.

Senior Technical Development Program

Each of the twenty-three skill communities has a set of career paths specific to the technical development for the professions associated with that community; defined technical career paths date to the mid-1980s. The greater challenge, though, is associated with developing our most senior technical personnel and, especially, technical leaders. NSA has long had development programs for managerial leaders but nothing for the highest-level technical leaders.

So in 1990, NSA decided to do something about that. The Agency had a Senior Technical

Review Panel (STRP) responsible for overseeing overall technical health and especially for assuring that the Agency's technical seniors were in appropriate positions. The STRP initiated a study of the technical workforce and associated career paths. The panel found, among other things, that a program focused on the more senior technical personnel was needed (Cotter, 1991). To address that need, in 1993 the Senior Technical Development Program (STDP) was launched, and the first class was selected in 1994. The goal of the program is to further develop NSA's technical leaders in their specialized disciplines and to enhance their knowledge, experience, and ability to respond to NSA's technical challenges of the future.

The program in place for developing senior managerial leaders did not serve as a good model because the path and skills were similar for all participants. The technical program/STDP needs to be highly specialized because NSA needs highly specialized technical experts and leaders. Basically, the Agency needs to take personnel already expert in their fields and make them experts' experts. To do this the STDP intensifies and accelerates the development of the already recognized expert, focusing on his or her narrow area of expertise. The program also broadens exposure to major technical changes, NSA issues, and leadership development through deep immersion. The focus is on fields that are not merely relevant to NSA today but also technically critical to our future.

Program Basics

Ten seniors collectively manage the STRP. The areas of expertise of the panel members span a broad range of NSA skill communities. Nine of these seniors are DISLs (technical), and the chair is a DISES (managerial leader). Even though the chair is a managerial leader, both the current and past chairs have deep technical backgrounds. The current chair, the first author, is the former NSA director of research, and she has also held the position of chief technical officer. The prior (and initial) chair was the NSA chief scientist.

Significant senior time and energy are devoted to each participant because we expect that our participants will technically lead the Agency in the future. Each participant has three seniors who devote considerable time to him or her: a DISL mentor, a DISES mentor, and an STRP member who is the participant's dedicated program monitor and liaison to the STRP.

Because each program is different and specialized for each participant, much collaboration occurs between the mentors and the participant in developing each individual program. The DISL mentor provides the bulk of the technical guidance, but all twelve of the seniors involved are on the lookout for opportunities for the participant.

The primary job of the DISES mentor is to open doors. For example, if a participant needs a developmental tour at another agency, the DISES may call a colleague and facilitate an introduction. At this level, and especially in the intelligence community, the introduction is key to assuring that a participant can be accepted in an organization and will be given meaningful development opportunities. The introduction establishes the bona fides of the participant. The DISES also uses the introduction to provide an explanation of the value of the program for both the recipient and the organization in which the participant will be working.

The length of individuals' programs can range from one to three years, but most programs require three years due to the depth and breadth of learning expected.

One of the most difficult aspects of any adult learning or professional development program is assuring that the learning is both relevant and then applied and adds value to the job. Application and relevance are especially important for the STDP because of the half-life of much technical knowledge. If our participants waited three years to apply the learning, it would be outdated. In addition, the participants would lose track of mission changes during that time.

To assure relevance and an immediate return on investment, the participants remain assigned to their parent organizations and are expected to contribute to their organizations' technical mission while in the program. Our participants must spend at least fifty-one percent of their time on STDP activities. For most, eighty percent is ideal because it gives them sufficient immersion in developmental activities to foster good learning while still allowing one day a week back on mission—applying the learning and sharing it with other mission personnel.

The program broadens exposure to major technical changes, NSA issues, and leadership development through deep immersion.

Eligibility

So, who are our participants? Each year the STRP asks major organizations (e.g., Mission Resource Authorities or MRAs) within the Agency to appoint a point of contact to coordinate applications and provide guidance regarding areas of technical skill that are important for our future.

A call for applications then goes out to personnel in the relevant grades; and the STDP program manager, with help from the STRP, provides educational briefs about the program throughout NSA. Anyone is welcome to attend the briefs. Aspirants as well as managers of potential candidates and personnel far too junior to apply who are doing long-term career planning typically attend.

Those who are currently DISLs and those at grade 15 may self-nominate for the program with their organization's acknowledgment. MRAs and other major organizations can nominate high-potential personnel in grades 13 or 14. DISLs, even though they are already in senior technical positions, can apply if they need to deepen or refresh their technical expertise. Most participants are in grades 14 and 15.

Skill Mix

As mentioned above, the major organizations provide the STRP with guidance and direction about the skills they view as important to the future. The STRP uses that information and its own broad technical expertise to inform the desired skill mix in the program. Due to the nature of advances in science and technology, though, there are times when NSA mid-level or early career employees have additional insight about critical emerging areas that are relevant for NSA's future. As a result, although the STRP provides some broad guidelines regarding desired areas of applications, technical experts in all professions may apply. Often an expert in an unanticipated specialty applies and, during the extensive application and selection process, she or he successfully convinces the STRP that this area of expertise is critical to NSA's future.

The application process involves paperwork that summarizes current expertise, the manner in which the individual develops others, and a proposal for development. The proposal needs to include a balance of education, training, tours, and self-study. We ask that the application focus on and address:

- Core competencies and how they can be developed
- What characterizes expert status in the field and specialty
- The relevant centers of excellence
- The relevant leaders in the field

The application paperwork also requires an endorsement from the individual's supervisor and from a current DISL. For those who are in grades 13 or 14, a nomination statement from the individual's MRA is also required. The board reviews the paperwork and selects individuals to interview. Based on the candidate's area of expertise, a three-person subset of the STRP is selected to interview each aspirant. A semistructured interview is used. This interview protocol was developed using the expertise of the panel members and with consultation from a graduate of the program who is an industrial/organizational psychologist. The three members who interviewed the individual then discuss the interview with the entire STRP, and the decision is made by the entire board. The director of NSA provides one final review and is the final selection authority.

Technical skills represented in the program have included:

- Computer science
- Cryptanalysis
- Engineering and physical sciences
- Health services
- Information systems security
- Intelligence analysis
- Logistics
- Legal
- Language
- Mathematics
- Networks
- Psychology
- Resources management
- Signals collection/signals conversion
- Signals analysis

Program Content

Even though each STDP participant's program is different, they have some commonalities.

Academics. Although most programs include some type of academic course work, many of our participants can (and do) teach doctoral-level courses, so finding relevant academic work is often a challenge. For those participants, creativity is key. Their academic activities may include using various government training opportunities, serving as a visiting professor, contracting with outside experts for individual study, and/or working with an expert in a lab at an academic center of excellence.

Internal tours within NSA. Because NSA is such a large organization, a participant's narrow area of expertise may be relevant to more than one mission area. For example, an employee who has spent his or her career working a specific type of technical analysis focused on protecting National Security Systems might do an internal tour using similar technical skills applied to a different mission set.

External assignments. All participants do some type of external assignment. Many do more than one. Most spend at least a full year outside NSA. Examples include tours in industry or other government agencies.

Immersion. Participants either develop an intensive activity that requires applying learning to a mission area, or deeply immerse themselves in a key technical activity.

Technical leadership. All participants must take technical leadership training and/or participate in activities in which they develop technical leadership skills. For example, they may lead some kind of working group or a research effort.

Short-term activities specific to the area of expertise. These activities include but are not limited to site visits, conferences, seminars, and project participation.

Participants' Commitment

The program is the participants' primary work obligation. It takes a significant commitment. Because the participants remain with their parent organizations and will ideally be applying their learning immediately, it may be the hardest three years of their employment because they will be balancing learning with continuing to perform and/or technically support NSA's missions. The STDP is not a sabbatical. The fact that the participants are still in the workspace also, at times, results in mission managers asking them to spend more time on mission than they had planned. This inherent pull between the STDP and the needs of the parent organization can easily become a challenge for the participant. For a mission emergency, such as immediately after the 9/11 terrorist attacks, participants can be granted a pause in their programs. Granting such a pause is the exception even though most participants experience this tension. Navigating the tension, however, is good technical leadership training as it helps the participants balance competing priorities—a skill that can be the difference between the success or failure of the most senior technical leaders and experts. If it becomes too difficult, though, the participants have significant support. The mentors, the monitor, and/or other members of the STRP will intervene with the individual's management and help the participant deconflict the requirements.

Challenges

The biggest challenge the STDP currently faces is identifying appropriate technical leadership training and development activities. For the first ten years of the STDP's existence, its technical leadership development activities focused on learning by doing, such as leading a research effort. More recently, the participants have been attending managerial leadership training and trying to adapt it to technical leadership. Although this approach provides value, it is not exactly what the participants need—even with the best providers.

We have added training on how to influence outcomes when one does not have position authority. This has been helpful but not sufficient. Coaching has also been helpful. We have designed an internal coaching program specifically for our STDP participants that differs from the program tied to NSA's more traditional leadership development. The coach for the STDP is trained both as a clinician and as a coach. Often coaching focuses on challenges associated with transitioning into the program or transitioning back to the workplace full time after graduation. Coaching in support of these and other transitions often involves a discussion of program goals and activities, as well as mission challenges.

Finally, because we are targeting our best and brightest, getting managers to "give up" these experts, even part time, is difficult. At NSA, as in most of the Defense Department components, there is a preference for rotating managerial leaders. Some managers take a long-term view and understand that the participant will give back over three years and will be an incredible resource at the end of the program. Unfortunately, the manager who supervised the participant at the time of application will probably not be in the same position after three years so will not reap the ultimate benefit when the participant graduates.

Return on Investment

Despite the challenges, this program is paying dividends. As members of the STRP, the authors regularly see participants make incredible mission contributions. In addition, very few STDP graduates leave NSA. Fisher (2001) discussed the critical need to focus retention efforts on technical personnel because of the cost of replacement. Fisher found that the most critical factor in retaining technical personnel is the opportunity to get ahead without becoming managers. She further recommended that organizations have a clear technical path to advancement. We believe the NSA technical career path and the STDP program have provided those dividends.

References

Abbey, A., and Dickson, J. W. 1983. R&D work climate and innovation in semiconductors. *Academy of Management Journal* 26:362-368.

Birnbrauer, H., and Tyson, L. A. 1984. Flexing the muscles of technical leadership. *Training & Development Journal* 38 (9): 48-52.

Blanchard, K., and Johnson, S. 1981. *The one minute manager.* New York: William Morrow.

Bowers, C., Salas, E., and Jentsh, F., eds. 2006. *Creating high-tech teams.* Washington, DC: American Psychological Association.

Civiello, C. L. 1999. Cyberspace, trusted insiders, and organizational threat: The role of the psychologist manager. *The Psychologist-Manager Journal* 3:41-48.

Civiello, C. L., and Welker, N. 2009. Developing technical leaders at the National Security Agency. *The Psychologist-Manager Journal* 12:149-162.

Cotter, G. R. 1991. *STRP study of the agency technical track.* Unpublished internal government study. National Security Agency: Fort George G. Meade, MD.

Drysdale, T. 1968. *Improvement of the procurement, utilization, and retention of high quality scientific and technical officers.* USAF PRL Technical Report, No. 68-570.

Dutta, S. K. 2001. Assessing the critical behavioral competencies of information technology (IT) project managers at Southern California Edison. *Dissertation Abstracts International: Section B: The Sciences & Engineering* 62(6-B), 2980.

Fisher, A. 2001. *If my career's on the fast track, where do I get my road map?* New York: Morrow.

Freedman, A. M. 1995. The consultant's sense of urgency: Steady-state versus front-line combat OD. In *The 1995 annual: Developing human resources*. San Diego: Pfeiffer.

Hackman J. R., and Wageman, R. 2007. Asking the right questions about leadership: Discussion and conclusions. *The American Psychologist* 62:43-47.

Helme, W. H., Willemin, L. P., and Grafton, F. C. 1975. *Dimensions of leadership in a simulated combat situation.* U.S. Army BESRL Technical Research Note, 1971 Jul75.

Hewlett, S. A., and Luce, C. B. 2006. Extreme jobs: The dangerous allure of the 70-hour workweek. *Harvard Business Review* 84(12): 49-59.

Howard, A., and Bray, D. W. 1988. *Managerial lives in transition: Advancing age and changing times.* New York: Guilford Press.

Hunt, J. G., Dodge, G. E., and Wong, L. eds. 1999. *Out-of-the-box leadership: Transforming the twenty-first-century Army and other top-performing organizations.* Vol. 1 of *Monographs in leadership and management*. Lubbock, TX: Elsevier Science/JAI Press.

Jaques, E. 2001. Diagnosing sources of managerial leadership problems for research and treatment. *Consulting Psychology Journal: Practice & Research* 53:67-75.

Kendra, K. A., and Taplin, L. J. 2004. Change agent competencies for information technology project managers. *Consulting Psychology Journal: Practice & Research* 56:20-34.

Kilburg, R. R. 2006. *Executive wisdom: Coaching and the emergence of virtuous leaders.* Washington, DC: American Psychological Association.

Kilburg, R. R. 2012. *Virtuous leaders: Strategy, character, and influence in the 21st century.* Washington, DC: American Psychological Association.

Levinson, H. 1982. *Executive.* Cambridge, MA: Harvard University Press.

Mael, F. A., Waldman, D. A., and Mulqueen, C. 2001. From scientific work to organizational leadership: Predictors of management aspiration among technical personnel. *Journal of Vocational Behavior* 59:132-148.

Pausch, R. 2008. *The last lecture.* New York: Hyperion.

Rath, T. 2006. *Vital friends.* New York: Gallup Press.

Robben, M. A. 1998. A study of the determinants of individual innovative behavior in a high-technology product development organization. In *Dissertation Abstracts International Section A: Humanities & Social Sciences* 59(4-A), 1252.

Rupp, D. E. 2006. A dedication by Douglas W. Bray. *The Psychologist-Manager Journal* 9:67-69.

Sayles, L. R. 1989. *Leadership: Managing in real organizations*. New York: McGraw-Hill.

Siegfried, Jr., W. D. 2006. Introduction. Developmental assessment centers. Special issue, *The Psychologist-Manager Journal* 9:71-74.

Sternberg, R. J. 2007. A systems model of leadership: WICS. *The American Psychologist* 62(1): 34-42.

Thompson, A. D. 2006, March. "The worthy leader: Turning the notion of leadership inside out!" Presidential address at the Society of Psychologists in Management Annual Conference, San Francisco.

Thompson, A. D., Grahek, M., Phillips, R. E., and Fay, C. L. 2008. The search for worthy leadership.

Consulting Psychology Journal: Practice and Research 60:366-382.

Wagner, R., and Harter, J. K. 2006. *12: The elements of great managing.* New York: Gallup Press.

Zaccaro, S. J. 2001. *The nature of executive leadership: A conceptual and empirical analysis of success.* Washington, DC: American Psychological Association.

Farmhouse Field Station Houlton, Maine: The U.S. Army's First Fixed Field Site

Betsy Rohaly Smoot

> There is a great need for a radio station which is not devoted to particular programs but which is always ready for immediate use on special examinations, a station which supplements but does not duplicate the work done elsewhere. The station at Houlton, Me., has apparatus available which has been shown to be well suited to this purpose and the personnel has unusual ability in reading cipher, Spanish, and German.
>
> —Colonel John M. Dunn, acting director of military intelligence in January 1919[1]

From just before the Armistice of 1918 until just before the reorganization of the Army in 1920, there was a unique experiment in signal collection and signals development—the first fixed field site in the U.S. Army, established in a rented seven-room farmhouse in Houlton, Maine. Houlton was intended to be exclusively a radio intercept site; however, conflict with the Navy would force it to shift mission from communications intelligence to radio experiments, and back, several times during its short, stop-and-start existence. Houlton faced continued challenges to its mission. Logistics were never easy, and personnel issues vexed the station commanders. But the site did make both cryptologic and experimental contributions before it closed in 1920.

This article is a revised and expanded version of the author's presentation, "Technology and Radio Intercept: The Site at Houlton, Maine, 1918-1920," given at the Center for Cryptologic History's 2013 Cryptologic History Symposium.

Why did the War Department's Military Intelligence Division (MID) want a site such as Houlton? The MID had a successful system of mobile Radio Tractor Units (RTUs) deployed along the U.S.-Mexican border but was very aware of the long-distance German radio stations that broadcast to much of the world. It was believed that collection of these broadcasts from German stations at Berlin, Nauen, and Eilvese could provide communications intelligence support to post-armistice peace talks.

The Army was not the only interested party. The U.S. Navy was interested in collecting these broadcasts. And the British Admiralty's Room 40 had been collecting and analyzing communications from Nauen since 1914.

By mid-October 1918, the chief of the MID's Radio Intelligence Service (RIS), Major Carl Kinsley,

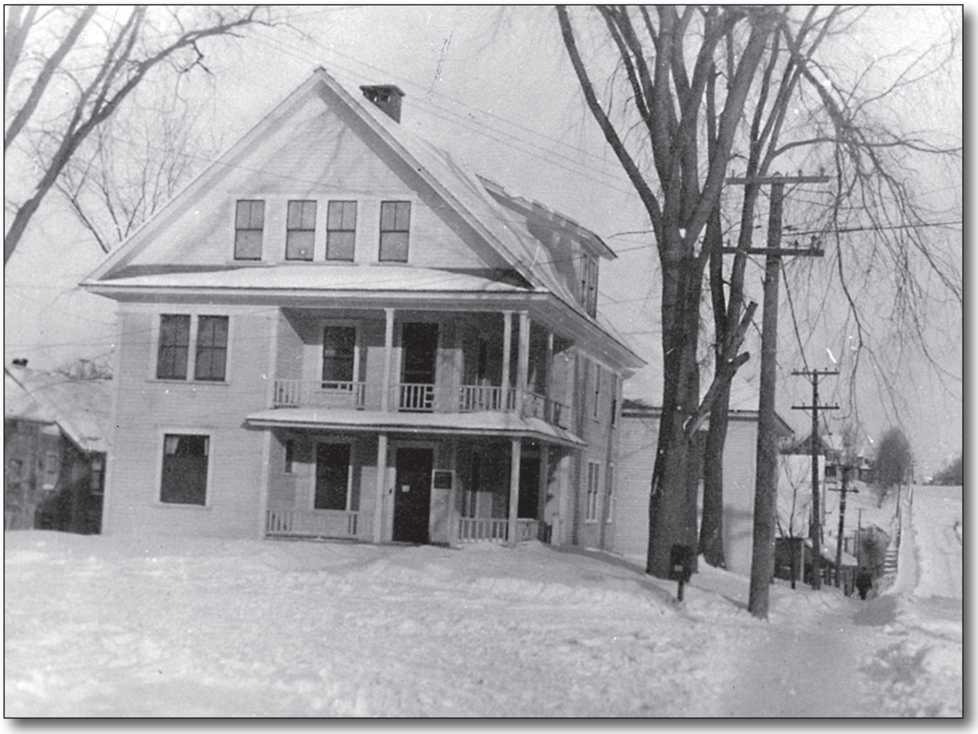


Fig. 1. The intercept house, Gillen Farm, Houlton, Maine (NSA Archives, Accession 41243)

noted that a station could be established to intercept traffic from Nauen "with no more delay than necessary to have radio operators ordered to the place where it was decided to establish such a station." The RIS controlled Army intercept facilities and operations in the United States and had been established in January 1918. Designated MI-10E, the RIS was under the control of MID's MI-10 Office of Censorship. The cryptanalytic (and other cryptologic) work of the MID was done in MI-8, which was run by Major Herbert O. Yardley.

The Beginning

How was the Houlton site selected? This remote location is now best known as the northern terminus of Interstate 95. A survey done sometime in 1918 reportedly noted that Houlton was "the best location in the United States for this purpose."[2] It is possible that the MID was drawn to Maine because of the interest of the Navy, which established its own radio station and intercept site at Bar Harbor in the autumn of 1918. But it is clear that Houlton is one of those places in the world that is just right for long-distance HF intercept, and the survey likely made that evident to the Army. The reception qualities of the area were not forgotten, for in 1927 AT&T would establish its transoceanic telephonic receiver station two miles west of the town.

The Army worked quickly to get its new Maine station in place. On October 28, 1918, orders were given to proceed, and Lt. Lee Sutherlin, who had extensive experience with the RTUs, was sent from Washington to Houlton to make preliminary arrangements. It was Sutherlin who located and executed a lease on the Gillen Farm (see Figure 1), on the southwest corner of White Settlement Road and Military Road (now U.S. 2). The house and property, plus all repairs, telephone service, electric light and battery service, stoves, fuel, and water were leased by the Army for forty-five dollars a month for a term of six months. The farm included a shed, a barn, and enough cleared ground for an antenna. The station was a mile and a half from Houlton's main square. There was no housing on the site; the men would board in town and walk the approximately twenty-five minutes to the station.

Radio Tractor Unit 33 at Laredo, Texas, was shut down to staff Houlton. Some of its equipment was stored; some was shipped to Maine. More apparatus was shipped from Washington. The Army's 3rd Service Company in Boston was asked to handle logistical support and pay, and the quartermaster immediately sent a Royal typewriter. Five boxes of equipment from Texas arrived before the men got there. Laredo's officer and five men were sent to Maine, with the intention of adding seven radio operators (three from Fort Sam Houston and four to be named later). The men left Laredo on the evening of November 4; three others left Fort Sam Houston on the morning of November 5.

It was unlikely that the Army could have found a better commander for this new station. Second Lieutenant Arthur J. Boeder of New York was just shy of his twenty-fifth birthday when he arrived at Houlton in early November 1918. He had enlisted in September 1917 and had an outstanding resumé, ideally suited for assignment at what was a new type of collection site. Boeder had worked for both the Marconi and United Wireless telegraph companies and had spent time at sea as a radio operator. He copied both American and continental Morse, had studied electricity at the Pratt Institute, and served as a radio instructor at the U.S. Aviation School at Cornell University before joining up. And, critically, Boeder had been an enthusiastic amateur radio operator from a young age. He was even mentioned in a newsletter for radio amateurs and called "a dandy little operator, and long before he was out of short pants, he left lots of others in the dust."[3]

Boeder and two privates arrived in Houlton on November 8. While some accounts have the station operating as early as November 9, some claim intercept began on the day of the Armistice, November 11. But personnel were still arriving on the 11th, and it was not until that day that the holes were dug for the poles and the lumber ordered for them. Ten poles were set, running southwest from the house, on November 12, and one thousand feet of antenna wire was strung from the poles on the 13th. Instruments were connected that same day, and Boeder reported that "reception started on a regular schedule." Houlton was in operation.[4]

A private telegraph line between the site and Washington was installed; intercepted messages were sent by telegraph by the Army operators rather than going through commercial operators in town to minimize the introduction of garbles. Confirmation copies were sent to Washington by U.S. mail. The operators noted that intercept conditions "were exceptionally good" and attributed this to the site being on "one of the highest hills east of Houlton."

Messages intercepted from the German radio stations were sent to Washington within half an hour of collection. By November 19 arrangements had been made with Yardley's MI-8 for rapid handling of coded and ciphered intercept. Everything seemed to be in place for a successful operation.

Conflict with the Navy

Then on November 20, a week after the intercept had begun in earnest, the order came from the secretary of war to halt operations immediately. That eternal enemy of the U.S. Army, the U.S. Navy, objected to the Houlton operation.

Various government studies and decisions resulted in the Navy having de facto control of government radio operations in the United States.[5] The Army had been permitted to control radio needed for Army purposes. RTUs on the Mexican border had not bothered the Navy; neither had the Army intercept operation inside the U.S. embassy in Mexico City.

But in the fall of 1918 the Army's Houlton site was seen as competition for, and duplication of, the new Navy radio transmission and interception station at Bar Harbor, Maine. At a cabinet meeting, the secretary of the Navy protested the operation of an Army station so close to the Navy station, and the secretary of war had little option but to order the MID to shut down collection operations. It is possible that the Navy considered long-distance transatlantic radio strictly its responsibility, particularly as Houlton could not easily have been said to support Army operations. Houlton discontinued intercept within two minutes of receiving the telegram from Washington.

General Marlborough Churchill, then director of the MID, was convinced that the site's collection capability would be needed to intercept German propaganda broadcasts during the upcoming peace conference and suggested the equipment and antenna be left in place.

Major Kinsley at the RIS now had three options to consider. The first was to return Boeder and six men to Laredo and leave the station in care of two men. The problem with this option was travel time to get the men back if the station had to resume collection rapidly.

Option two was to reorganize for experimental work, building on work the MID had been doing with the RTUs and the Bureau of Standards. Kinsley noted that the work "could be discontinued and the men ordered to Laredo after a week or two, if at the end of that time it appears that there is no possibility of resuming regular reception operations at Houlton." This was the RIS's best solution if there were to be any possibility of resuming communication intercept.

The third option was to order Lieutenant Boeder and six men to Washington for experimental work for a few weeks, leaving two men in charge of the Houlton station. This was suggested as a solution in case the Navy objected to the operation of even an experimental station at Houlton.

> The operators noted that intercept conditions "were exceptionally good" ... Messages intercepted from the German radio stations were sent to Washington within half an hour of collection.

After considering the matter for forty-eight hours, the RIS chose option two and placed Houlton on experimental status on November 23. Aware that this change in mission could hurt operator morale, General Churchill sent a memo to the site noting that operations were not discontinued because the director of Military Intelligence or the chief of staff considered it unimportant. "In fact, the very opposite is true," wrote Churchill, "and the efforts now being made to make arrangements to resume the service are evidence of its importance for the period of the armistice and peace conference, and possibly for some time afterwards." The site was directed to "organize your work [so] that if a telegram is received to resume operations immediately, you can resume as promptly as you discontinued and, once started, maintain the service with the same degree of efficiency that characterized your former operations."

The Way Forward?

Interestingly, and likely in violation of whatever promise had been made by the Army to the Navy, the site was instructed to intercept the code mes-

> [The men] ... made a condenser of tin foil and paper which they placed across the terminals of the simplex set. They found this almost doubled the strength of the signal from Nauen [Germany].

sages transmitted by the German radio transmitter at Chapultepec, Mexico, each night and to take audibility readings and watch for any related transmissions.[6] This was due to a cryptologic breakthrough in Washington. On November 13, the same day Houlton had begun collection, MI-8 had broken code messages sent out by Chapultepec for the first time since August 14, and a message intercepted by an RTU on November 9 showed a relationship between the German station at Nauen and the station at Chapultepec. It was hoped that Houlton would be able to intercept traffic that could not be collected by other stations. Boeder was ordered to report progress against the Nauen-Chapultepec link daily.

Meanwhile, on the experimental front, Houlton started to receive instructions for taking audibility readings, conducting direction finding, and plotting polar curves. Personnel were also given instructions for various adjustments of the loop antenna. And they were directed to listen for testing of a radio set operated by General Electric (GE) at Schenectady, New York. Houlton did intercept the GE test on November 29.

The men installed two additional antennas, one a 600-foot, insulated-wire ground antenna at right angles to the regular antenna, and they tried to work a simplex set on the regular antenna and a multiplex set on the ground antenna, but this didn't work. In fact, Boeder asked if it were really important to conduct the ground antenna tests as these experiments meant taking equipment out into the snow and exposing men to the very cold weather.

Inside, they tinkered with the equipment and made a condenser of tin foil and paper which they placed across the terminals of the simplex set. They found this almost doubled the strength of the signal from Nauen. Another experiment showed they could increase intercepted signal strength by more than three times by fastening a wet piece of coal to the upper input tap on their amplifier.

Cryptanalytic Breakthrough

On December 12, likely while listening for Chapultepec, Houlton intercepted fourteen cipher messages sent by Berlin to Madrid. These messages were forwarded to MI-8 where by December 19 John Matthews Manly, Yardley's second-in-command, had deciphered seven of them, a total of 720 words. Manly felt that it was of the "highest importance that these messages be obtained daily and transmitted here without delay. They come from the heart of Germany and are the confidential communications of a minister to his home government."[7]

Notably, the Navy's site at Bar Harbor had *not* copied these messages; they were unique to Houlton. Manly consulted with the Office of Naval Intelligence and the Navy's Radio Communications department and said that the Navy had not intercepted any German cipher messages in two months and that few had been collected by any other site. Manly claimed that "the Navy were no longer paying any attention to the German cipher messages and that Captain [David W.] Todd, Chief of Radio Communications, had expressed himself as in favor of the immediate resumption of operations by the Houlton Station."

Despite Manly's assurances, MID leadership on December 14 noted Navy opposition was still preventing the resumption of collection operations at Houlton. However, likely relying on Manly's conviction that this was important, Colonel John Dunn, who was serving as acting director of the MID while Churchill was temporarily away, ordered Houlton to resume regular interception activities on December 19. Dunn was hopeful that this was a permanent move, and told the station that there had been some favorable developments and that "definite instructions" would be provided in a few days. His hope was extremely short-lived. The next day, December 20, Houlton was again told to discontinue intercept operations.[8]

To Siberia?

While it is probable that Manly's work and his queries to the Navy caused the brief resumption of intercept operations in mid-December, the restart may have reflected a more general confusion within the MID about the role of Houlton.

For the RIS had badly misinterpreted some communication from the Signal Corps. On November 19, the Committee on Public Information—charged with pro-war American propaganda—wrote to the Signal Corps suggesting that the Corps set up a long-distance radio receiving station in Omsk, Russia, in southwestern Siberia. General George O. Squier, head of the Signal Corps, then ordered that "certain special receiving apparatus, which has been used in the trans-Atlantic [*sic*] investigation recently discontinued" be sent to Omsk along with an officer familiar with these investigations and the workings of long-distance radio communications. Squier meant for this to be acted on by the Signal Corps Engineering and Research Division. Squier's endorsement of the idea on December 6 so near to the November 20 halt in operations at Houlton certainly contributed to the MID misunderstanding of the task. It seemed clear to all in the RIS that Houlton's discontinued transatlantic radio work was the activity Squier had mentioned.

So the RIS sprang into action. An urgent message was sent to Kinsley, who was visiting the RTUs along the Mexican border. Dunn specified that the needed personnel would be volunteers from the RTUs, and that gaps in those units would be backfilled by the men of Houlton, who were not currently conducting intercept. Boeder polled the Houlton men, but only two had expressed interest in the Siberian expedition. Houlton's set of equipment was thought to be ideal for what would be needed by a station in Omsk, and a list of needed parts and radios was compiled.

The MID was likely surprised and perhaps embarrassed when a letter from Lieutenant Colonel Joseph Mauborgne[9] reached it on December 17 making evident a misunderstanding on the part of the RIS. Despite its transatlantic work, the Houlton station belonged to the MID and was not administratively connected with the Signal Corps. While the Signal Corps, unlike the Navy, had no objection to Houlton's work, Mauborgne made it clear that the RIS was not to be involved with the Omsk effort.[10]

All the conflicting orders prompted Dunn to write to the men of Houlton on December 23 in an attempt to explain the confusion. He tried to reassure them but admitted it was impossible to say what the ultimate status of the site would be. Dunn continued to hope that intercept soon would resume.

But it was not to be. Houlton would not be tasked with intercept again until late April 1919.

Experimental Work

When intercept was halted by politics in the early months of 1919, the site was kept running to conduct radio experiments. These were still the early days of long-distance radio communication, and it was thought this was a productive way to keep personnel at Houlton and support the Army's desire to better understand the physics of radio.

Houlton was deeply involved in collecting data to support ongoing investigations of whether a definite relationship existed between the sizes of the loop

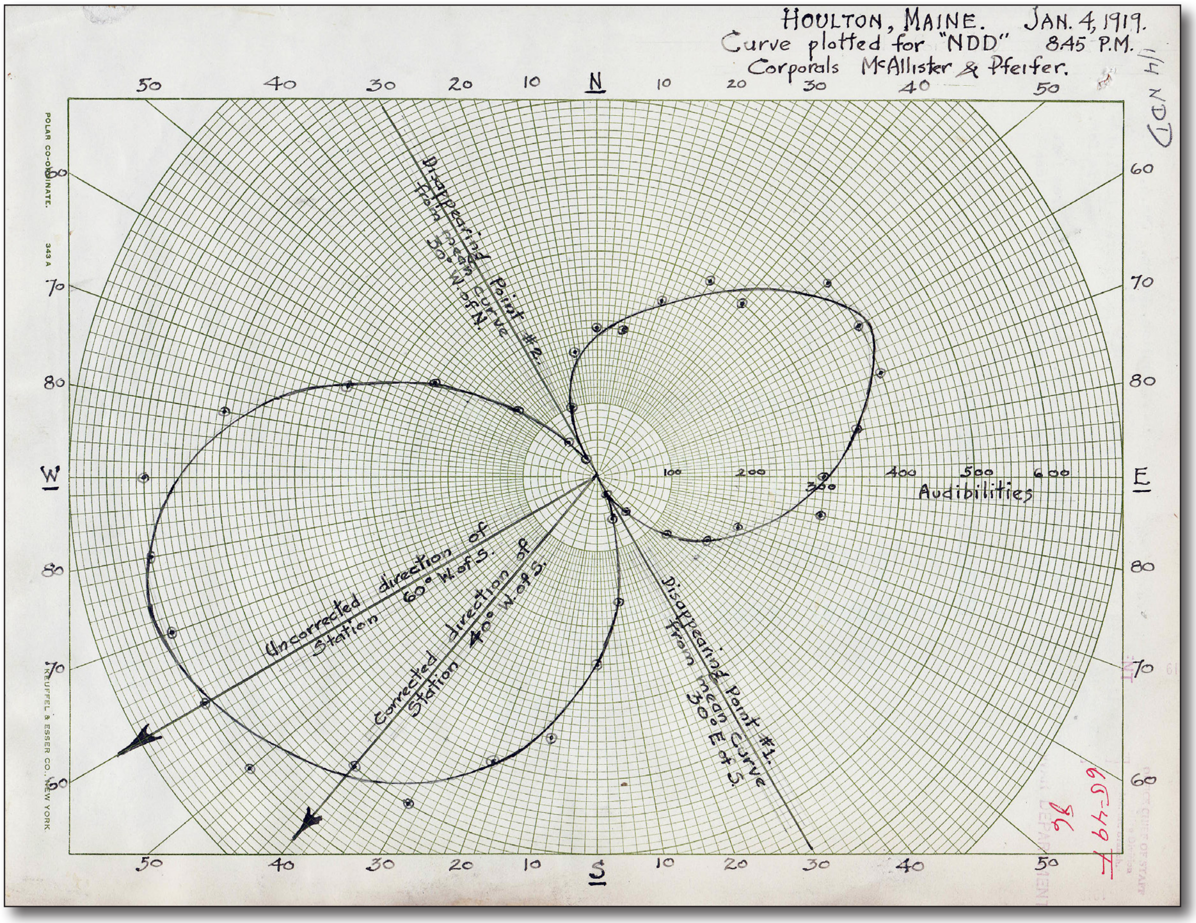


Fig. 2. Typical polar curve diagram made at Houlton by Corporals McAllister and Pfeifer (records of the Military Intelligence Division at the National Archives, College Park, MD)

antennas used to plot polar curves used for direction determination (see Figure 2), and the absolute direction of the stations. This was admittedly something MID had wanted to pursue but which it had "been unable to give it the necessary time." It was emphasized that this was important work, and not just a temporary arrangement, but the work was not interesting to the radio operators who were trained to intercept communications. And, despite the cold winter weather, the men were ordered to continue with the outdoor work on the ground antenna.

As part of the antenna experiments, the men constructed a large inverted-L loop antenna in a barn adjacent to the station, which they mounted on a platform with compass markings (see Figure 3). The wires from the end of the loop were brought through the wall into the room where the intercept operators sat. When the weather became too severe, they built a loop inside. But the test was deemed disappointing as "the difference in audibility between one side and the other is not as great as was expected."

The operators tested equipment and conducted direction-finding experiments using known U.S. and foreign radio broadcasts. Site personnel developed their own antennas, often using supplies they bought locally without specific authorization, which caused

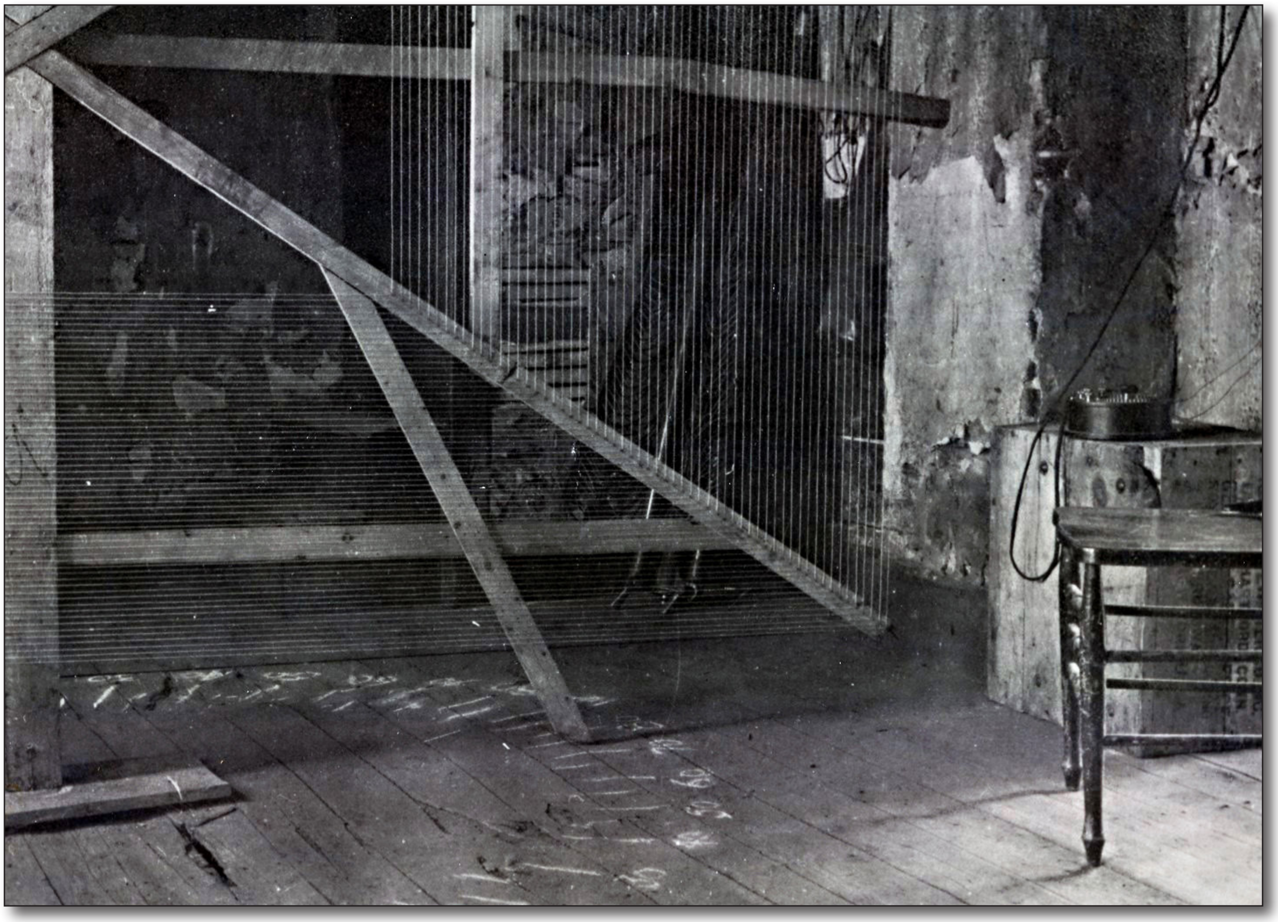


Fig. 3. L-shaped loop antenna at Houlton; note the compass markings chalked on the floor (records of the Military Intelligence Division at the National Archives, College Park, MD)

problems with reimbursement. A triangle loop was built early in January 1919. Testing showed it acted exactly the same as the square loop and, like the inverted-L loop, did not provide greater hearability.

The experiments may have bored the men (although Boeder seemed to be enthusiastic), but they did contribute to at least one technical paper. Kinsley and his deputy, Captain Albert Sobey, published "Radio Direction Changes and Variations of Audibility," based on RTU and Houlton experiments made during the winter and spring of 1919. The experiments used a radio goniometer (direction finder) and attempted to discover how long-distance radio waves propagated by examining how waves might bend in reaction to atmospheric conditions, and how changes of audibility might relate to changes in direction of the signal.

While Holton was on experimental status, Dunn had been working very hard to reinstate the collection mission. In mid-December 1918 he wrote a memo to General Squier. In January, Dunn sent a memo to the War Department chief of staff with a suggested draft of a letter for the secretary of war to send the secretary of the Navy regarding the work at Houlton. Dunn's argument rested on the cipher messages intercepted in December. He asked that the secretary of the Navy

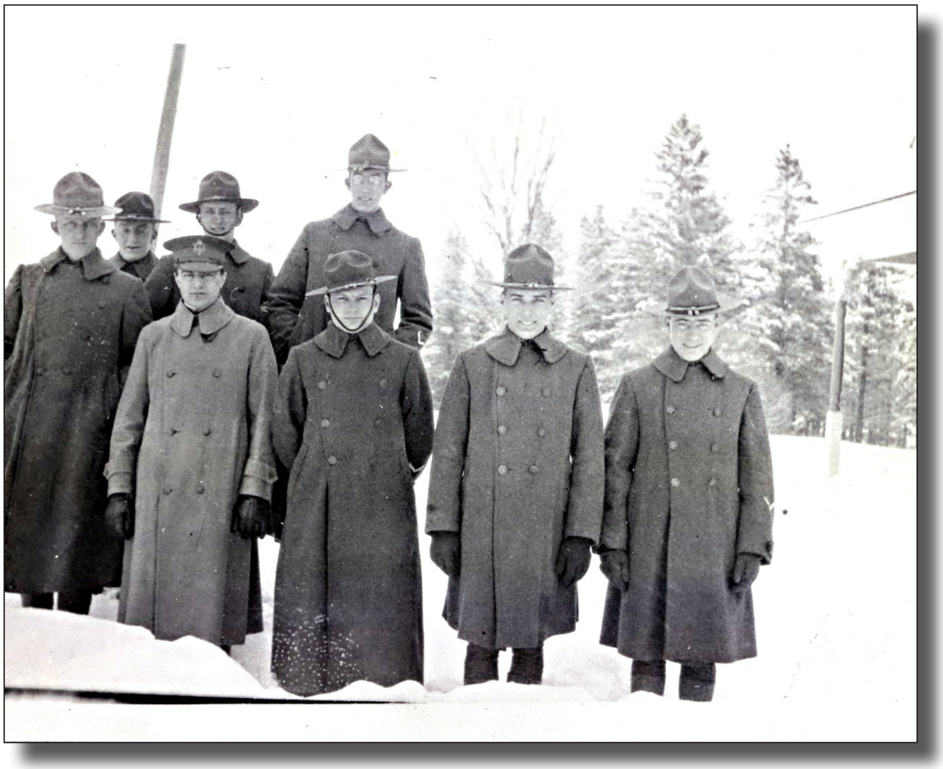


Fig. 4. The staff of the Houlton site, date and names unknown (NSA Archives, Accession 41243)

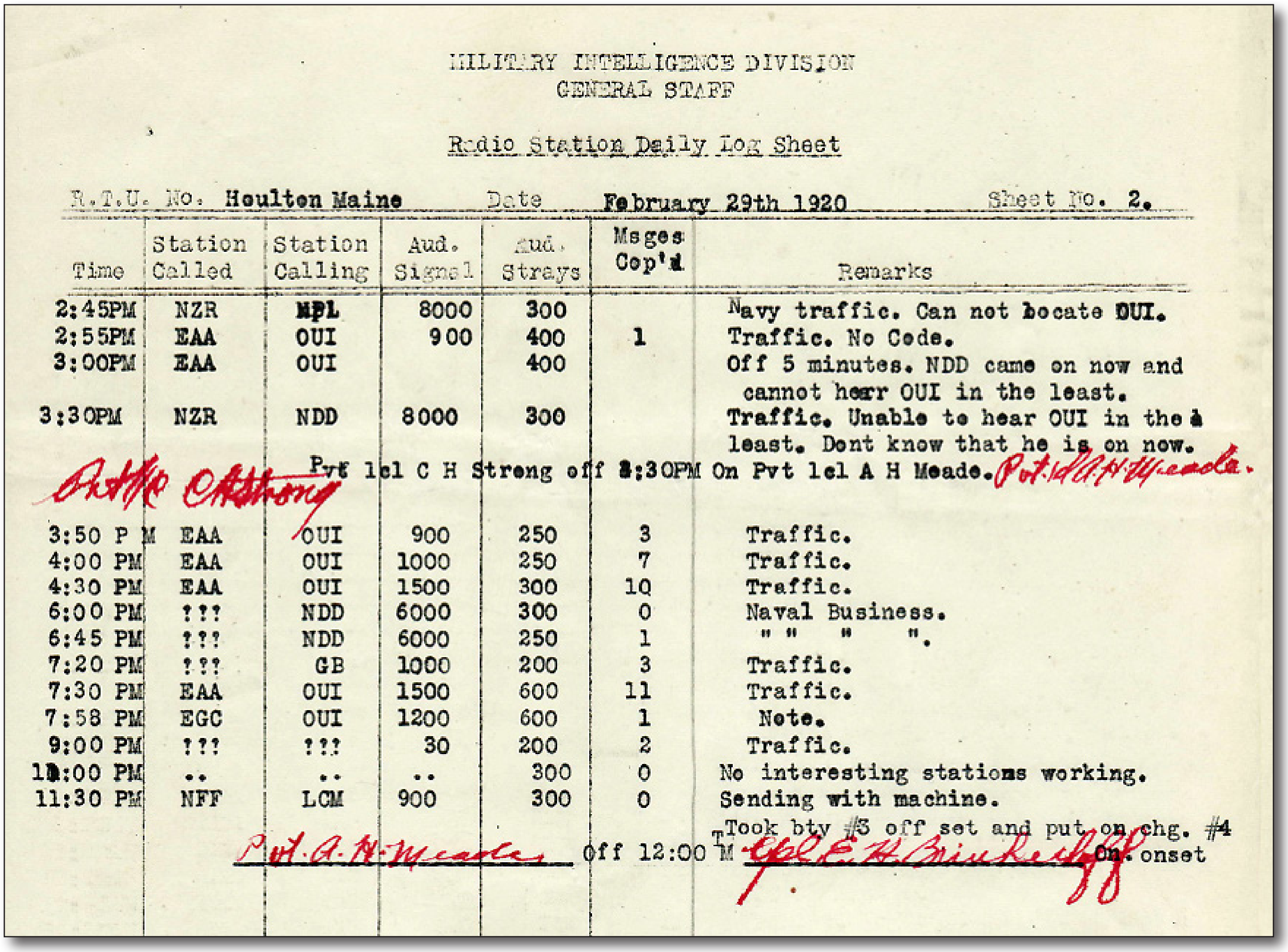
"recognize as desirable the employment of the radio receiving station at Houlton, giving his consent to its use for the confidential assistance of the Military Intelligence Division along the lines set forth herein." Churchill's memorandum to the War Department chief of staff on April 16, 1919, with Dunn's draft letter for the secretary of war to sign and send to the secretary of the Navy, emphasized that the Navy had stopped intercepting foreign code and cipher messages and that the Navy and Signal Corps agreed to resuming operations at Houlton. This evidently worked, as Houlton resumed intercept on April 20.

Personnel Problems

Just prior to the resumption of intercept, on April 10, personnel issues came to a head. The enlisted men of Houlton sent a memo on the subject "Discharge" to the director of military intelligence. The men had heard (in error, as it turned out) that most of the RTUs were to be demobilized, yet Houlton was expected to continue on experimental work indefinitely. In their minds, the national emergency of World War I, which had triggered their enlistment, was over and it was time to go home.

According to the men, "the experimental work now being carried on here and which has been going on for more than four months, may be of great interest to scientific men, but it is for the most part very monotonous to the practical radio operators who compose [*sic*] the unit. There is injustice in the fact that we are being held in the Army to do this work which has no connection with the emergency which brought us into the Army, and which work in our opinion should be done by civilians with laboratory facilities." Nearly all the men had civilian positions waiting for them, some in commercial radio, and they felt "every minute spent here in this work is setting back our future prospects considerably."

Boeder forwarded the memo with his comment that this attitude had begun when intercept operations were halted. Despite his best attempts to explain the value of the experimental work to them, he felt the men had no desire for the work and were extremely dissatisfied. In separate correspondence of April 14, Boeder declined to put forward any of the men for promotion because of their poor attitude toward the work they had been assigned. Churchill, by now back in place at the MID, replied on April 16, refuting the idea that Houlton would be a permanent experimental station and stressing that the site would be needed for intercept again soon. Critically, Churchill noted that if Houlton were to be maintained indefinitely,



MILITARY INTELLIGENCE DIVISION
GENERAL STAFF

Radio Station Daily Log Sheet

R.T.U. No. Houlton Maine Date February 29th 1920 Sheet No. 2.

Time	Station Called	Station Calling	Aud. Signal	Aud. Strays	Msges Cop'd	Remarks
2:45PM	NZR	NPL	8000	300		Navy traffic. Can not locate OUI.
2:55PM	EAA	OUI	900	400	1	Traffic. No Code.
3:00PM	EAA	OUI		400		Off 5 minutes. NDD came on now and cannot hear OUI in the least.
3:30PM	NZR	NDD	8000	300		Traffic. Unable to hear OUI in the least. Dont know that he is on now.

Pvt 1cl C H Strong off 3:30PM On Pvt 1cl A H Meade. Pvt 1cl A H Meade. Pvt 1cl C H Strong

Time	Station Called	Station Calling	Aud. Signal	Aud. Strays	Msges Cop'd	Remarks
3:50 P M	EAA	OUI	900	250	3	Traffic.
4:00 PM	EAA	OUI	1000	250	7	Traffic.
4:30 PM	EAA	OUI	1500	300	10	Traffic.
6:00 PM	???	NDD	6000	300	0	Naval Business.
6:45 PM	???	NDD	6000	250	1	" " " ".
7:20 PM	???	GB	1000	200	3	Traffic.
7:30 PM	EAA	OUI	1500	600	11	Traffic.
7:58 PM	EGC	OUI	1200	600	1	Note.
9:00 PM	???	???	30	200	2	Traffic.
10:00 PM	..	..	..	300	0	No interesting stations working.
11:30 PM	NFF	LCM	900	300	0	Sending with machine.

Took bty #3 off set and put on chg. #4

Pvt A H Meade Off 12:00 M Cpl E H Brinkerhoff On. onset

Fig. 5. Intercept log, Houlton, 1920, completed by PFC C. H. Strong, PFC A. H. Meade, and CPL E. H. Brinkerhoff (records of the Military Intelligence Division at the National Archives, College Park, MD)

the unit would be reorganized and men who desired to leave the service would be allowed to depart.

Intercept *and* Experiments

The station's personnel (Figure 4) were pleased to return to what they considered their real job on April 20. And the MID was pleased to have cipher messages again coming in regularly and noted in late April that about half were easily readable and half were being "vigorously worked on." Washington asked if Houlton could set up another antenna so that they could work two stations simultaneously. By May 1 the station was told to concentrate on interception of cipher messages rather than plaintext press. The German station at Eilvese was the only one found to be sending code at that time, but Houlton continued to monitor Berlin and Nauen's short- and long-wave broadcasts (see Figure 5).

Between April 26 and May 6, Houlton collected ninety-eight code messages. Nineteen were decoded by MI-8. These were all diplomatic messages, and Washington noted that in certain cases they had been "decoded, translated and put before our Secretary of State before they reach their reader." Houlton was providing timely, actionable intelligence, likely supporting the Paris Peace Conference.

In May the site was tasked to make some experiments during the eclipse of the sun of May 29. These were to determine whether the cone of shadow which passes over the earth's surface changed the direction of radio signals or their audibility; it was theorized that these factors were dependent upon the state of ionization of the upper atmosphere. The tests were organized by a British committee for radio telegraphic investigation appointed by the British Association for the Advancement of Science and involved a radio transmitter in the Ascension Islands. Houlton received two thousand feet of wire for the test and erected an antenna in a northwest-southeast direction selected to receive a signal from Ascension (see Figure 6). This required permission of another landowner and more poles. The farmer consented but wanted to know how long the poles would stay up.

Also in May, the site was told that the collection from Eilvese was primarily diplomatic traffic and propaganda. While the Navy was intercepting press messages sent by Nauen, it was not intercepting either the cipher or clear text sent by Eilvese.

The rivalry with the Navy continued, but the possibility of sharing information was broached by May 26, 1919. "Navy still copies Nauen at Bar Harbor and reports to Washington by mail," said the RIS, and noted that Houlton might be able to obtain a carbon copy of this intercept.

In late July 1919 the last general set of radio experiments relating to direction and audibility took place with detailed instructions for a twenty-four-hour intercept watch.

Logistical Issues

Logistical problems with this remote fixed site became apparent almost immediately, as MID records reveal. For example, in mid-January 1919, Boeder discovered that the landlord was not receiving the rent payment because no one in the Northeastern Department in Boston had taken action on the lease. He informed MID that the landlord threatened to stop the station's supply of coal, electricity, and telephone service. This seems to have been put right quickly.

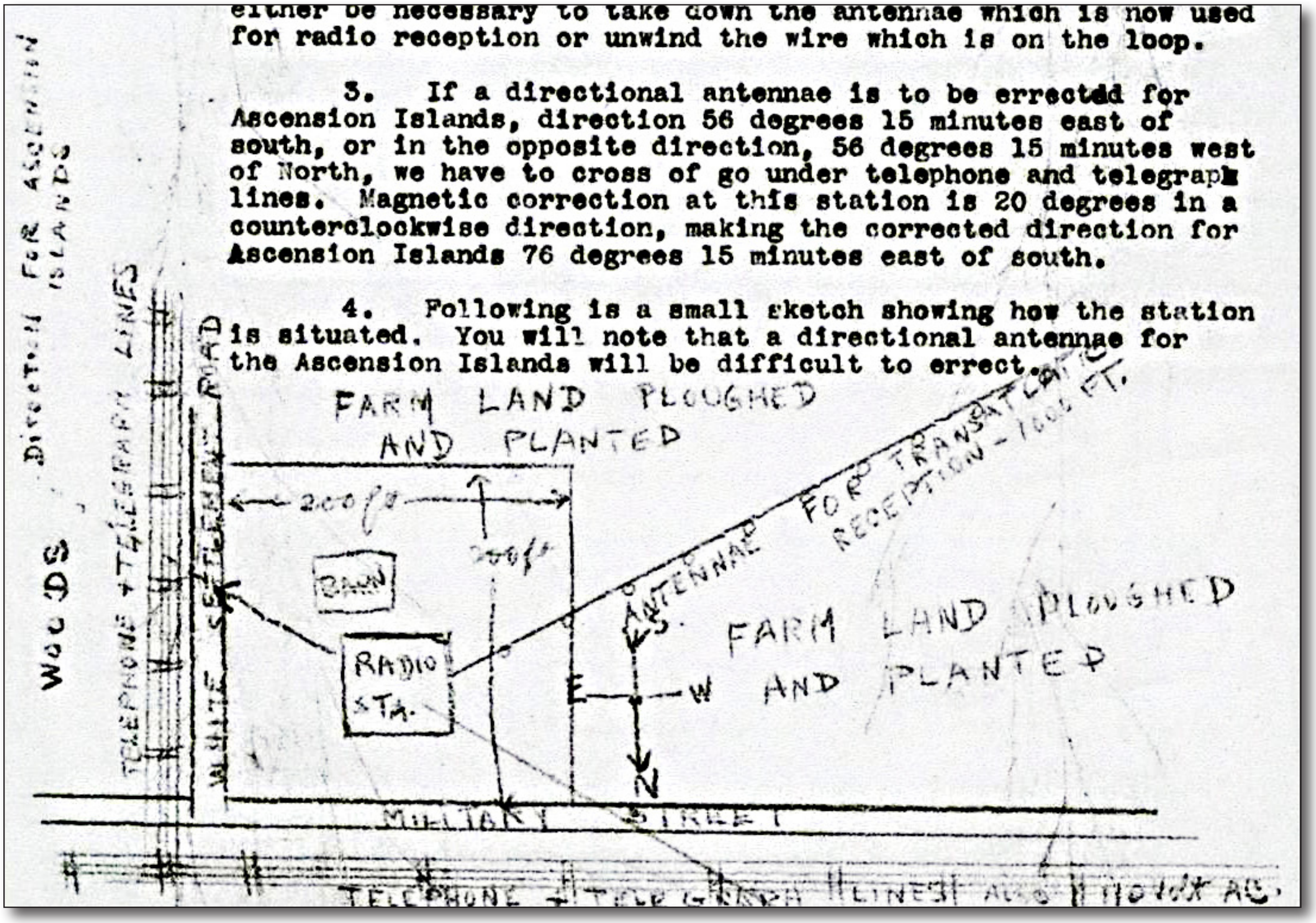
Commanders of RTUs were accustomed to contracting for repair locally and being reimbursed by the MID or the Southern Department at Fort Sam Houston in San Antonio, Texas. Boeder, who had run an RTU, made the mistake of thinking that these same rules applied at Houlton. He contracted for repairs and parts to fix equipment after a March 1919 fire in the station's telegraph room, and was still having to explain himself six weeks later.

The station had a near-constant need for blank paper, intercept forms, and the special paper needed to graph polar curves. In June 1919 Boeder told MID that the quartermaster of the Northeastern Department would not reply to requests for paper supplies. MID noted that it seemed that the quartermaster had not been granted authority to supply Houlton, and it would have to rely on Washington in the future.

In late April 1919, an urgent request for six typewriter ribbons for Houlton's Royal typewriter resulted in the receipt of only one ribbon, for a Remington typewriter. An apologetic note from MID suggested that they should wind the Remington ribbon around their Royal spool, and if this worked, they would be sent more of the same ribbon. It seems that Royal ribbons were difficult to procure. Fortunately, the Remington ribbon worked.

The End

To their great relief, all the enlisted men were demobilized in August 1919, and the station was thrown into a transition period from which it never really recovered. In June 1919 the lease had been extended to June 30, 1920, at the increased cost of forty-eight dollars per month. Most experienced radio operators left the Army for more lucrative civilian work as soon as they were demobilized. The new recruits sent to the



either be necessary to take down the antennae which is now used for radio reception or unwind the wire which is on the loop.

3. If a directional antennae is to be errectdd for Ascension Islands, direction 56 degrees 15 minutes east of south, or in the opposite direction, 56 degrees 15 minutes west of North, we have to cross of go under telephone and telegraph lines. Magnetic correction at this station is 20 degrees in a counterclockwise direction, making the corrected direction for Ascension Islands 76 degrees 15 minutes east of south.

4. Following is a small sketch showing how the station is situated. You will note that a directional antennae for the Ascension Islands will be difficult to errect.

Direction For Ascension Islands
WOODS
TELEPHONE + TELEGRAPH LINES
WHITE SETTLEMENT ROAD
FARM LAND PLOUGHED AND PLANTED
200 ft
200 ft
BARN
RADIO STA.
ANTENNAE FOR TRANSATLANTIC RECEPTION - 1000 FT.
S
E
W
N
FARM LAND PLOUGHED AND PLANTED
MILITARY STREET
TELEPHONE + TELEGRAPH LINES ALSO HOULTON AG.

Fig. 6. Houlton map showing alignment of antenna for eclipse investigation (records of the Military Intelligence Division at the National Archives, College Park, MD)

station were not, for the most part, trained radio operators, and Boeder noted in September that he alone was copying all the messages from Germany to Spain as "the new men will need several months training before they can be relied upon for reception work." Boeder attempted to have several local amateur radio operators taken on by the Army, providing that they could be assigned to the Houlton station. This effort failed when one recruit was determined to be underage and another was found to be underweight.

The shortage of trained operators left Boeder not only covering the most important watches but also devoting the rest of his time to training the new men. The MID tried to lighten the load by telling Houlton it was not necessary to copy banking communications "due to the lack of clerical help" but that the station should copy all plain language communications between Germany and Spain. All plain and code messages were needed, as the plain text helped MI-8 to decode the coded messages. Boeder was told that MID would try to find one or two operators who were competent, but "it is doubtful as it is very hard to get good operators even at high salaries outside the Army."

Yardley specifically tasked Houlton in late September with intercepting code sent between Madrid and Vienna, Madrid and Sofia (Bulgaria), and Madrid and Morocco, as these codes could now be broken. But regarding the Spanish codes, the RIS wrote: "This office thoroughly understands the amount of work which you are called on to do, and does not expect the impossible."

At the end of October the site was tasked to look for communications between an improved station near Madrid and facilities in the Americas. It was also told to listen for communications between Sofia and San Sebastian (Spain), as well as between Madrid and Morocco. Houlton reported back on November 7 that it had not yet seen those stations, but "watch will be kept on each morning until men are sufficiently trained to cover all periods of the day."

Boeder, who had not been allowed leave since his arrival in Maine in November 1918, was relieved of duty October 1919 and subsequently left the Army. He was replaced by First Lieutenant Fred H. Parish, another officer with extensive experience with the RTUs.

The MID continued to be optimistic about Houlton's future. In late December a delegation from Washington visited the Marconi station at Chatham, Massachusetts, to see equipment. The members recommended that Army radio operators receive training at the Chatham facility and noted that the equipment used there could be employed at Houlton with good results, although it was too large to be practical for the RTUs on the Mexican border.

On December 17, 1919, Houlton implemented the first known use of what were called "personal signs," now more commonly referred to as "opsigns" or "operator signs." Each operator was allowed to choose a digraph to represent his work in the collection logs, with the intent of eliminating the need for the operator to sign the log at the end of his shift. In practice, the operators continued to sign intercept logs.

Things began to falter in January 1920. The site found itself unable to collect a target station using the 10,000-meter wave length as the Navy station at Sayville, New York, began transmitting on that frequency, creating interference. Still, Houlton carried on with the task of copying German press broadcasts. If code messages were encountered and copied with sufficient accuracy, they were forwarded to MI-8. In mid-February operations came to a near halt after an extremely heavy snowfall (see Figure 7).

In late April 1920 the site was directed to send traffic by mail to Yardley, now in New York, except for "important" codes, which were to be telegraphed instead. Three copies of all foreign language intercept were to go to MID in Washington, two copies of plain language English to the Military Intelligence (MI) office of the Northeastern Department, and one copy of the same to the MID.

The last traffic appears to have been copied in April or May 1920. In May 1920 control of Houlton was given to the MI personnel in the Northeastern Department. The lease on the farm ended in June and does not appear to have been renewed. By August 1920, as part of the reorganization of the Army, responsibility for whatever remained of the Houlton site moved to the Signal Corps in the newly created 1st Corps area under the First Army.

Houlton's Legacy

In retrospect, the MID was not really prepared to operate a fixed site. While tasking procedures and the collection process seem to have been relatively straightforward, materiel and logistics were always problems and never really solved. The operators were expected to modify or build some of their own equipment and antennas, shovel the snow, and clean the intercept house, all while maintaining a twenty-four-hour watch for important communications intelligence.

Houlton did receive some of the best radio equipment available to the Army and was able to intercept signals from at least thirty-five U.S. and foreign stations. The site collected unique traffic from the German high-powered radio stations, collection which enabled MI-8 to break German codes. Information gleaned from Houlton intercept seems to have provided timely intelligence in support of the Paris Peace Conference of 1919, judging from the reaction the MID relayed to the site.[11] By virtue of its location, the site provided collection that the smaller Radio Tractor Units could not.

Houlton was remote from support in a very different way from the mobile Radio Tractor Units. The RTUs were well established in the Southern Department, and the RIS had people at department headquarters at Fort Sam Houston who could ease the logistical problems and the flow of funds. There was no similar arrangement with the Northeastern Department in Boston, and many of Houlton's frustrations were caused by the inability of Boston's quartermaster to provide what they needed, which necessitated MID headquarters in Washington having to supply small items such as paper and typewriter ribbon. Demobilization of the most experienced operators and the inability of the peacetime army to supply qualified personnel made Houlton only marginally effective after August 1919.

While Houlton used and refined some cryptologic procedures we would recognize today—

Fig. 7. Shoveling out at Houlton after the February 1919 snowstorm (records of Military Intelligence Division at National Archives, College Park, MD)

such as digraphic operator signs—the experience of the site does not seem to have influenced the Army's development of procedures and practices for the monitoring stations established two decades later. Houlton was not a failed effort, just a forgotten one. The farmhouse field station should be remembered as the Army's first attempt to establish a fixed CONUS collection facility.

Notes

1. Unless otherwise noted, all details of the Houlton operation, quotes, and referenced memoranda and documents are from the archived records of the Military Intelligence Division (MID) and can be found in Record Group 165, Entry 65, MID file series number 65, at the National Archives at College Park, College Park, MD. Specific documentation is available from the author upon request.
2. Comments about the survey exist in MID files, but the survey itself has not yet been located in those records.
3. Irving Vermilya, in "Amateur Number One," *QST* March 1917. Interestingly, Boeder's sister seems to have been a radio operator as well. According to Vermilya "he has one of the finest sisters a brother ever wanted to have, and she can send too. At least she used to, for after I knew her, my electric light meter registered at least ten dollars a month more for juice consumed in talking to her."
4. James Bamford in *The Puzzle Palace* implies the station was operational "a fortnight before the close of World War I," when "Lieutenant Arthur E. Boeder flipped a switch and brought to life America's first transatlantic eavesdropping station" (155). This conflates the visit of Sutherlin in late October and the arrival of Boeder just three days before the Armistice and contradicts official records.
5. See Hugh G. J. Aitken*, The Continuous Wave*, 253-254. Also Jonathan Reed Winkler, *Nexus*, 165. As the largest user of radio in the government, the Navy felt it had a mandate to exercise control.
6. German undersea cables and several German long-distance radio stations overseas had been destroyed by the Allies in the early days of World War I. In early 1917 Germany worked with authorities in neutral Mexico to reconstruct German long-distance telecommunications; the transmitting station at Chapultepec, a suburb of Mexico City, was part of this plan. See Jonathan Reed Winkler, *Nexus*, 166-168, for further details.
7. John Matthews Manly was a University of Chicago professor whose interest in and aptitude for codebreaking led to an association with Riverbank Laboratories and wartime employment with the MID's MI-8. It is likely that Manly was assisted, in whole or in part, by Charles J. Mendelsohn, a classics professor who was commissioned a captain and who was in charge of German codes for MI-8. David Kahn, in his article "Charles J. Mendelsohn and Why I Envy Him," has Mendelsohn breaking messages purportedly intercepted at Houlton in January and February 1918, more than nine months before the station opened. Further research is required to determine if these messages were collected by a different station and misattributed to Houlton at some point, or if these messages were collected during a survey conducted at Houlton, or even if the dates given by Mendelsohn were incorrect.
8. An April 1919 account of this shutdown by General Churchill says that it was because Houlton "on one occasion duplicated certain work being done by the Navy Department." However, it seems more likely that Churchill was describing the November shutdown.
9. Mauborgne later would serve as chief signal officer of the Army from 1937 to 1941.
10. For further discussion of the Omsk matter, see this author's *Cryptologic Almanac* item "A Grand Misunderstanding or a Turf War? The Radio Intelligence Site in Omsk That Wasn't," May 10, 2013.
11. Further research on this subject could possibly link intercepts from Houlton to specific intelligence that may have provoked the enthusiastic reaction at the MID. Intelligence reports as we know them today did not exist in this period, and the information is likely scattered across multiple files of both the MID and the Department of State.

Bibliography

Aitken, Hugh G. J. *The Continuous Wave: Technology and American Radio, 1900-1932*. Princeton, NJ: Princeton University Press, 1985.

Bidwell, Bruce W. *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941*.

Frederick, MD: University Publications of America, 1986.

Bamford, James. *The Puzzle Palace*. Boston: Houghton Mifflin, 1982.

Gilbert, James L. *World War I and the Origin of U.S. Military Intelligence*. Lanham, MD: The Scarecrow Press, 2012.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics 1851-1945*. New York: Oxford University Press, 1991.

Historical Cryptologic Collection. Records of the National Security Agency, Record Group 457. National Archives at College Park, College Park, MD.

Kahn, David. "Charles J. Mendelsohn and Why I Envy Him," based on talk given at the University of Pennsylvania on April 15, 2003. http://david-kahn.com/articles-charles-mendelsohn-envy.htm accessed March 8, 2013.

Kahn, David. *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*. New Haven, CT: Yale University Press, 2004.

Kinsley, Carl and Sobey, Albert. "Radio Direction Changes and Variations of Audibility," *Proceedings of the Institute of Radio Engineers*, Vol. 8, New York, 1920.

Military Intelligence Division Correspondence, 1917-1941. Records of the Military Intelligence Division, Records of the War Department General and Special Staffs, Record Group 165. National Archives at College Park, College Park, MD.

Records of the National Security Agency, NSA Archives, Accession 41243. Fort George G. Meade, MD.

Smoot, Betsy Rohaly. "A Grand Misunderstanding or a Turf War? The Radio Intelligence Site in Omsk That Wasn't," *Cryptologic Almanac*, May 10, 2013.

Vermilya, Irving. "Amateur Number One," *QST*, February 1917, 8-12, and March 1917, 10-15. http://earlyradiohistory.us/1917verm.htm, accessed September 2, 2013.

Winkler, Jonathan Reed. *Nexus: Strategic Communications and American Security in World War I*. Cambridge, MA: Harvard University Press, 2008.

The Thought behind High-Level Cryptological Discovery, 1930–1945

Peter W. Donovan

In this Schorreck Memorial Lecture of May 2013, some of the key Allied discoveries in World War II cryptology, particularly Pacific War cryptology, are discussed from the mathematical and psychological viewpoints.

1. Data Processing and Communications

The punched-card-based electromagnetic devices (tabulators, sorters, collators, card-punches, etc.) evolved relatively slowly in the years 1930–1963. The NSA website documents some early postwar and once-secret initiatives in using electronics in cryptology. By 1963 the electronic computer was totally replacing the tabulator machinery while data was still entered on punched cards. So the cryptologists of WWII had to make do with something like one ten billionth of modern capacity. At least they knew that the enemy encryption machines had to be simple enough to be manufactured. The output of cryptanalysis, communications intelligence, was often written out on cards and stored in this form on trestle tables. The database underlying this talk is electronic!

In 1937–1945 the capacity of communication channels was very limited. Yet data from interception could be and was superencrypted and sent to the appropriate decryption center.

2. A Junior Cryptologist of the Era

In 1946 Irene Brion wrote an account of her three years in the U.S. Army. She left it in a drawer until 1996, when it was published with the title *Lady GI*.[1] After some training she had been accepted as qualified in specialty 808, cryptologist, which was defined as follows:

- Decodes and deciphers enemy messages and cryptograms without the aid of the device or key used in preparing them.
- Using deductive reasoning and employing knowledge of the various cryptographic codes, analyzes messages and determines key to code.
- May supervise others in cryptanalysis. Must have cryptographic clearance.
- Must have training in cryptanalysis and be familiar with all types of cryptographic systems and their variations in military communications. Must possess initiative, patience and marked deductive ability.
- Should have some mathematical training and be familiar with at least one foreign language.

A high level of intelligence was needed to do anything like specialty 808 work. The U.S. Army would have had difficulty in finding potential junior cryptologists with all these skills.

Brion was initially sent to the Army base in Hollandia (now Jayapura) near the middle of the north coast of New Guinea. After the recapture of the Philippines, she was transferred to the then-new Central Bureau base at San Miguel and repatriated after the Japanese surrender. An amusing example of the relevance of initiative occurred in July 1945 when the contractor providing laundry services returned washed underclothing separated by pieces of paper that turned out to be pages of a Japanese Army codebook still in use in China. These were exploited for the last few weeks of hostilities.

Notes for Section 2

Some key work in WWII cryptology was carried out by people with much more than a familiarity with a foreign language. They utilized extreme linguistic talent. I am not qualified to discuss extreme linguistic talent. Likewise this talk does not discuss work on lower-level codes (double Playfair and the like[2]) other than to note that the FBI website reveals that it has a team working on encrypted material that occasionally turns up in criminal cases.

Central Bureau was the radio intelligence unit attached to General MacArthur's Southwest Pacific Area command and had a staff of more than 4,000 in 1945.

3. Andrew Hodges on "The Military Use of Alan Turing"[3]

Hodges' text is highly recommended and has some overlap with this talk. Four key sentences are:

> Sometimes it is blithely asserted that what one mathematician can do, another can undo. Not so: the possibilities of cryptanalysis are highly contingent on details; and even if a system is breakable in the long term, short term considerations may be of the essence. In assessing Alan Turing's place in mathematics and war, we cannot overlook the culture of mathematics itself, of which he was part. It was and is a reticent and quiet culture.

The following comes from Peter Calvocoressi of the Government Code and Cipher School (GC&CS, now GCHQ), UK:[4]

> In order to break a machine cipher, two things are needed: mathematical theory [often ad hoc] and mechanical aids. [All this applies also to the principal nonmachine ciphers too.]

Another useful quotation is due to Peter Hilton (of GC&CS):[5]

> Was it inevitable that we would be successful? I think that people like us on the other side could have stopped us being successful. I really think that it was an unequal contest, to be brutally frank. I really think that they did not have the people there who could envisage the things that we would be trying to do, and envisage the sort of errors that would naturally be made by their operators.… We helped win the war.

A combination of blunders by the other side and talent at the genius or near-genius level was not enough. There might or might not exist an appropriate "mathematical theory," and there had to be a feasible way of processing the data. At least the government was happy to pay almost any cost! The key point to be made here is that WWII cryptology depended heavily on exploitation of blunders, of which letting code books fall into the wrong hands is only the most elementary.

A principal blunder is the giving away of information that need not be given away. If it is not going to be given away, there is no need to worry about the possible consequences of giving it away! An interesting example is the serial numbering of pieces of military equipment of some type. The other side may well capture a random sample of these and be able to infer something about the total number produced. This is the German tank problem. The method is Bayesian (see section 7). Apparently Andrew Gleason of Op-20-G and Alan Turing of GC&CS discussed this matter in 1942. By 1944 the U.S. Army had a small captured-equipment intelligence unit in London. The WWII rifles I handled in 1959–1960 had dates, serial numbers, and other marks in profusion.

Another blunder is the use of 12-letter indicators (see sections 5 and 11) for the early phases of the use of the Fish encrypted teleprinter (teletypewriter). It could be and was observed that there were 25 possibilities for 11 of these letters but only 23 for the twelfth. So from this alone, it is likely that the number 23 comes into the structure somewhere. A competent mathematician then might well anticipate that other primes in the range 25 to 100 do as well.

Notes for Section 3

Various published "Tips on How to Understand Mathematics" include something like "Mathematics is not a spectator sport." Classical cryptography is not either.

Outsiders can study the "culture of mathematics" and the closely related culture of theoretical physics by both reading some biographies of appropriate senior practitioners (including of course Hodges' well-known book on Alan Turing) and talking with experienced workers in the fields. The multiauthor twenty-five-page obituary of I. M. Gelfand (1913–2009), the giant of the post-WWII mathematical community, is useful.[6]

The television series *Numb3rs* portrayed a mathematical genius who assisted the Los Angeles branch of the FBI in a sequence of varied cases. While very interesting to those in the business and also to many others, the image of a polymath (sorry!) who can provide answers to almost anything at short notice misrepresents the true situation. Turing did not solve naval ENIGMA in an afternoon.

4. Henri Poincaré's *Science et Méthode* (Paris, 1914)

The following comes from A. de Groot's *Het Denken van den Schaker*, Amsterdam, 1946, via Reuben Fine's *The Psychology of the Chess Players*:

> The chess player in analyzing a position goes through much the same kind of process that the research worker goes through in solving a problem. The chess player is in a state of continual tension and uncertainty until he finds the right move and in many cases cannot be sure what the right move is.[7]

As the chess player is subject to a time limit measured in minutes, the comparison with the research worker is not fully appropriate. It may well be argued that Andrew Hodges and Peter Donovan have been excessively influenced by mathematical research and the continuing electronic revolution from the 1960s onwards, and so their experience is not fully appropriate for the issue at hand either. But Hodges is very well qualified to comment on Turing, while I have rediscovered some aspects of WWII cryptology and picked up a trick that was overlooked at the time.

In 1908 the distinguished French mathematician (and cousin of President Poincaré) Henri Poincaré gave a talk on the psychology of mathematical discovery; this was expanded into the book *Science and Method*.[8] He related the story of one of his own major discoveries:

> Every day I sat down at my table and spent an hour or two trying a great number of combinations and I arrived at no result. One night I took some black coffee, contrary to my custom, and was unable to sleep. A host of ideas kept surging in my head. I could

> almost feel them jostling one another, until two of them coalesced, so to speak, to form a stable combination. Morning came...

This incident had a happy ending: the idea survived careful analysis in daylight. Poincaré would have been assessing prospective combinations of ideas for the elegance that correlates strongly with good mathematical innovation. The key inspiration behind my PhD thesis came during a walk taken in 1967 to get away from my desk. It was a new combination of ideas that also needed careful analysis in daylight!

Mathematical research is a long and tiring process.

Walter Isaacson's biography of Steve Jobs[9] notes that Jobs designed the Pixar Building "to make people get out of their offices, and mingle with people they might not otherwise see." This approach is evident at the Princeton, NJ, Institute for Advanced Study, which has long experience in providing the peaceful environment and appreciative company needed for serious scientific work. Not all WWII cryptology could be done on the run.

The rest of this talk looks at key aspects of seven principal examples of WWII cryptology at the highest level. There is a bias toward the Pacific Theater. Collectively those named had immense influence on the development and outcome of the war. Indeed, *we are analyzing the bottom layer of what must be seen as the most complicated human activity ever held*. This must be done without forgetting the immense sacrifice and suffering elsewhere, particularly in Eastern Europe.

Notes for Section 4

The Belgian physicist Léon Rosenfeld used the memorable phrase "the peace necessary for intense intellectual work and the stimulation of an elite audience." Most of the seven cryptological breakthroughs discussed here were facilitated by such stimulation. For example, William Friedman's report on the breaking of PURPLE (see section 9) acknowledges assistance from various members of SIS (the Secret Intelligence Service, the U.S. Army Communications Intelligence group of the time) not primarily working on the project.

The surviving records of the U.S. Navy mathematics research group in Op-20-GM indicate that it provided such an environment.

Time restraints prevent any description of other key contributions of science to WWII. But the thought behind, say, tropical medicine research, was quite different from that discussed here.

5. The Polish Cipher Bureau and ENIGMA, 1930–1939

Marian Rejewski had studied in the Mathematics Department at the University of Göttingen in the late 1920s. This had been the venue for Emmy Nöther's seminal lectures (1922) on modern algebra which were written up by B. L. van der Waerden into a book of that title.[10] So when the Polish Cipher Bureau recruited Rejewski, he had a technical background scarcely available before 1922. He also was fluent in the German language. By December 1932 he had worked out enough special-purpose theory to make the early reading of ENIGMA traffic proceed. His account "Mathematical Solution of the ENIGMA Cipher" published in *Cryptologia*[11] contains a very useful "theorem," that is, a central general fact about the matter to hand. Later two other highly talented young mathematicians joined in.

The Polish Cipher Bureau did possess "initiative, patience and marked deductive ability." The freely available commercial ENIGMA had to enter the twenty-six letters in some order into twenty-six places uniformly spaced on a circle. The standard German typewriter keyboard order was used. The military ENIGMA used a different, but unknown, order. The Cipher Bureau tried alphabetical order and it worked! The celebrated "Dilly" Knox of GC&CS was held up by this problem.

If a cipher machine such as ENIGMA were always used with the same initial setting, the output would be easy to decipher. So this setting had to be varied, and the intended recipient needed knowledge of the

Monument to Marian Rejewski in Bydgoszcz, Poland, including sculpture of the ENIGMA machine he reconstructed (Wikimedia)

current initial setting of the rotors. This information, called the indicators, was transmitted twice using two different encryptions by the standard setting for the day. Rejewski worked out how to exploit this redundant encryption to get information about the initial setting. Here the theorem mentioned earlier came in. Hugh Alexander's *Cryptologic History of Work on the German Naval Enigma*[12] calls the practice "throw-on" and explains that it enables "a system to be broken on a quite small number of messages and the enemy's use of it undoubtedly played a very large part in our success." Naval throw-on stopped on May 1, 1937.

Thinking all this through must have taken quite a while. Rejewski had to break off his research after realizing that he needed more specific knowledge of the military ENIGMA machine. When this turned up (from bribery of H.-T. Schmidt), he was able to take advantage of the bonanza.

Handling the essential theoretical work needed appropriate notation. This has been part and parcel of the mathematical process since the time of the ancient Greeks. It also needed some abstract concepts that all became easier to manage after Emmy Nöther's contribution. And it needed talent and time as well as the exploitation of any windfalls that happened to turn up. Thus the Polish work on ENIGMA depended upon the three windfalls mentioned already.

Notes for Section 5

The early common practice of using *AAA* as the 3-letter indicator made life easier for the Cipher Bureau. In modern times many computer passwords are not robust.

For the mathematician only: There are 101 partitions of 13, that is, ways of expressing 13 as a sum of numbers from 1 to 13 with repetitions allowed. Rejewski found a method of obtaining three partitions of 101 from a modest number of intercepted signals and thus working out which of 101^3 = 1,030,301 possibilities was in effect on the day. This materially helped with decryption.

It was not always easy to design a secure communications system. For example, consider the following quotation from Marian Rejewski's account:

> Finally, the order of the rotors could be changed and as a result the number of possible combinations grew, given three rotors, six-fold, and given five rotors, sixty-fold. The last of the above-mentioned complications carried an implication not foreseen by Enigma's designers. It caused each of the three [later five] rotors to be located every so often on the right-hand side of the rotor set. As a result, the method described above for reconstructing rotor N [on the right] could be applied by turns to each rotor, and thus the complete inner structure of the Enigma machine could be reconstructed.

Here we are considering a blunder, albeit a very subtle one, by the German designers. If they had brought in five replacement rotors I, II, III, IV, and V using only IV and V in the right position and only I, II, and III in the center and left, the important early work on the ENIGMA might well have been stymied. See Peter Hilton's comment quoted in section 3.

6. Initial Breaching of JN-25 at Bletchley Park,1939

An explanation of 5-digit additive cipher systems is needed. They consist of a codebook assigning a group (called a book group; these were 5-digit "numbers," initial zeros allowed) to each word or phrase to be used, and a long table of randomly chosen groups. For example, if the signal encodes into the book groups in the line immediately below:

62341 32519 03490 80394 95103 97764 81231 46825 10430 98691 66408 16894 23735 88356 86430

and the selected part of the "long table of randomly chosen groups" is:

06284 89058 57984 52622 03057 92867 61073 20100 32521 80095 22849 75756 55789 97762 49346

the groups as transmitted (GATs) are worked out by noncarrying (or "false") addition:

68525 11567 50374 32916 98150 89521 42204 66925 42951 78686 88247 81540 78414 75018 25776.

In this context the indicators convey the starting place in the random table. They should be encoded, encrypted, or concealed, and preferably two of the three. In August and September 1939 a team led by John Tiltman of GC&CS worked on the then-new JN-25A system intercepted by the outstation Far East Combined Bureau (Hong Kong and then Singapore) and broke into the indicator encryption system.[13]

Tiltman conjectured that all the code groups were such that the sum of the five digits was a multiple of three. Later the jargon *scannable* was adopted for groups with this property. Thus 24681 is scannable, as is 00243, but 76543 is not. There are 33,334 scannable groups and 66,666 others. Of course a group is scannable if and only if the corresponding number (24,681, 243 or 76,543 in our examples) is a multiple of three.

In WWII jargon, a *depth* was a set of GATs that had been encrypted by the same additive. In the JN-25 context, a *depth of ten* consists of GATs $a + x$, $b + x$, ..., $j + x$ where a, b, ..., j are all scannable. A possible decryption is any y such that $a + x - y$, $b + x - y$, ..., $j + x - y$ are all scannable. Evidently the true decryption x is one of the possible decryptions.

Those seriously interested in the decryption of JN-25 will ask, "How many possible decryptions does a randomly chosen depth of ten JN-25 GATs have?" This cannot be answered by looking in contemporary records. But it is now essentially trivial to generate 30,000 such depths using an electronic random number generator and count the number of

Mathematician Emmy Nöther. Her work on modern algebra was key to solving the ENIGMA. (Wikimedia)

decryptions of each. One discovers that while only 3 percent of depths of ten have a unique decryption, 41 percent have between 1 and 10, 24 percent have between 11 and 20, 20 percent have between 21 and 40, 10 percent have between 41 and 70, and 5 percent have more than 70 decryptions. More on this is given in section 13.

Tiltman found that a few places in the additive table had been heavily used and so sets of up to 25 signals could be placed in depth. Most depths of 25 would have exactly one decryption, which could be found by examining all 100,000 possibilities. This was tested (by co-opting all available GC&CS staff) and found to work. Tiltman's conjecture (his word was *hunch*) was confirmed.

The hunch must have been inspired by Tiltman's work in 1938 on a Japanese Army four-digit additive system. We may speculate that the 1938 achievement was similar to the breaking in 1943 of the Water Transport Code, documented in the invaluable *Central Bureau Technical Records*.[14] (The WTC was also called system 2468, after the early Japanese practice of putting this group as an unenciphered "discriminant" early in each WTC signal. Yes, this gave information away!)

In general any fixed group y can be added to all book groups (groups in the code book) and subtracted from all groups in the encrypting table without changing any GAT. So in general the cryptologists can at best recover only *nonprimary* book groups, that is, groups obtained from the correct (*primary* was the jargon of the time) by the addition of an unknown y. In attacking the WTC code book, initially a group denoting "START" was detected and provisionally taken to be 0000. Two groups that frequently occurred just before it—indeed with approximately equal frequency—could then be taken to mean Part 1 and Part 2. (Longer messages were often sent in parts.) After this the less frequent Part 3 and Part 4 were identified. It became apparent that much greater regularity in the book groups for the parts would be obtained if 6666 were added to each. Thus the primary book groups were recovered and it was observed that about half of the most common of them were divisible by 11![15] Apparently exploiting this phenomenon was not a major part of the decryption process.

Agnes Driscoll of Op-20-G obtained the primary book groups for JN-25A by a similar method but apparently failed to see how this could be used as a method of decryption. Tiltman remarked in his *Reminiscences*[16] that although not a mathematician, he had always been prepared to seek advice from the professionals. He must have brought in Turing, Welchman, and the others to consider the key issue: how to exploit this use of multiples of three in decryption work. Quite possibly this challenge brought Turing to Bayesian methods in cryptology.

Suppose, for example, that the 100 most common JN-25A book groups have been reasonably accurately identified and there is some knowledge of the frequency of occurrence of each. We further suppose that a depth of 10 is being attacked and a possible decryption has been found. Experience may well have shown that a correct decryption of a depth of 10 usually contains at least three of the fifty most common book groups. So the decrypting staff might well have been told something like "for depths of 10, if you award two points for each occurrence of a book group in the top fifty and one point for each in the second fifty, then you may accept any decryption with a score of at least 6." Such a rule of thumb could have been tested by taking randomly ten GATs from a depth of 17+ whose decryption was known and going through the decryption process on the ten.

Turing would have been left with the puzzle of finding some theoretical basis for such a rule of thumb and then making it more precise.

Notes for Section 6

Part 1 of a long signal would have been transmitted just before Part 2! Assembling the basics of the JN-25 story takes quite a while. The junior staff did not need to know the overall picture and were not told. The more senior staff were older and died before discussion of WWII cryptology became legitimate.

A lovely example of the difficulty in working out what really went on is to be found in a note made by someone in CDR Joseph Rochefort's unit at Pearl Harbor soon after the raid of December 1941. It states that after the decision to switch the unit over to JN-25B8, the Op-20-G unit Cast at Corregidor transmitted only the 100 most common JN-25B book groups. This was precisely the information needed to initiate decryption of JN-25B8!

At least when a real problem is identified, a competent mathematician who understands the data-processing methods of the 1940s can try to work out how it should have been handled and then seek evidence in the database that indeed some variant of the speculated method was in fact used.

One annoying complication was that a message like the classical "Send reinforcements. We are going to advance" would be re-ordered to read "are going to advance START send reinforcements we" before the encoding and encrypting began. And there were numerous other difficulties to confront the teams of cryptanalysts. Years of experience with traffic analysis helped.

7. Turing's Work on JN-25A and Bayesian Inference, 1939–1941

The basic idea behind logarithmic Bayesian probability theory is simple enough. Suppose we are given a set of letters and told that they are either (a) chosen randomly from an English language text or (b) chosen totally randomly. **The frequencies (per 10,000 letters) of the 26 letters in written English text are known to be as given on line 2 in the chart below.** It is clear that every A, E, H, I, N, O, R, S, or T in the given set is evidence that the origin was from English text while every J, Q, X, or Z is evidence that it was random. The theory suggests that one assigns the "weights" given in the third row to each letter and takes the sum of the weights. If this exceeds some threshold value (depending on the size of the sample), it is fairly safe to conclude that the sample came from English text.

E	T	A	O	I	N	S	H	R	D	L	C	U
1270	906	817	751	697	675	633	609	599	425	402	278	276
10	7	7	6	5	5	4	4	4	1	0	−3	−3
M	W	F	G	Y	P	B	V	K	J	X	Q	Z
241	236	223	201	197	193	149	98	77	15	15	10	7
−4	−4	−5	−6	−6	−6	−8	−12	−14	−28	−28	−32	−35

All this is an example of Bayesian inference in action. The weights are just base 10 logarithms scaled by a factor of 20 and then rounded. For example, with the letter *A*, 7 is the integer closest to $20\log_{10}(817 \times 26/10000)$. "Scaling base 10 logarithms by a factor of 20 and then rounding" amounts to the "half-deciban" usage at Bletchley Park.

Natural (for students of JN-25!) examples are the following sets of 20 letters.

```
 H  E  S  T  O  P  P  E  T  H  O  N  E  O  F  T  H  R  E  E

+4+10 +4 +7 +6 -6 -6 +10 +7 +4 +6 +5 +10+6 -5 +7 +4 +4 +10+10  total = 97.

 I  F  T  U  P  Q  Q  F  U  I  P  O  F  P  G  U  I  S  F  F

+5 -5 +7 -3 -6-32-32 -5 -3  +5 -6 +6 -5 -6 -6 -3 +5 +4 -5 -5   total = -90.
```

The first set is from "The Rime of the Ancient Mariner," while the second is obtained from the first by the simplest possible cipher: advancing each letter one place in the alphabet. The former has a Bayes score of 97 while the second shows its near-randomness by having a Bayes score of –90. This is the beginning of a process which (much of the time) distinguishes correct decryption from wrong decryption. Most desirably, the calculations can be carried out by clerks or (better still) be automated. The 1941 report by Alan Turing on such methods ultimately led to mechanized applications of it, such as in Colossus. Some quotations from the 1945 GC&CS *General Report on Tunny*, by Jack Good, Donald Michie, and Geoffrey Timms[17] are:

> The fact that Tunny can be broken at all depends upon the fact that P, χ, Ψ', K and D have marked statistical, periodic or linguistic characteristics which distinguish them from random sequences of letters.

Here "Tunny" was the code (and also jargon) for a German encrypted teleprinter. The above simple example with the English language illustrates the exploitation of statistical characteristics.

> First method, stage 1. Solution of $Z = \chi + D$.
>
> Various χ-patterns (or settings) are tried mechanically and the correct one is distinguished by the statistical properties of ΔD.

Recall that "In order to break a machine cipher, two things are needed."

> The special case of Bayes' Theorem $\mathbf{O}[H|E]/\mathbf{O}[H] = \mathbf{P}[E|H]/\mathbf{P}[E|\overline{H}] = f$ was first used in Bletchley Park by A. M. Turing. The fact that it was a special case of Bayes' theorem was pointed out by I. J. Good. The great advance of Turing consisted of the invention and application of the deciban in Hut 8. Deciban is abbreviated to db. This is defined simply as $10\log_{10}(f)$ where f is the factor defined above.

Jack Good noted elsewhere that he convinced his colleagues that the half-deciban (hdb) was a more convenient unit. Turing came quite close to inventing what would now be called Information Theory. This was pioneered after WWII by Claude Shannon of MIT. It is recorded that Shannon and Turing did meet during the latter's 1942–1943 visit to the United States.

> In cryptography one looks for needles in haystacks and the object chosen has to have a large factor in favour of being a needle in order to overcome its prior odds. It will be observed that one could take a long time to find the needle if one could not estimate the factor very quickly—hence the necessity of machines in such problems.

This general remark comes from Turing's 1941 comments in his *Applications of Probability Theory* *to Cryptology*.[18] There is every reason to interpret Turing's work in this direction, as extended by Jack Good, as being a major advance in its own right.

The JN-25 decryption process was essentially Bayesian. Given a "depth of 11" (say), that is, GATs a + x, b + x, ..., k + x, there will usually be more than one group y other than the original encrypting group x such that all of a + x - y, b + x - y, ..., k + x - y are all scannable. One can usually determine which y is correct by checking whether several of the 11 scanning groups obtained are known common book groups. This is inherently a Bayesian type process. Indeed, with depth of only about 8 much could be done. With depths of 5 or 6 the full Bayesian machinery is needed. See the *GYP-1 Bible*[19] and the notes below.

Notes for Section 7

Edward Simpson's article, "Bayes at Bletchley Park,"[20] includes Bayesian methods used on ENIGMA traffic. Both Simpson and the *GYP-1 Bible* state that "horizontal decrypting" (using known context or previously decrypted parts of a signal) played its part.

In 1945 Simpson was co-author of certain technical reports on the Japanese Naval communications problem. According to the British Archives index, checked in January 2014, items HW43/26 to HW43/43 except HW43/34 and HW 43/41 are still kept secret by GCHQ. Researching this topic is quite hard enough without artificial obstruction.

With modern computing capacity, one would not bother to round the weights: the machine is happy with 25-digit arithmetic!

As one with a limited background in statistics, I have found the Bayesian material the hardest part of WWII cryptology to enter. Simpson's recent writings and the release of Turing's account by the GCHQ have been most helpful. In retrospect, I should have put more thought into Friedman's claim that cryptology is really a branch of science, requiring total objectivity, and read more of Jack Good's writings. For more on this, see the Friedmans' book on the Shakespearian ciphers.

8. Turing's Work on Naval ENIGMA

We begin with some background knowledge. First, German Naval Intelligence had broken into British Naval Cipher Number 3. Thus the German submarines were given information about routes of shipping. Eventually ENIGMA breaks picked this up and security was restored. Second, there was another battle to be fought in the Pacific between Japanese merchant ships and American submarines. The USN had a safe enough cipher machine while a disproportionally large segment of signal intelligence in the Pacific related to Japanese merchant shipping.

Due to lack of time and expertise, no more space will be allotted to this very significant achievement by a very significant mathematician.

An example of Hilton's dictum "they did not have the people there who could envisage the things that we would be trying to do" (see section 3) arises from the Allied use of "cribs" in attacking ENIGMA. Suppose that an operator frequently sends out signals containing a known stereotyped phrase, such as INWASHINGTONYESTERDAYTHE. As ENIGMA encrypts each letter by a different letter, the possible locations for encrypted versions of this phrase may be found and then treated as potential cribs.

The cryptologists would, with help from special machines, search for initial settings of the ENIGMA that would encipher the stereotyped phrase into an appropriate segment of the intercept. Security would have been enhanced by bringing in a few errors and extra letters randomly, yielding something like INUUASHINGTENYESTARDAYKTKE. As Hilton remarked, "they did not have the people there who could envisage the things that we would be trying to do."

9. Reconstruction of the "PURPLE" Diplomatic Cipher Machine

Friedman’s report of October 1940 (online at cryptocellar.org) contains some, but far from all, technical details. This extract illustrates the sophistication of WWII cryptology. Frank Rowlett was a major player in this achievement.

> 7. In all, the plain texts for parts of some 15 fairly lengthy messages were obtained by the methods indicated above, and these were subjected to the most intensive and exhaustive cryptanalytic studies. To the consternation of the cryptanalysts, it was found that not only was there a complete and absolute absence of any causal repetitions within any single message, no matter how long, or between two messages with different indicators on the same day, but also that when repetitions of three, or occasionally four, cipher letters were found, these never represented the same plain text. In fact, a statistical calculation gave the astonishing result that the number of repetitions actually present in these cryptograms was less than the number to be expected had the letters comprising them been drawn at random out of a hat! Apparently, the machine had with malicious intent—but brilliantly—been constructed to suppress all plain text repetition. Nevertheless, the cryptanalysts had a feeling that this very circumstance would, in the final analysis, prove to be the “undoing” of the system and mechanism. And so it turned out![21]

One lovely example of giving away something that did not need to be given away was the transmission from the Japanese Embassy in Washington of PURPLE encryptions of letters prepared within the U.S. State Department. Copies were made available to Friedman’s team! Another clue was to be found in the probable use of standard telephone switching apparatus in the PURPLE machine. After 18 months a full reconstruction of the unseen Japanese machine was achieved.

By 1945 decryption of PURPLE had provided transcripts of invaluable reports from the Japanese ambassador in Berlin. It is likely that these were of greater interest in Washington than in Tokyo.

10. Fish and Bill Tutte

Tutte records that John Tiltman had been able to take two versions of the same message processed through an unknown encrypting teletype to obtain a run of about 4,000 columns of “dots” and “crosses.” This was of itself a serious achievement, but no further progress had been made for three months. A piece of the output would have looked like the following:

```
● ● ● × ● × × × ● × × × ● ● × ● × ● × ● × × × × ● ● ● × ● × ● × × ● ● × × × × ●
● ● × ● × ● × ● × ● ● × ● ● ● ● ● × ● ● × × ● ● ● ● ● ● × × × ● × × × ● × ● ● ●
● × × ● ● × ● × ● × × ● ● × × ● ● × ● ● × × ● × ● ● × ● × × ● ● × ● ● ● ● × ● ●
● × × × × × × × ● × × ● ● ● ● × ● ● ● × ● ● ● ● × ● × ● × × × ● × ● ● × × × × ×
× × × ● ● ● × × × ● × ● ● ● ● × × ● × × × × ● ● ● × ● ● ● ● × × ● ● × ● ● × × × ×
```

[This sample was generated randomly by my symbolic algebra facility. Those who seek patterns in it will be disappointed: randomness tends to create illusions of clustering and patterns.]

Tutte discovered that the first row tended to repeat every 41 places. There was a discrepancy which almost had periodicity 43. This led to all of the Research Group searching for near-periodicities in the other four rows. Eventually the whole structure (twelve rotors all up) was deduced. The periodicities involved were 41, 31, 29, 26, 23, 43, 47, 51, 53, 59, 37, 61. As these twelve numbers have no common factors, the encrypting machine will repeat itself only after 41 × 31 × 29 × 26 × 23 × 43 × 47 × 51 × 53 × 59 × 37 × 61 = 16, 033, 955, 073, 056, 318, 658 steps. Tutte had the idea that it might be worthwhile checking if each individual row repeated after a fixed number of entries. This started him on his way to great things.

Notes for Section 10

This is the best documented of all the great WW II cryptological triumphs: Bill Tutte gave a full account in *Fish and I* in 1998.

Tutte recounted that there was a second encrypted teletype system that GC&CS could not exploit even though it was quite similar to the Fish system that was read with such effect.

> There was another teletype machine that we called "Sturgeon," used by the Luftwaffe. It mixed the five impulses more thoroughly than did Tunny. There was a permutation of the five impulses in the course of key construction. ... Though we found out how Sturgeon worked we failed to think of a way to apply that knowledge to the reading of messages.[22]

11. The Indicators of Cipher 2468

The key reference here is part G of the invaluable *Central Bureau Technical Records*, page 17.

> The effort applied towards reading the Water Transport System, a higher echelon army shipping system, was well repaid. Resulting intelligence concerning shipping movements was extremely valuable. ... A large part of the original work on the Water Transport problem was contributed by CBB. [Joe Richard must be credited with designing and then examining tabulator printouts and then making the key original observation.]
>
> It took much time and concentrated effort until it was found that by using the relationship between two digits of similar plain text and dissimilar cipher text it was possible to recover a non-primary square. [Probably Abe Sinkov and T. G. Room were heavily involved.]

It also took me much time and concentrated effort to work out what a nonprimary square was! In this case some of the work was carried out in Arlington, VA, and some in Ascot, Queensland, Australia, with frequent exchanges of progress.

Water Transport signals were basically less complex than JN-25 ones and so the step from decryption to decoding was easier.

The underlying mistake here had much in common with that exploited by Rejewski in 1932. As with the ENIGMA indicators, the algebra of permutations was extremely relevant. Intelligence from the WTC not only helped identify the locations of Japanese Army outposts but also helped the USN use its submarines to attack Japanese merchant ships.

Notes for Section 11

The solution to the Water Transport indicator decryption problem seems to have survived only in the form of my reconstruction, published in *Cryptologia* in 2006. I had the advantage of knowing that there was indeed a solution which involved first constructing a "nonprimary square" and then getting what was really needed, the primary square. At least one thought was there from the start: I knew what a 10 × 10 Latin square is.

The whole project was done off and on for a few weeks with finally a "rush of blood to the head" resulting in a process that worked. It is most unlikely that the original method was much different. Having worked out the method, I was able to run a computer program that worked out how many intercepts were needed to enable this sort of calculation to be made.

It is far from clear what, if anything, is the common mathematical basis of Rejewski's early work on the ENIGMA indicators and the CBB-AHS work on the Water Transport indicators. Sinkov must have been informed of the throw-on (terminology of section 5) at Bletchley Park in February 1941. Indeed, the German Army was using this unsound redundant encryption until April 1940.

The November 2009 issue of the *Notices of the American Mathematical Society* contains an obituary of Andrew Gleason. The segment on his work for Op-20-G in WWII and for the NSA in the early 1950s mentions the exploitation of yet another throw-on: that of Seahorse ENIGMA.[23]

12. The Characteristic Distribution and Mamba

The *characteristic* $\chi(g)$ of a group g such as 24681 is defined to be the sum *taken modulo 10* of its digits. So $\chi(24681) = 1$, $\chi(00243) = 9$ and $\chi(76543) = 5$.

Well, someone in Op-20-GM (quite probably Marshall Hall) had the idea that it might be worthwhile working out the numbers of scannable groups having each of the ten possible characteristics. I cannot explain how this brain-wave happened. Turing and the GC&CS mathematicians missed this one. The numbers are:

(0) 3247 = 9.7% (1) 5875 = 17.6% (2) 1780 = 5.3%
(3) 1780 = 5.3% (4) 5875 = 17.6%
(5) 3247 = 9.7% (6) 925 = 2.8% (7) 4840 = 14.5%
(8) 4840 = 14.5% (9) 925 = 2.8%

This has "marked statistical characteristics" which are not shared by "random sequences of" groups. In the immortal words of Sherlock Holmes, "You know my methods, Watson." Here the methods are ramifications of the Bayesian methods of section 7. Anything in the Op-20-G archives mentioning Mamba is about exploiting this phenomenon.

I repeat from section 3: A principal blunder is the giving away of information that need not be given away. JN-25 was giving away information *about the encryption* all the time. As Winston Churchill remarked in his account of the Battle of Midway in *The Second World War,* "The importance of secrecy and the consequences of leakage of information are here proclaimed."[24]

Notes for Section 12

The characteristic was known to play a role in handling some other additive cipher systems. A trained cryptologist of the era would know the identity $\chi(a + x) - \chi(b + x) = \chi(a) - \chi(b)$.

Marshall Hall was in Op-20-G and later became a very distinguished algebraist. His autobiographical comments note that he made substantial contributions to the cryptanalysis of both Japanese and German material. Some information about the latter is available in the obituary of Andrew Gleason mentioned in section 11.

A puzzle for the mathematicians is to check that the difference (taken modulo 10) of two randomly chosen scannable groups takes the 10 possible values with probabilities as tabulated below:

Difference	0	1 or 9	2 or 8	3 or 7	4 or 6	5
Probability (%)	13.05	9.06	7.54	12.47	10.94	6.94
Weights	30	−11	−32	25	10	−41

To determine whether two reasonably long portions of intercepted JN-25 signals are in alignment, one works out the differences modulo 10 of the characteristics of corresponding GATs, scores 30 for each 0, −11 for each 1 or 9, etc., and adds up these scores. If there is an alignment, the total should be positive! The "Hall weights" of the Op-20-G era would have been something like these. And the mathematicians may work out where the 30, –11, –11, etc., came from.

A serious challenge for those with mathematical background is as follows. Suppose you are given 20 depths of 8 GATs in a new 5-digit additive cipher. It is believed that the codebook either (a) uses only scanning groups or (b) uses randomly chosen groups. Find a method of determining whether (a) or (b) holds. Your data look like the following:

— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —
— — — — — — — — — — — — — — — — — — — —

13. Modern Computer Calculations

As already noted twice, modern electronic computing facilities can be used to carry out experiments with certain aspects of WWII cryptology. The idea is that one uses data satisfying the known constraints but otherwise random. The outcome can be noted. This process can be repeated lots of times and the average outcome noted. This provides a method of checking whether one's current views on what went on are reasonable.

For example, suppose we choose a depth *d*, one of 6, 8, 10, 12, 14, 16, 18, 20, and 22. It is assumed that the Japanese Navy randomly chooses *d* scannable 5-digit groups and encrypts them by false adding the same randomly chosen group. The average number of possible decryptions of such a depth of *d* are tabulated below.

$d = 6$	320	$d = 8$	73	$d = 10$	22
$d = 12$	8.6	$d = 14$	4.4	$d = 16$	2.9
$d = 18$	1.9	$d = 20$	1.4	$d = 22$	1.2

And so we come to the point. Much less information (occurrence of common book groups or the context of a message) is needed to produce an acceptably high probability that a proposed decryption in the JN-25 situation is correct than for a general 5-digit additive cipher, for which the number of decryptions is 100,000! Here is the basis of the almost total victory of the U.S. Navy in the intelligence war in the Pacific. Claude Shannon's *Communication Theory of Secrecy Systems*[25] is generally relevant.

The various books on military blunders of the twentieth century all overlook JN-25.

Suppose we know something about what is now called information theory and measure information in hdb. A 5-digit group gives 100 hdb of information while a 5-digit scanning group gives about 90.5 hdb. So JN-25 uses 100 hdb to carry 90.5 hdb and somehow has 9.5 hdb of redundancy. This should at least indicate that there is some prospect of the enemy exploiting the use of only multiples of three as book groups.

14. A Highly Contrived Example for Mathematicians Only

The following list of 144 JN-25 GATS will be called *List A*.

00001	00010	00022	00100	00112	00121	00202	00211	00220	01000	01012	01021
01102	01111	01120	01201	01210	01222	02002	02011	02020	02101	02110	02122
02200	02212	02221	03001	03010	03022	03100	03112	03121	03202	03211	03220
10000	10012	10021	10102	10111	10120	10201	10210	10222	11002	11011	11020
11101	11110	11122	11200	11212	11221	12001	12010	12022	12100	12112	12121
12202	12211	12220	13000	13012	13021	13102	13111	13120	13201	13210	13222
20002	20011	20020	20101	20110	20122	20200	20212	20221	21001	21010	21022
21100	21112	21121	21202	21211	21220	22000	22012	22021	22102	22111	22120
22201	22210	22222	23002	23011	23020	23101	23110	23122	23200	23212	23221
30001	30010	30022	30100	30112	30121	30202	30211	30220	31000	31012	31021
31102	31111	31120	31201	31210	31222	32002	32011	32020	32101	32110	32122
32200	32212	32221	33001	33010	33022	33100	33112	33121	33202	33211	33220

If List A is considered as a depth of 144 GATs, an electronic calculation shows that there are 8363 decrypting groups. This may be used to produce a depth of 8363 GATs with 144 decrypting groups. The first 9 rows (108 groups) of List A form a new List B which has 9558 decrypting groups. Alternatively, the last 9 rows (108 groups) of List A may be used as a new List C which has 9557. This line of thought can be used to produce, seventy years too late, a rather more secure JN-25!

Thus there are subtle aspects of JN-25 not yet properly understood. But, as said in section 3, if information is not going to be given away, there is no need to worry about the possible consequences of giving it away!

Afterword

This paper assumes some general familiarity with the history of World War II, which has considerable overlap with the general history of the United States from 1935 to 1950. A globe (rather than a paper map) helps you understand the sequence of events. Some modern DVDs usefully complement the numerous good books available.

Declassification has made it possible for a modern mathematician who puts a lot of work into the matter to assess the technological and mathematical achievements behind the Allied signals intelligence successes that at the very least shortened the war by as much as two years.

References

1. Irene Brion, *Lady GI* (Novato, CA: Presidio, 1997).
2. National Archives and Records Administration, RG 467, Box 936, Item 2699.
3. Andrew Hodges, “The Military Use of Alan Turing,” in *Mathematics and War*, ed. Bernhelm Booß-Bavnbek and Jens Høyrup (Basel: Birkhäuser, 2003), 312-325.
4. Wladyslaw Kozaczuk and Jerzy Straszak, *Enigma: How the Poles Broke the Nazi Code* (New York: Hippocrene, 2004), 270.
5. David Joyner and David Kahn, Interview with Peter Hilton for “Secrets of War,” *Cryptologia* 30 (2006), no. 3, 236-250.
6. Vladimir Retakh, “Israel Moiseevich Gelfand,” *Notices of the American Mathematical Society* 60 (2013), nos. 1, 2; www.ams.org.

7. Reuben Fine, *The Psychology of the Chess Player* (1967; repr., New York: Ishi Press, 2009).
8. Henri Poincaré, *Science et Méthode* (Paris: Flammarion Science Press, 1913).
9. Walter Isaacson, *Steve Jobs* (New York: Simon & Schuster, 2011).
10. Bartel van der Waerden, *Moderne Algebra* [lectures by Emmy Noether] [in German] (Berlin: Springer, 1931); [in English] (New York: Ungar, 1949).
11. Marian Rejewski, "Mathematical Solution of the Enigma Cipher," *Cryptologia* 6 (1982), no. 1, 1-18.
12. C. Hugh O'D. Alexander, *Cryptographic History of Work on the German Naval Enigma*, The National Archives, Kew, UK, HW 25/1 (c.1945); www.ellsbury.com/gne/gne-000.htm.
13. GC&CS (UK) file TNA HW 8/102.
14. *Central Bureau Technical Records*, Part G, 17-18 [available online via Recordsearch at www.naa.gov.au].
15. National Archives and Records Administration, RG 457, Box 926, Item 2649.
16. National Archives and Records Administration, RG 457, Box 1417, Item 4632.
17. Jack Good, Donald Michie, and Geoffrey Timms, *General Report on TUNNY with Emphasis on Statistical Methods*, 1943, National Archives, Kew, UK, HW 25/4, HW 25/5.
18. Alan Turing, "The Applications of Probability to Cryptography," 1941, National Archives, UK, HW 25/37.
19. GYP-1 Bible, National Archives and Records Administration, RG 38, Commander Naval Security Group library, Boxes 16, 18.
20. Edward Simpson, "Bayes at Bletchley Park," *Significance* 7 (2010), no. 2, 76–80.
21. William Friedman, "Preliminary Historical Report on the Solution of the 'B' Machine," 1940 PURPLE History, cryptocellar.org.
22. William T. Tutte, *Fish and I*, transcript of a lecture given at the University of Waterloo (June 19, 1998), cryptocellar.web.cern.ch/cryptocellar/tutte.pdf.
23. Andrew Gleason obituary, *Notices of the American Mathematical Society*, Nov. (2009), 1236-1267.
24. Winston S. Churchill, *The Second World War* (London: Houghton Mifflin, 1975).
25. Claude Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal* 28 (1949), no. 4, 656-715.

Contributors

Cathleen L. Civiello, Ph.D., ABPP, is board certified in clinical psychology and in organizational and business consulting psychology. A corporate psychologist-manager, Dr. Civiello has been with NSA since 1988 and a senior since 1999. She has spent her career designing, implementing, and managing programs that effectively address some of NSA's most difficult leadership, security, and counterintelligence challenges. She is a graduate of the NSA Senior Technical Development Program and has served on the Senior Technical Review Panel for more than a decade.

Peter Donovan was a member of the Mathematics Department faculty of the University of New South Wales in Sydney, Australia, for many years. Now semiretired, Dr. Donovan has published notable contributions in algebraic geometry, algebraic topology, representation theory, and homological algebra. Currently his interests are modular representation theory, geometrical physics, and the insecurity of Japanese naval ciphers in World War II. He has published three papers related to the latter in *Cryptologia*. One was the first account of the insecurity created by the Japanese Navy's use of only multiples of three in its principal series of operational ciphers in the Pacific War, very important in setting up the ambush at Midway. The second paper reconstructed the breaking of the indicator encryption of the Water Transport Code. The third dealt with the Mamba phenomenon that was discovered and exploited by the U.S. Navy cryptological team. See also "Alan Turing, Marshall Hall and the Alignment of WWII Japanese Cipher" in *Notices of the American Mathematical Society*, March 2014.

David A. Hatch is currently the NSA Historian and also technical director of the Center for Cryptologic History (CCH). He has worked in the CCH since 1990. From October 1988 to February 1990, he was a legislative staff officer in the NSA Legislative Affairs Office. Previously, Dr. Hatch served as a Congressional Fellow. He earned a B.A. degree in East Asian languages and literature and an M.A. in East Asian studies, both from Indiana University at Bloomington. Dr. Hatch holds a Ph.D. in international relations from American University.

Erin Higgins is professionalized as a cryptologist, although she also enjoys just hand-solving old-fashioned ciphers. During her career, she undertook a six-month detail to the Center for Cryptologic History to study Renaissance cryptology and, as a consequence, "fell down the rabbit hole of German humanism."

Betsy Rohaly Smoot came to the National Security Agency in 1983 as a traffic analyst. She has worked in analytic, staff, and managerial positions at Fort Meade and overseas. She joined the Center for Cryptologic History as a historian in October 2007. Her particular research interests include World War I, the Cold War, and terrorism. Mrs. Smoot received a B.A. from Mary Washington College with a double major in geography and economics and an M.S. in strategic intelligence from the Defense Intelligence College.

Nancy Welker came to NSA with an A.B. degree in physics from Mount Holyoke College and completed M.S. and Ph.D. degrees, also in physics, from American University while conducting research in basic and applied physics. She has served in multiple technical leadership roles at NSA. Dr. Welker chairs the Senior Technical Review Panel, a major duty of which is oversight of the Senior Technical Development Program.

CENTER FOR CRYPTOLOGIC HISTORY