Rare Books

The Rare Book Collection

The National Cryptologic Museum display offers a look at some of the most rare and interesting books ever published on cryptology. The publications date from the 16th to the early 20th century and represent authors from all over Europe.

The NSA Rare Book Collection has existed in one location or another since at least the 1930s. The first volumes were probably acquired by William F. Friedman and his associates during the early days of the Army's Signal Intelligence Service. The collection grew during World War II, when it was possible to obtain almost anything if it was "for the war effort."

It is likely that these volumes were purchased not for their physical value, but for their worth as early code and cipher manuals. Evidence of their use as training and research tools exists in the books themselves, for example, in the pencil notations and from clues that the books were available for loan from the SIS Library.

The collection was subsequently housed for many years in the NSA Language Library and Cryptologic Collection, where it was protected from the public handling it had suffered in earlier days. When the Language Library was absorbed by the NSA Main Library, the Rare Book Collection was transferred as well. Then, in 1984 the rare books and the Cryptologic Collection were moved to the Office of Archives and History. Although apart from the library system, it was still under the aegis of Information Resources Management.

The NSA Archives has tried to halt some of the deterioration of these books resulting from aging and early misuse. With proper archival and preservation methods, old glued book pickets and date due slips, adhesive stickers and such are removed. The original leather bindings of the books have been cleaned and restored. Some of the damage is permanent, but future wear is being prevented by several means, including individual custom-made acid-free boxes for storage.

Following is some additional background information about some of the volumes and their authors.

- *Polygraphia (1518) Johannes Trithemius (1462-1516)*
- *Opus Novum (1526) Jacopo Silvestri (born about 1500)*
- *Subtilitas de Subtilitate Rerum (The Subtlety of Matter) (1554) Girolamo Cardano (1501-1576)*
- *Giovanni Battista Porta*
- *Hieroglyphics, the Rosetta Stone, and Cryptology*
- *From Grammaire Egyptienne by Champollion*

- *Rare Book Exhibit Selected Bibliography*

Polygraphia (1518) Johannes Trithemius (1462-1516)

Abbott Johannes Trithemius, the author of the first printed book on cryptology, was considered one of the intellectuals of his day. Unfortunately, he was also considered to be an occultist, and even in league with the "darker forces," which did much to destroy his reputation as a scholar.

Born in Trittenheim, Germany, in 1462 and known simply as Johannes, the future abbot had a love for learning. His grim stepfather, although wealthy, had no use for intellectual pursuits, and did not approve of Johannes' desire for higher education. On his own, Johannes appealed for entrance to the University of Heidelberg, where the chancellor was so impressed that he accepted the youth and even arranged to waive the tuition fees.

While at the university, Johannes and two others formed the Rhenish Literary Society and chose Latin and Greek names for themselves. Johannes chose Trithemius, after his home. It was the name by which he was known from then on.

A chance visit (to escape a snowstorm) to the 436-year-old Benedictine abbey of Saint Martin at Spanheim, Germany, impressed the young Trithemius so much that he soon entered the novitiate there. Only a short time after taking his final vows, he was elected abbot. (David Kahn - in The Codebreakers - says the reason for this was probably either that the monks recognized his brilliance or that they thought that he would be too young to enforce discipline.) Whatever the reason, he stayed on as abbot and soon published a book of sermons which was instantly successful. He continued to write as his fame and reputation for genius grew. His chronological list of about 7,000 theological works by over 950 authors earned him the title "Father of Bibliography."

Some of his other writings began to be questioned, however. *Steganographia*, ostensibly a book on secret writing, was filled with names and images of planetary angels, along with instructions on how to employ the angels for thought transference and other mystical uses. Acquaintances and friends who saw the manuscript were horrified; the book was not finished.

Legends began to surround the abbot. A reputation as a "wonder worker" with magical powers grew and followed him and was probably even abetted by him, as he was hardly known to be modest or shy of publicity. In fact, believing that his practices were wholly Christian, Trithemius did not even deny the tales, except to say that there was no demonic influence in his life or work.

While Trithemius was away on a trip, the monks at Saint Martin's mutinied. This was apparently as a result of the abbot's reputation as a magician and the widespread negative talk about the *Steganographia* manuscript, which was being hand-copied and circulated throughout Europe; many people were fascinated by the "secrets" the book was supposed to contain.

Trithemius did not return to Spanheim. Instead, he obtained a transfer to the monastery of Saint Jacob in Wurzburg, where he was elected prior. There, in 1508, he began the writing of *Polygraphia*, a series of six books devoted *in actuality* to cryptology. The work was finished very quickly, but was not published at once. Abbot Trithemius continued to write and study at Wurzburg, where in 1516 he died.
Two years later, in 1518, descendants of the university chancellor who had guided Johannes' intellectual progress paid for the publication of *Polygraphia*. Although public opinion still held firmly to the view that Trithemius was working with the black arts and many copies of the book were destroyed, *Polygraphia* survived to be acknowledged as the first published volume on cryptology. In *An Historical and Analytical Bibliography of the Literature of Cryptology*, Joseph Gallard wrote:

The strange and bizarre terms and characters which Trithium [Trithemius] interspersed throughout the composition of the work soon caused him to be suspected of dealing in the black art… This suspicion continued all during the course of the 16th century …. However, a number of more judiciously-minded readers of the work now came to the belief that Trithium had done nothing more serious than to use the conventionalised language of the magicians.

Opus Novum (1526) Jacopo Silvestri (born about 1500)

Opus Novum, the second book printed on cryptology, was written by Jacopo Silvestri and was published in 1526. Little is known about Silvestri apart from what he himself wrote in the preface to *Opus Novum*. He wrote that he was a citizen of Florence and was staying in Rome when an epidemic struck and he moved into a rural area. A friend who visited him there engaged him in a conversation about ancient methods of writing, which led to a discussion of cryptology. His friend urged Silvestri not to withhold his knowledge of a subject that could be so useful to others, and so he wrote his little book. (It is indeed little, only 88 pages.) Philip Arnold, in an article in *Cryptologia* entitled "An Apology for Jacopo Silvestri," supposes that since a copyright privilege at the end of the book appears from Pope Clement VII, in which the Pope calls him "beloved son," Silvestri may have been a cipher clerk in the Vatican.

It is interesting that this is not a book written for scholars; after each section in Latin there is a section in Italian ("the vulgar tongue"). Silvestri's title page, translated by Philip Arnold, delightfully illustrates his purpose and his intended audience.

Title page, *Opus Novum*

A new work, exceedingly useful to lords of castles, commanders of armies, spies, defenders of the fatherland, travellers abroad, merchants, soldiers, inventors, and all princes devoted to diligence and learning, for correctly writing and interpreting in cipher the Latin, Greek, Italian, and as many other tongues as you will.

A New work, most useful to gentlemen merchants, and to every other sort of person, which teaches how to make many kinds of ciphers according to the practice of ancient and modern lords and princes of the world. And furthermore teaches another kind of cipher, newly discovered, which cannot be read by any human device without knowledge of its solution, explaining that knowing one is not harmful to another one. And further the present work teaches how to decipher many kinds of ciphers by rules, and by other secret methods of deciphering the said ciphers, whether they be made in the Latin tongue, common Greek, or in any other language of any other country whatever, which work is written in the Latin language and repeated in the vulgar tongue.

Silvestri's cipher wheel

Silvestri's book is not often mentioned by historians, being always overshadowed by Trithemius , but Arnold proposes that this is largely because the book had only one edition and is so rare that few have had access to it. Arnold also quotes F. Wagner's *Studien zu einer Lehre von der Geheimschrift*, written in 1887.

. . . the author proposes distinctly more practical and simpler methods than his predecessor Tritheim [Trithemius]. Scarcely any influence of the theories of the latter on practice is noticeable… while the cipher methods suggested by Silvestri have survived in only slightly altered form in the ways and means employed by the modern diplomatic corps. From that alone his little book acquires unique significance.

Subtilitas de Subtilitate Rerum (The Subtlety of Matter) (1554) Girolamo Cardano (1501-1576)

Girolamo [Geromino, Jerome] Cardano was known more as a mathematician and scientist than as a cryptographer, but his works included some new cryptologic ideas. Cardano was born in Naples in 1501 and had ambitions to become a physician, but his illegitimate birth would not allow him that profession. Instead, he became a medical astrologer, and then a mathematician, scientist, and prolific writer. In 1536 he was finally admitted to the College of Physicians. He was indeed a fine man of medicine, affecting cures that some called miraculous. (Those who felt the cures were miracles may have included Cardano, who fancied himself a prophet and magician.) In *The Codebreakers*, Kahn proposes that Cardano had "an overwhelming desire simply to be remembered - not even caring whether the memory was of good or ill." Publishing 131 books in his lifetime, plus an additional 111 left in manuscript, Cardano wrote on such diverse topics as mathematics, astronomy, astrology, physics, chess, gambling, the immortality of the soul, consolation, cures, dialectics, death, Nero, gems and colors, Socrates, poisons, air, water, nourishment, dreams, urine, teeth, music, morals, and wisdom.

One of his pioneering studies was in the field of games and probability, in which he developed equations, and in turn advanced theories on the subject. This is, in fact, what Cardano is best known for.

Cardano was the first cryptologist to put forth the autokey method of encipherment. Although his method was faulty, his idea of using the message itself as the enciphering key was sound. Later cryptographers perfected the method, and Cardano was not to find his fame for this cryptologic discovery. Instead, he became famous for a system of steganography, called the Cardano grille.

The Cardano grille for secret writing was simply a sheet of stiff material with irregularly placed rectangular holes which was placed over the writing paper. The secret message was written in the holes, the grille was removed, and an innocuous message was filled in around the secret message to disguise its being there. To read the message, an identical grille was placed over the writing. A major fault in the system was the awkwardness in phrasing the surrounding message often led to suspicions of a secret message within. Despite this, a number of countries used the Cardano grille in the 1500s and 1600s for diplomatic correspondence.

Giovanni Battista Porta

Giovanni Battista Porta was another famous cryptographer who lived in the 16th century. Born in Naples, Porta was a well-rounded physician, mathematician, and scientist. When he was only 22, after taking the "grand tour" of Europe, Porta published *Magia Naturalis*, a study of natural phenomena, oddities, and curiosa, which became extremely popular. He formed the first scientific society, the Accademia Secretorum Naturae [or Accademia dei Secreti], in which a group of men interested in natural magic met in Porta's home and conducted experiments. The members called themselves the Otiosi (Men of Leisure). The society was, however, called forth on charges of occultism, and after clearing his name with Pope Paul V, Porta closed the association. The "magic" of the association was actually no more than parlor tricks. Later, he was a founder and vice president of another scientific society, of which Galileo was a member.

Porta's writings continued to evidence his interest in magic, along with studies on the relationship of human physiognomy to animal characteristics (which had an influence on the profession of criminology), meteorology, the refraction of light, pneumatics, the design of villas, astronomy, astrology, and the improvement of memory. He also published fourteen prose comedies, two tragedies, and one tragicomedy. An expanded edition of *Magia Naturalis* was translated and printed at least twenty-seven times. Porta's work on cryptology, *De Furtivia Literarum Notis*, was published when he was twenty-eight. The book encompassed all the cryptologic knowledge of the time. Porta dealt with historical ciphers, linguistic peculiarities, and modern ciphers, he introduced the first digraphic cipher (in which two letters are represented by one symbol) and published other "new" cipher systems, including his own cipher disk.

Fletcher Pratt, in his book *Secret and Urgent: The Story of Codes and Ciphers*, wrote that Porta's work was the talk of cryptographers in Rome and that his accurate frequency tables and "safe from attack" cipher were considered remarkable. The use of the cipher itself, however, was tricky and impractical, requiring both sender and receiver to carry key tables with them, a dangerous practice. Pratt further states, "though his book earned for Porta the title of 'Father of Modern Cryptography', it does not appear that his system was ever much used anywhere."
In *The Codebreakers*, however, Kahn quotes Dr. Charles J. Mendelsohn, a Renaissance scholar:

He was, in my opinion, the outstanding cryptographer of the Renaissance. Some unknown who worked in a hidden room behind closed doors may possibly have surpassed him in general grasp of the subject, but among those whose work can be studied he towers like a giant.

Hieroglyphics, the Rosetta Stone, and Cryptology

The mystery of ancient Egyptian hieroglyphics has held the imaginations of scholars ever since the Persians and then the Greeks overran Egypt. Because the script fell into disuse after the fall of the pharaohs, its meaning was soon forgotten.

By the Middle Ages, the discovery of a manuscript written by a 4th century author known as Horapollo set the standard as the (inaccurate) authority for centuries. From this point on, most believed that the hieroglyphic symbols formed a truly "picture" language in which a bird represented a bird, or some aspect of bird-life, such as flight.

In the 17th century, Athanasius Kircher, a Jesuit, put forth a theory based on extensive study. He was the first to state that the Coptic language, which was still in use, was the most recent form of the hieroglyphic language, but written in Greek characters. This was a major turning point in the search, but Kircher's other theories on the subject were found to be worthless.

It was in 1799 in the city of Rosette that an Egyptian laborer working for Napoleon's conquering French army discovered the slab of black basalt that would be later named the Rosetta Stone. The stone was clearly divided into three sections. The bottom third of the stone was written in Greek, the top third in hieroglyphics, and the middle section in Demotic, a form of Egyptian "shorthand."

When the French surrendered Egypt to the English in 1801, the stone was given to Britain. Today it resides in the British Museum in London.

The importance of the stone was immediately recognized. It was suspected that the two lower portions of the stone said the same thing - the hieroglyphics needed only to be translated. The puzzle was far from being solved, however.

The ancient Greek portion was translated by several highly regarded linguists. The text concerned Pharaoh Ptolemy V in the year 196 B.C. It listed all of his titles and the gifts he had bestowed upon his people (i.e., money and corn to the temples, remission of taxes, etc.) In return, the Egyptian priests celebrated the Pharaoh by making his birthday a festival, erecting golden statues of him in every temple, and copying *the priests' decree in Egyptian and Greek* and placing a copy with every statue.

Now it was known for certain that all three scripts contained the identical text. Some of the most learned and respected men of their times attempted to solve the mystery. The first major breakthrough was made by a British physician, Thomas Young. He made some progress with the Demotic script and then tackled the hieroglyphics. Young first assumed that characters within a cartouche were names of royalty. He next thought that as the Demotic language seemed to consist of letters that stood for sounds, perhaps the hieroglyphics were simply more elaborate forms of the same figures. He tried his theory on the name Ptolemy and by using its Greek sounds and studying a similar cartouche on the ceiling of the temple of Karnak, proved his theory to be correct. Young gave up soon after, however, claiming not to have found any more alphabetic elements.

From *Grammaire Egyptienne* by Champollion

Finally, Jean-Francois Champollion took up the challenge. Champollion had been convinced since he was a child that he would someday read the writings of the Egyptians. In preparation, he studied Sanskrit, Arabic, Persian, Hebrew, and Coptic. A bilingual text from an obelisk contained an appeal to Ptolemy and Cleopatra (the children of the Ptolemy in the Rosetta Stone.) Using cryptanalytic techniques (letter counts and cribbing), he was able, using the characters in their names, to cross check and correctly identify letters as symbols of individual sounds.

After this triumph, it was only a matter of months before Champollion had nearly completed the translation of all the royal names. Armed with this and his knowledge of Coptic, he was able to refine and complete his work.

Champollion died less than ten years afterwards. Others would later translate writings yet to be discovered and would clear up some of the problems he had been unable to solve. But Champollion died with the knowledge that he had been the first man to truly unlock the mysteries of the Pharaohs.

Rare Book Exhibit Selected Bibliography

- Arnold, Klaus, ed. *Johannes Trithemius: In Praise of Scribes (de Laude Scriptorum)*. Lawrence, Kansas: Colorado Press, 1974.
- Arnold, Philip M. "An Apology for Jacopo Silvestri," *Cryptologia*, Vol. 4, No. 2, 1980.

- Arnold, Philip M. "A View of Renaissance Cryptography - A Book Review," *Cryptologia*, Vol. 8, No. 2, July 1984.
- Center for Cryptologic History. *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, 1992.
- Galland, Joseph. *An Historical and Analytical Bibliography of the Literature of Cryptology* . New York: AMS Press, 1945.
- Grun, Bernard. *The Timetables of History: A Horizontal Linkage of People and Events*. New York: Simon & Schuster, 1975.
- Haldane, R. A. *The Hidden World*. New York: St. Martin's Press, 1976.
- Kahn, David. *The Codebreakers*. New York: Macmillan, 1967.
- Kruh, Louis. "A Xerograph of a Classic," *Cryptologia*, Vol. 3, No. 1, 1977. (Review of a University Microfilms reprint of a French translation of Trimethius' Polygraphie.)
- Ore, Oystein. *Cardano, the Gambling Scholar*. New York: Dover Press, n.d.
- Pratt, Fletcher. *Secret and Urgent: The Story of Codes and Ciphers*. Garden City, NY: Blue Ribbon Books, 1942. (Original copyright 1939)
- Shulman, David. *An Annotated Bibliography of Cryptography*. New York, London: Garland Publishing Co., 1976.
- Shumaker, Wayne. *Renaissance Curiosa*. Binghamton, New York: Center for Medieval & Early Renaissance Studies, 1982. (Contents: John Dee's "Conversations with Angels"; Girolamo Cardano's "Horoscope of Christ"; "Johannes Trithemius and Cryptography"; George Dalgarno's "Universal Language")
- Smith, Laurence Dwight. *Cryptography: The Science of Secret Writing*. New York: W.W. Norton & Co., 1943.

Produced by The Center for Cryptologic History.

For more information contact:

- National Security Agency
- ATTN: Public Affairs Office
  -
  - 9800 Savage Rd., Suite 6248
  - Ft. George G. Meade, MD 20755