Rochford's Cipher: A Discovery in Confederate Cryptography

BY DAVID W. GADDY

Unclassified

Details the decryption and historical background of a Confederate message in a grille cipher system (Rochford's Cipher) previously unknown to the cryptography of the U.S. Civil War period.

The "Mason and Slidell affair" played a significant role in Anglo-American relations during the American Civil War.[1] Captured on the high seas by an energetic U.S. naval officer, James M. Mason and John Slidell, former U.S. Senators who had become envoys of the fledgling Confederacy, were subsequently released and allowed to continue on to London and Paris. There these "commissioners" provided Richmond with a diplomatic presence and assisted in the extensive effort to procure warships, ordnance and other much needed supplies abroad. Much of their correspondence has been preserved and published in the *Official Records of the Union and Confederate Navies in the War of the Rebellion.*[2]

Buried in an obscure place in a volume of that work, published in 1922, is an inventory of "Papers of the Confederate State Department ('Pickett Papers')." Among the items listed is one with the intriguing description "Cipher tables used in correspondence with Mason, Slidell, Mann and others."[3] Now, a half century later, those materials have been located, resting safely in a folder in the Manuscript Division of the Library of Congress, seemingly untouched since they were deposited there. What they reveal sheds little light on Mason and Slidell, but illumines instead a clandestine activity and yields a type of cryptosystem previously unknown to the cryptography of the Civil War period.

When the folder was examined in the summer of 1970 it was found to contain a few scraps which suggested the familiar Vigenere cipher widely employed by the Confederates. In addition there were slips of paper bearing what appeared to be cipher, and, most important of all, detailed instructions for something termed "Rochford's Cipher." A quick scanning of the last item revealed a description of a rotating grille cipher—a type of cryptography not encountered before in the literature of the Civil War. The unique character of the "find" alone was enough to make one immediately suspicious. No other examples of transposition had been found in official Confederate usage, let alone a system of such obvious complexity as this one appeared to be. What proved it to have been Confederate?

Aside from the descriptive label on the folder, there was nothing. The writing, the ink and the paper appeared to be of the proper vintage, but nothing actually said "Confederate." Since time was pressing, we made a copy of the instructions for later study, and, against the possibility that the encrypted texts reflected the cipher, made copies of them as well.

Subsequent study of the materials revealed that the cipher texts comprised one long message and a postscript, but in two copies, each in a different hand. The instructions, which had seemed straightforward at first, produced real problems as an attempt was made to understand and follow them. The handwriting, some of the terminology, and, in a few crucial places, simply the legibility, became stumbling blocks, but the real barrier was the growing realization that, even if the texts did employ the cipher, the keyword was unknown (barring some fluke such as the use of the same one employed for illustration in the instructions!). While the instructions warranted further study, the texts would have to be tackled as a cryptanalytic problem. Meanwhile there was the question of the name. Who, or what, was Rochford? Seemingly the simplest of the problems, it was the last to yield.

Assuming various possible spellings of the name, we checked the standard Civil War sources. They produced nothing. A survey of available cryptologic literature—too superficial a search, as it later turned out—was likewise fruitless. Biographical and geneological works confirmed the name, or variations, in the British Isles, but no identification in the time and context sought could be made.

The bleak outlook ended in the spring of 1971. A chance conversation with a friend led to a re-examination of the instructions and ultimately to the solution of the enciphered message. Since the instructions were available before the analysis of the texts, it might be helpful in understanding the task which followed if they were read now (see Fig. 1):

"Method of Constructing and Using 'Rochford's Cipher'"

> "The patterns sent were on half size Scale—Rule a sheet of paper on double the Scale with heavy black lines exactly as the one sent was ruled. Paste this paper on a common pine board, of the proper size. In the narrow border at the top, bottom & on each side number one and abreast of such squares from 11 to 30. This will constitute a *writing board*."

(The description given is that of a 20 × 20 matrix with the squares numbered 11-30 on the top, bottom and sides. To continue with the instructions, . . .)

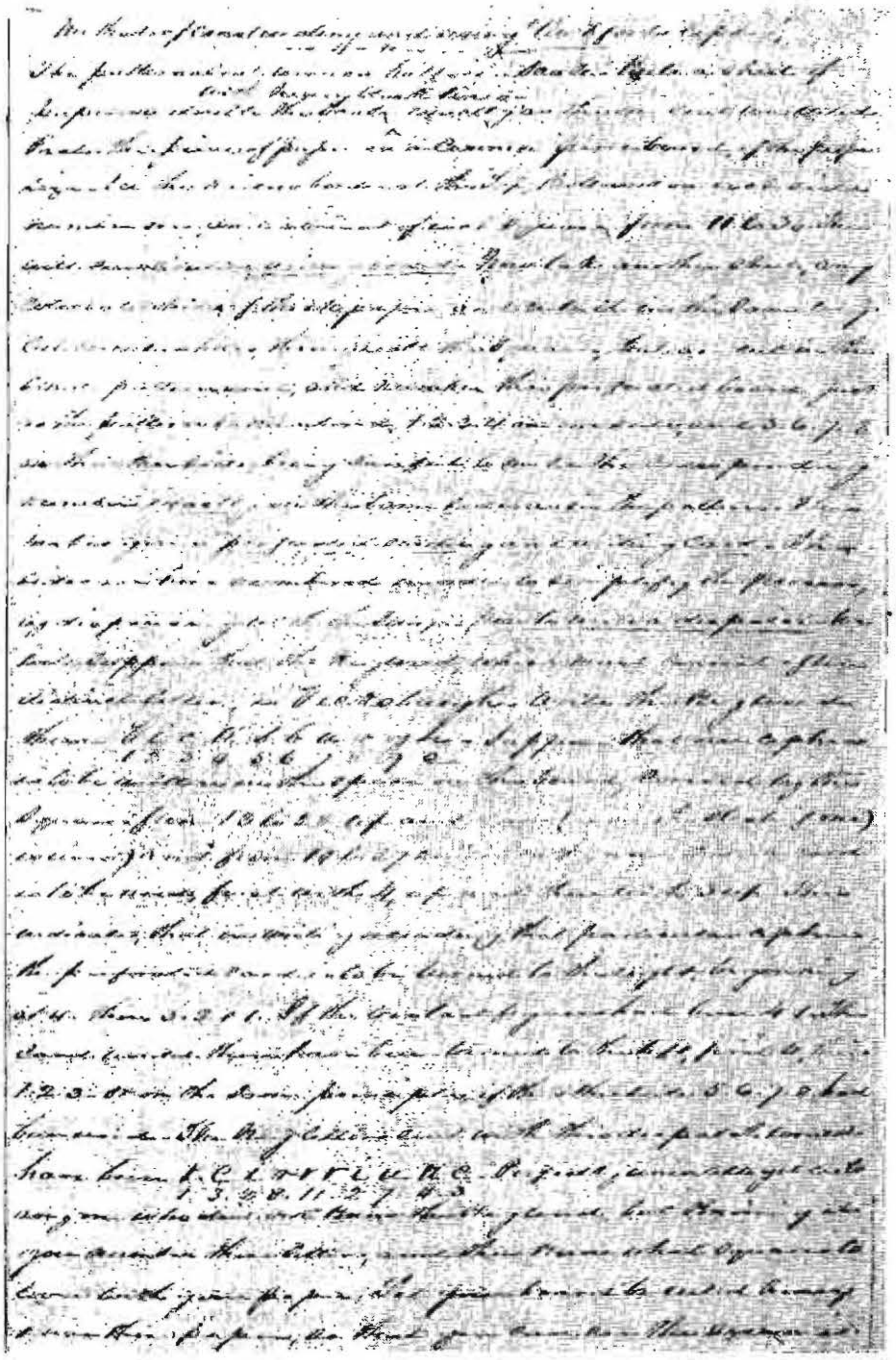

Fig. 1—The Method of Constructing and Using "Rochford's Cipher"

[redacted]

> "Now take another sheet, any color but white, of thick paper, and rule it in the same way. Cut circular holes through all the squares, that are cut in the small pattern sent, and number this perforated board, just as the pattern is numbered, 1 . 2 . 3 . 4 on one side, and 5 . 6 . 7 . 8 on the other, being careful to make the corresponding numbers *exactly* on the same sides as in the pattern. This makes you a *perforated reading and writing card*."

(In other words, using a different-colored heavy paper, prepare a grille the same size as the "writing board," with the openings cut out to correspond with the "pattern sent." The grille is then numbered, the first side numbered 1 at the top, 2 at the side, 3 at the bottom, 4 at the side; the reverse side accordingly numbered 5–8. The patterns, unfortunately, were not found with the instructions.)

> "The sides are here numbered in order to simplify the process, by dispensing with the strap."

("The strap" was to remain a mystery until later.)

> "*Now to write a dispatch*—We will suppose that the Keyword, which must consist of ten distinct letters, is Vicksburgh—write the Keyword thus—
> V I C K S B U R G H—Suppose that our
> 1 2 3 4 5 6 7 8 9 10
> cipher is to be written in the space on the board, covered by the squares from 13 to 28, up and down (or on the strap if one is used) and from 11 to 27 horizontally, and that the card is to be used, first with 4 up, and then with 3 up. This indicates, that in writing or reading, that particular cipher, the perforated card is to be turned to the right, beginning at 4. Then 3 . 2 & 1. If the last two figures had been 4 . 1 the card would have then have been turned to the left, first 4, then 1 . 2 . 3—or on the same principle, if the other side 5 . 6 . 7 . 8 had been used. The key letters sent with this dispatch would have been
> V C I R VV IU K C—Perfectly unintelligable [sic] to any one who did not
> 1 3.2 8 11.27.4.3
> know the Key word, but knowing it you number these letters, and this shows what squares to cover with your paper. Let your board be ruled heavy & use thin paper, so that you can see these squares."

(Note that the letters in the keyword are numbered in direct sequence, rather than in their order of appearance in the alphabet, but the explanation is fairly clear. The "key letters sent" passage refers to a hypothetical message in which an *indicator* would be placed at the end of the message to tell the recipient the dimensions of the matrix and the order of placing and turning the grille, i.e., 13-28 for the vertical, 11-27 for the horizontal; the final two digits giving the rotation of the grille—descending order, the grille turns to the right, ascending order, it turns to the left.)

> "*To write a dispatch*—Secure a piece of thin paper covering the exact squares you intend to use, remembering that the up and down numbers are always first, the horizontal numbers next & the two numbers, first to be used on the perforated card last, making ten in all. The paper being secured to the board, & on the proper squares, with four draftsman's pins, place the perforated card

> exactly covering the entire board & with the 9th number of the Key letters on top. Then begin on the left, going to the right, and put a letter (or word, if you use words) through each of the holes. Having filled every hole, coming over the paper in regular order, turn the card with the 10th number of the Key letters up, repeat the process until every hole has a letter in it, then turn the card in the same direction, to its 3rd & 4th sides, filling each hole. You will then find a letter in every square. If you find you have skipped a hole, & consequently one square lacks a letter, put in a X there. If your dispatch is not all written, turn the sheet over, secure it as before, and repeat the process, 'till all is written. Page the sheets used 1.2.3 &c. Do not send the dispatch in that form, as it will give some clue, but copy the letters off plainly & distinctly, in regular order from left to right, and at the bottom put the Key letters VCIRVVIUKC—*To read a dispatch*—Place numbers *under the Key letters*, taken from the *Key word* "VICKSBURGH" and you have the squares to be used. Cover those squares with a piece of paper, the exact size. Let the letters be called out to you, write one in each square from left to right, as they occur, till all are filled. If an X occurs, put it in its place—Place the board with the 9th figure up, and reading off throughout the holes, some one else writing down the letters as you call them off, into words. It will readily be perceived that the thousands of changes of which this process is capable, make it utterly incomprehensible, without the Key word."

As noted earlier, only two dispatches were available for analysis, a long, three-page message and a postscript. These were in two copies, in different handwriting and with different corrections noted, both of which were of assistance in ascertaining the correct text. In size they were small, approximately 3 × 5 inches, as though concealment might have played a role in their transmission (see Fig. 2).

Different indicators were used in the dispatch and the postscript, EE IH EI MR NY in the former and EE MN EL MI IM in the latter. An initial assumption was that the same key word had been used for both, as implied by the repeated letters E and M. Based on the instruction for the use of the key word and the dimensions (11–30) of the fixed matrix, it was obvious that the value of the initial letter of each of the first four digraphs would be 1, 2 or 3, and that the value of the initial letter of the second and fourth digraphs would progress over the value of the initial letter of the first and third. The values of the ninth and tenth letters would then be in consecutive order, ranging 1-4, 5-8, or in reverse order.

Let E = 1.

```
(a)  EE IH  EI MR    N    Y
     11 30  13 28   (6)  (5)
(b)  EE MN  E L   MI I    M
     11 2(6)1(4)  23 3    2
```

Then M should be 2 and I=3, since (*a*) is the long message. H would be 10, since the dimensions of the matrix are 11–30. On this line of reasoning a hypothetical keyword was developed:

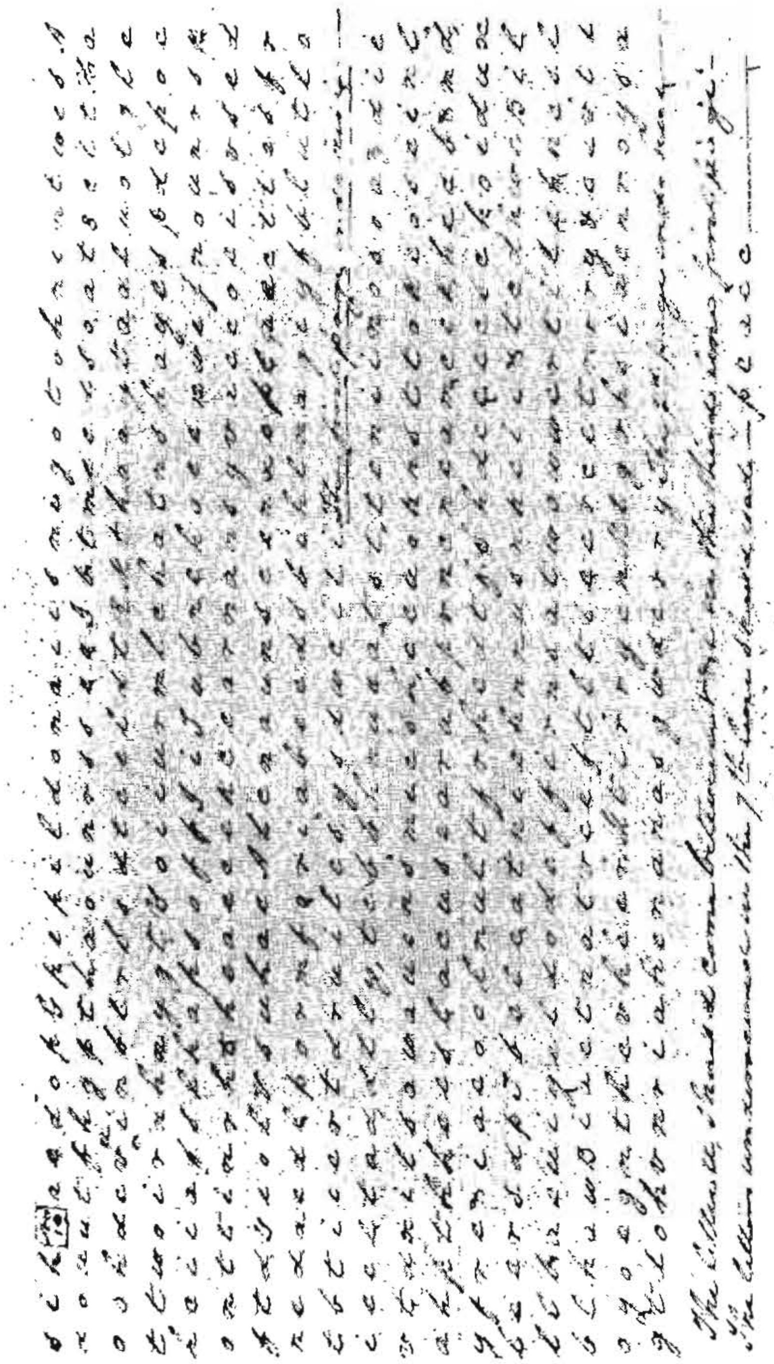

Fig. 2A—First Version of Cipher Text

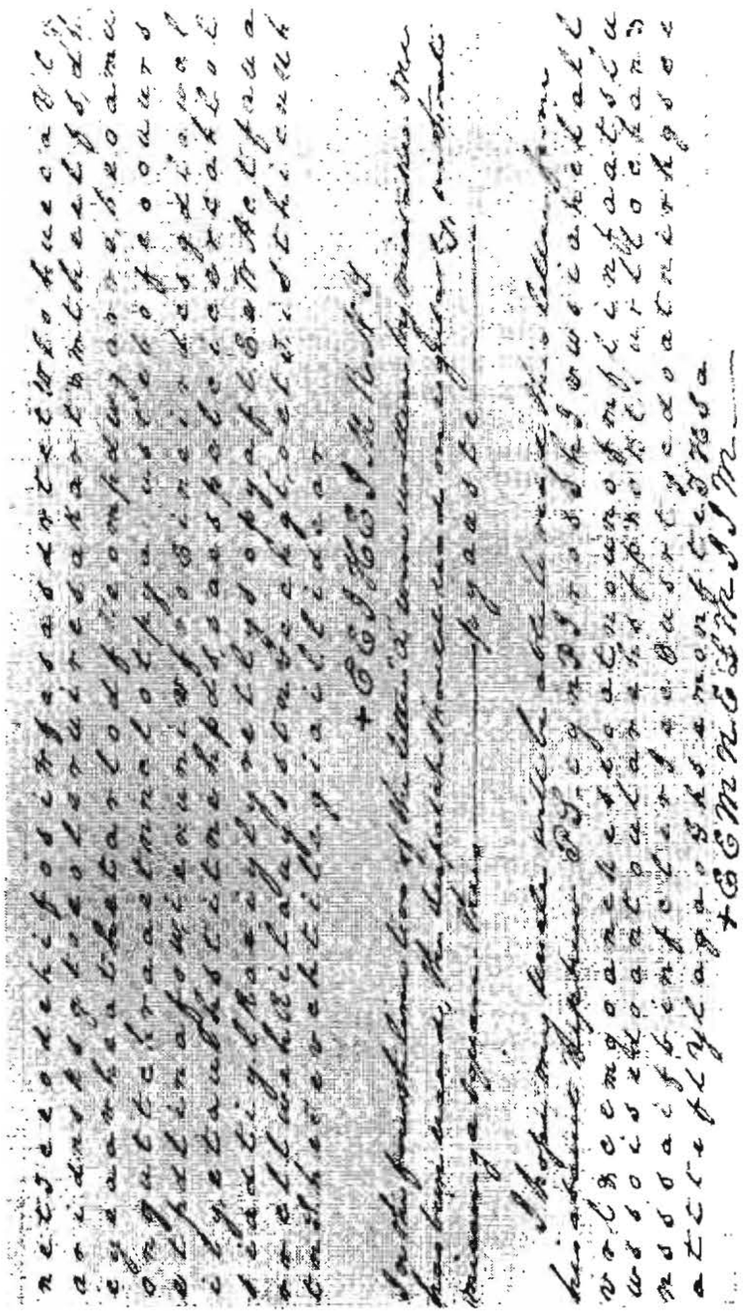

Fig. 2A, continued

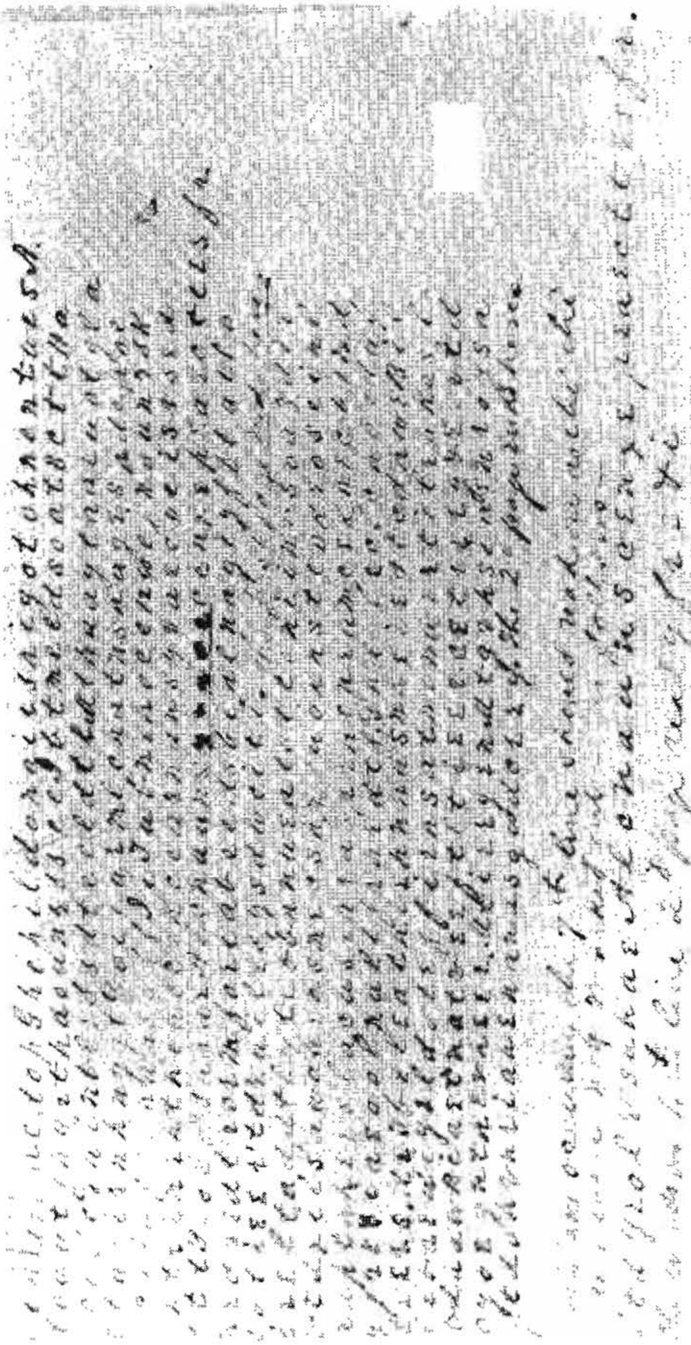

Fig. 2B—Second Version of Cipher Text

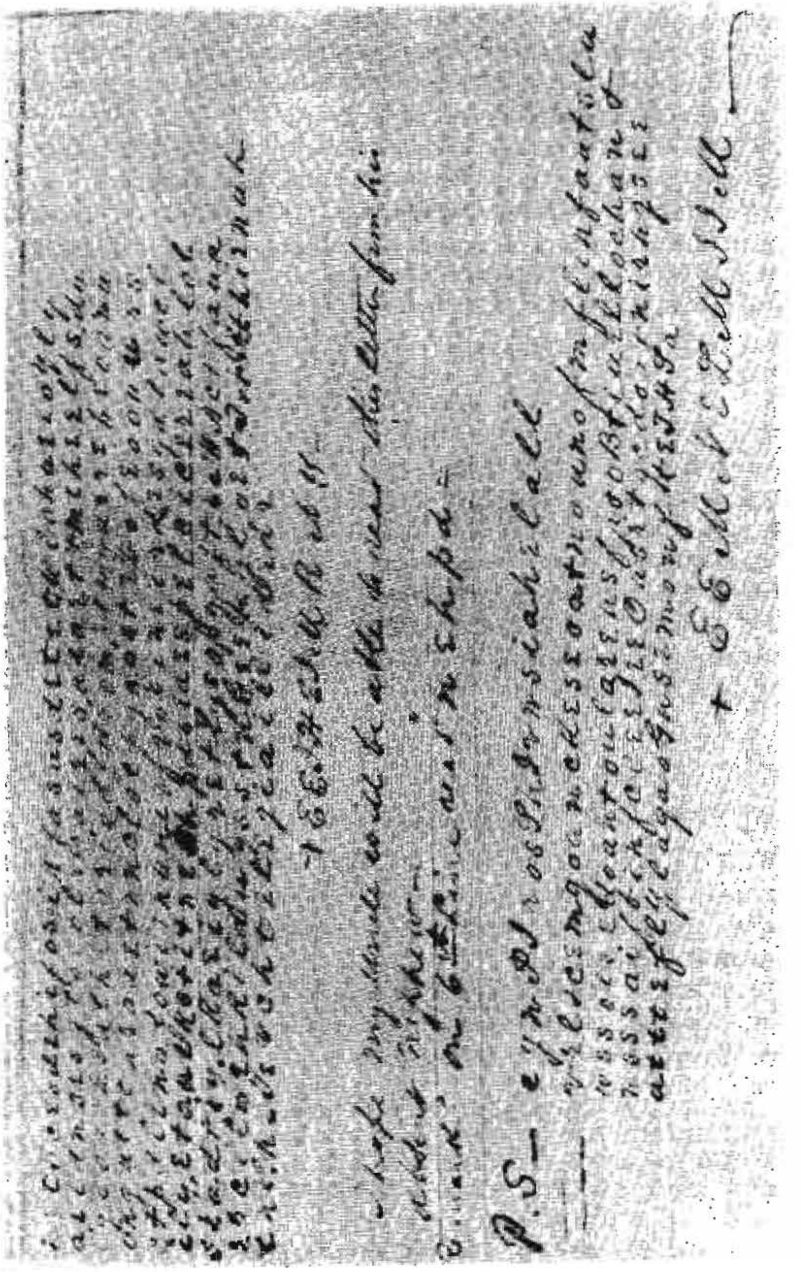

Fig. 2B, continued

```
1 2 3  4    5     6   7 8 9 10
E M I (L)  (Y)   (N)  O R T  H
```

(A person's name? The only Confederate named North who came readily to mind did happen to have been overseas in the British Isles. That was James H. North, a Confederate Naval officer sent to purchase ships and supplies for the Confederacy.

Each page of the message (*a*) contains 320 letters. The page appeared to be 20 deep, so the width would be 16, thus making R = 8. The P.S. (*b*) contains 160 letters, but neither dimension was fixed, leaving N, L and Y undetermined. Anagramming for a name or a place led to trying L = 4, Y = 5, and N = 6, EMILY NORTH.

These values satisfy the conditions:

(*a*) a matrix 20 × 16 (320) and the grille rotating to the right, first 6 up, then 5 up;

(*b*) a matrix 16 × 10 (160), with the opposite side of the grille used, also rotating to the right: 3 up, 2 up, 1 up, then 4 up.

The message consisted of three pages, each containing 320 letters. In effect, this was like having three messages of the same length. Based on the note in the instructions to "repeat the process" if the message was longer than one page, it was logical to assume the same size matrix and the grille used in the same manner for each page, giving a depth of three. In addition, due to the symmetry of the matrix when the grille has rotated to the third position, the openings would be reversed—top, left to right and bottom, right to left:

```
row  (1)  (11 12) 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 (29 30)
                           X                 X              X
                     X              X                X
row (20)  (30 29) 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 (12 11)
```

and similarly, for positions two and four; therefore, the depth could be increased to six with four levels of text, one for each position of the grille. (Note that the text of one stream will read backwards when matching columns.)

The recovery of the text was thus reduced to matching respective columns. Because of the nature of a grille transposition, the sequence of positions was relatively close, e.g.:

Pos	27	29	31	36	41	46	53	57	61	63	70	76	81	86	90	
Page 1	T	H	E	S	U	P	R	E	M	E	C	O	U	R	T	
2	I	N	S	I	X	W	E	E	K	S	S	H	E	C	A	(N)
3	W	O	U	L	D	G	R	E	A	T	L	Y	H	E	L	(P)

Pos	294	292	290	285	280	275	268	264	260	258	251	245	240	235	231
Page 1	U	B	Y	L	D	I	P	A	R	S	E	C	N	A	V
2	Y	R	E	V	E	T	E	C	O	T	R	E	T	T	E
3	U	E	H	T	H	T	I	W	R	A	W	Y	L	L	A

With the entire text reconstructed, recovery of the grille became a relatively simple process, but because the message used only a portion of the entire 20 × 20 matrix, the two columns on the left and right of the grille were not used in the first placement of the grille and had to be recovered on the second placement (after we rotated it from 6 to 5). We constructed the matrix, using the designated portion, 11-30 down and 13-28 across, as follows:

										6													
		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
	11			S	I	H	19	A	E	D	O	P	G	P	E	P	I	L	D			11	
	12			O	N	A	I	I	S	N	I	G	O	T	O	H	N	E	N			12	
5	13			T	W	E	S	A	D	O	U	U	T	F	H	G	P	T	H			13	7
	29			I	Y	F	B	L	U	T	L	O	T	B	T	I	E	E	R			29	
	30			T	D	R	U	I	L	E	S	Y	S	D	W	C	I	T	I			30	
										8													

The cipher text was then written into the matrix, left to right. The 6 was placed on top, for that was the designated position in which the grille was to be placed initially.

Following the reconstructed text, beginning with #19 (which could be a message number, and thus a logical beginning), we blocked the squares indicated by the text:

#19 GLASGOW AUG. . . . ITTERLY OI

Now construction of the matrix was begun:

										6													
		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
	11						X						X					X				11	
	12					X			X			X			X							12	
5	13				X			X			X					X						13	7
	29			X						X					X			X				29	
	30					X			X			X		X			X					30	
										8													

As the grille was rotated to the right, 5 came up on top, and since columns 11, 12, 29 and 30 were not used in the previous position (6), it was necessary to repeat the above process to reconstruct the missing rows 11, 12, 29, and 30. (Then *row* 13 became what had been *column* 13.)

										5													
		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
	11			S	I	H	19	A	E	D	O	P	G	P	E	P	I	L	D			11	
	12			O	N	A	I	I	S	N	I	G	O	T	O	H	N	E	N			12	
8	13			T	W	E	S	A	D	O	U	U	T	F	H	G	P	T	H			13	6
	29			I	Y	F	B	L	U	T	L	O	T	B	T	I	E	E	H			29	
	30			T	D	R	U	I	L	E	S	Y	S	D	W	C	I	T	1			30	
										7													

The reconstructed text continued: DI SAPPOINTED TH. . .Y BUT IT IS T. Again rotating to the right, 8 on top, the text continued T HE OPINION OF TH. .LL BE DEC. . . And again rotating to the right, 7 on top, DEC IDED IN THE SUP. . . FOR US WI. .

At this point the first page of the text was complete, and the grille could be reconstructed, except for the four corners, which were not used. (The entire grille contains 100 open cells, of which 96 were located.) Pages 2 and 3 were then read merely by writing the cipher text in the matrix of the proper size, placing the grille in the designated positions and extracting the letters appearing in the opening as the original recipient would have done. (Since the postscript used the reverse side of the grille placed at position 3, back of 7, the cipher text was written in the matrix 11-26 vertical and 14-23 horizontal—16 × 10— placing the grille with the 3 on top and extracting the plain text as before. Rotation was again to the right, 3, 2, 1, then 4, completing the postscript.

The enciphered text had been unlocked and the secret it had held for a century was revealed:

Glasgow
#19 August 8

Honbl. S R. Mallory,

Yours of June 12 just received. You cannot feel more bitterly disappointed than I do of the delay at getting my ship off The work on her advances rapidly but it is the opinion of those best advised that until the decision in the case of the ALEXANDRA shall be decided in the Supreme Court, to which an appeal has been taken, any vessel suspected of being for us will be seized as soon as launched & all the expense & delay of the law inflicted on her. Mr. Mason has written to advise me to keep her back & my friends here think it will be far better to get everything ready but not launched until the Supreme Court decides. The builders will have everything so advanced that in six weeks she can be off. She could be launched in two weeks. This delay is like death to me but cannot be avoided with the hostility of Earle [sic] Russel [sic], the vigilance of the Yankees & the fear of war among the people universally, especially war with the U.S. The late disasters to our arms have added greatly to our difficulties already great. A change in the tide of war would greatly help our cause just now, in England especially.

Respectfully,

Geo. T. Sinclair

(The following portion was written "in the clear," unenciphered:)

> "I hope that my Uncle will be able to read this letter from his absent nephew."

The deciphered postscript then follows, with the letters "P.S." in the clear:

```
P.S.
I will consult with Bulloch & if I can get the
money I shall make a nominal sale & transfer to
the flag of Hanover & get off as soon as possible.
Our disasters have confused our finances greatly.
                                            G.T.S.
```

Mallory, Sinclair, Bulloch—not diplomats, but hardworking members of the Confederate Navy Department: Stephen R. Mallory was Secretary of the Navy in Richmond. Although not as well known as James D. Bulloch, who contracted for the famous raider CSS ALABAMA, and who wrote a book about clandestine Confederate supply efforts in Europe, Lieutenant (later Commander) George Terry Sinclair, Sr., was also a Confederate States Navy officer. He had been sent to Europe as a member of a CSN Procurement Commission under Cdr. Samuel Barron, whose headquarters were set up in Paris. Sinclair operated in the British Isles. His mention of the ALEXANDRA helps to establish a date, for the ALEXANDRA, launched in March, 1863, at Liverpool, became a test case in U.S. efforts to contest the legality of England's permitting the construction and outfitting of warships for the Confederacy. She was seized in April, 1863, and not released until April, 1864. Sinclair's pet project, a ship known variously as PAMPERO and CANTON, was to become the TEXAS in the CSN. She was launched in November, 1863, at Glasgow, and seized the following month. The cipher message is therefore to be dated 8 August 1863; among the "disasters" to which it refers may well have been, by odd coincidence with the sample key word used in the instructions—Vicksburg.

Confederate usage was thus confirmed, and a missing fragment of history restored, for a search of the published naval records failed to disclose the message or any evidence that it had been broken before.

One question still remained: why "Rochford's cipher"? An intensified search in the library produced the answer at last. It was a cipher set forth by William H. *Rochfort*, "late Lt. Col. of Artillery in the service of HMFM Donna Maria II," in *A Treatise Upon Arcanography; or a New Method of Secret Writing, Defying Discovery or Detection, and Adapted for All Languages; Together with Working Plates and Directions for Use*, published in London in 1836. The misspelling of Rochfort's name, as well as certain differences in terminology and modifications in practice, suggest that the writer of the Confederate instructions was not working directly from the book. The peculiar word "strap" which caused puzzlement in the instructions was cleared up by the book, however, for it turned out to have been one of the devices prescribed by the inventor, who also apparently collected royalties on patented grilles and writing paper, sold openly in stationery stores.

How extensive was the use of "Rochford's cipher" by the Confederates is not known. Numerous examples of encrypted Confederate texts appear in the *Naval Records*, most of them by James H. North, a colleague of Sinclair, but they employ the common dictionary code.[5] Could the complexity of the procedures for use have doomed Rochford's cipher to a few exchanges? Looking back from the vantage point of a century, and recalling the boasts of Yankee telegraphers and "codebreakers" concerning their success with Confederate ciphers, one can only wonder. . . what if they had been confronted by "Rochford"? Or were they?

REFERENCES

[1] See Evan John, *Atlantic Impact, 1861* (London: William Heinemann Ltd., 1952).

[2] U.S. Navy Department, 31 vols. (Washington, 1894-1927), hereinafter cited as NR, with reference to series, NR, volume and page, e.g., II NR 2, 123 refers to vol. 2 of series II, page 123.

[3] II NR 3, 22. A. Dudley Mann was another Confederate commissioner to Europe. (To anticipate a possible question, no, the Pickett of the Papers was not the Pickett of the Charge.)

[4] Philip Van Doren Stern, *The Confederate Navy: A Pictorial History* (New York: Bonanza Books, 1962), p. 34. A sketch of *Alexandra* is found on page 166 and Sinclair's ship, *Pampero* (intended to be CSS *Texas*), is on page 167. See also U.S. Navy Department, *Civil War Naval Chronology* (Washington, 1961-1966), Part VI, pp. 195-196 and 314. In a letter of 1 August 1863, North to Bulloch (II NR 2, 474-475), North laments the fall of Vicksburg, as well as Union advances on the coast around Charleston, S.C.

[5] Terminology is of little help: Mallory to North, 29 July 1862 (II NR 2, 229) refers to North's dispatch in cipher, yet the reference is evidently to one which employed the dictionary code (*op. cit.*, 206).