19 August 2011

Update to 8 June 2011 Press Release

In June 2011, the National Security Agency (NSA) declassified and released to the National Archives and Records Administration (NARA) over 50,000 pages of historic records. In a press release issued 8 June 2011, NSA highlighted an early publication on cryptography, a record on the book *Kryptographik Lehrbuch der Geheimschreibekunst* from 1809. This update provides more detailed information on that particular cryptography record.

What is the cryptographic record released to NARA?

The record consists primarily of information from *Kryptographik Lehrbuch der Geheimschreibekunst*, a book written by Johann Ludwig Klüber and published in 1809. The Klüber book is still cited as a noted reference book on the history of cryptography. The record released by NSA appears to have been created by a German cryptographer who excerpted sections of information from the Klüber book, presumably as a reference, and hand-wrote an example applying a cryptographic technique from the Klüber book.

Why does NSA have documents from German cryptographers?

The record is a Target Intelligence Committee (TICOM) document. During the closing months of World War II (WWII), British and American authorities carried on extensive research of the Axis cryptologic organizations and their operations during and prior to WWII. TICOM was one of these joint research efforts. TICOM teams were sent into the field behind the frontline to recover cryptologic documents, material and equipment and to conduct interrogations. Researchers used this recovered war-time information in an effort to exploit cryptologic targets in Germany and German-occupied territories. TICOM intelligence analysis activity of the recovered information continued past 1950.

If NSA was created in 1952, why does the Agency have records from WWII?

The U.S. Army Security Agency (ASA) was one of the American entities involved in TICOM. In 1949, the code-breaking organizations of the Army, Navy and Air Force were merged into the Armed Forces Security Agency (AFSA). After NSA was founded in 1952, many of the cryptographic records from ASA and AFSA went to NSA. This included many TICOM documents.

Why was a German document captured in World War II considered classified?

The cryptologic relationship between the U.S. and U.K. governments was treated as classified after WWII, to include information about the initial cooperative efforts, such as TICOM. Records captured as part of TICOM efforts were classified because they would have revealed details of the success of the joint intelligence analysis efforts between the U.S. and U.K. Thus, while this particular cryptography record was not stamped as classified, the folder for the record showing that it was a TICOM document was classified as SECRET. (Figure 1)

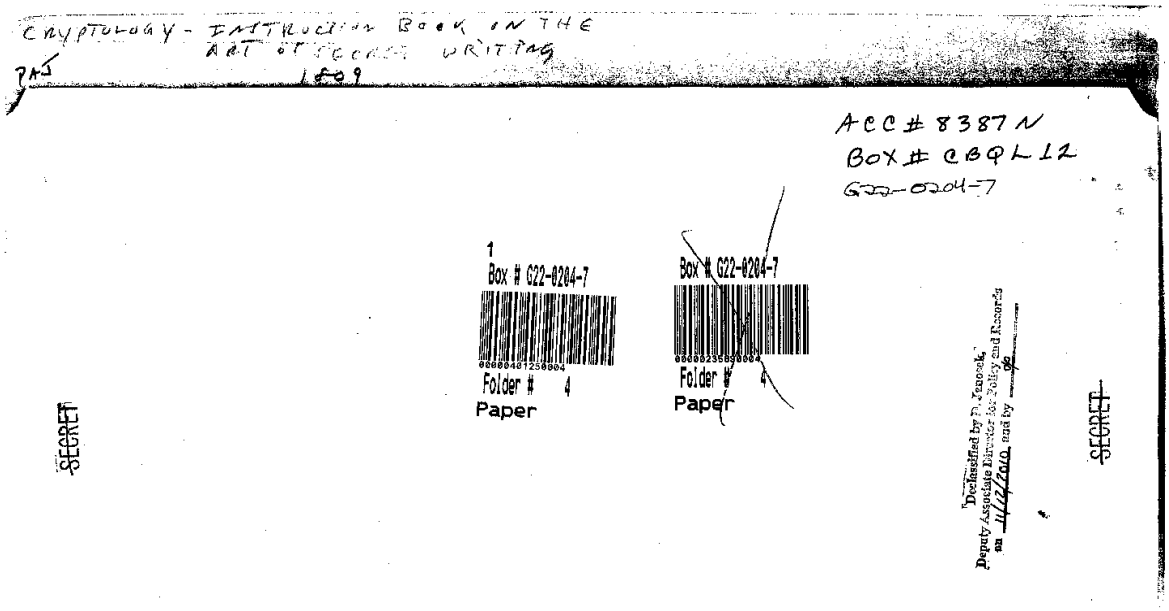


Figure 1: Declassified cover of the folder for the Cryptography Record

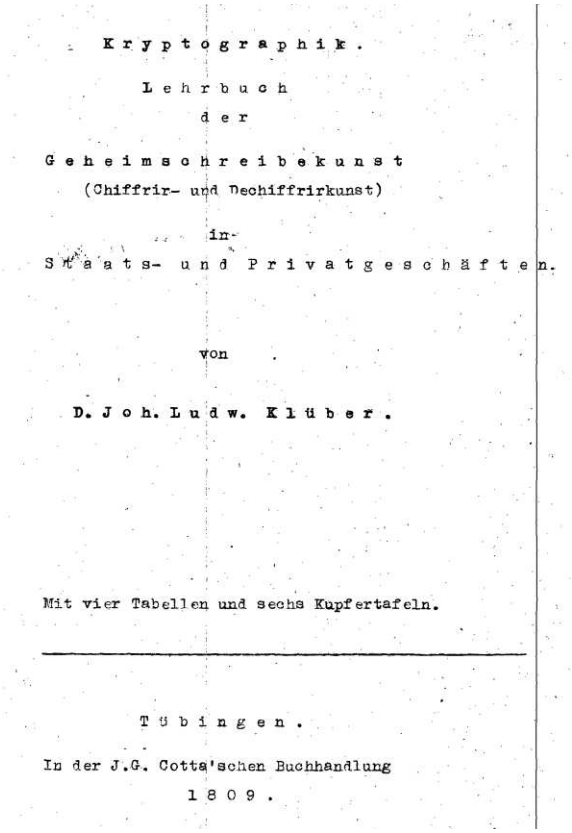
Is this one of the first TICOM documents publicly released by NSA?

No. In 2002, NSA released to NARA for public release almost 1000 TICOM documents. A lower quality version of this cryptographic record was released in that set of documents. That version included hand-written cover sheets showing that it was a TICOM document. For unknown reasons, the TICOM records were accessioned individually. Under NARA's current standard archival process, all TICOM records would be put into a single accession, thereby keeping them together and providing the necessary context.

What is in this record?

The cryptography record created by the unknown German cryptographer includes the information from the title page of the Klüber book, many typed excerpts from the Klüber book, and a hand-written cryptography example.

The first page of the body of the cryptography record (Figure 2) has the information from the title page of the Klüber book (Figure 3).



Kryptographik.

Lehrbuch
der
Geheimschreibekunst
(Chiffrir- und Dechiffrirkunst)
in
Staats- und Privatgeschäften.

von

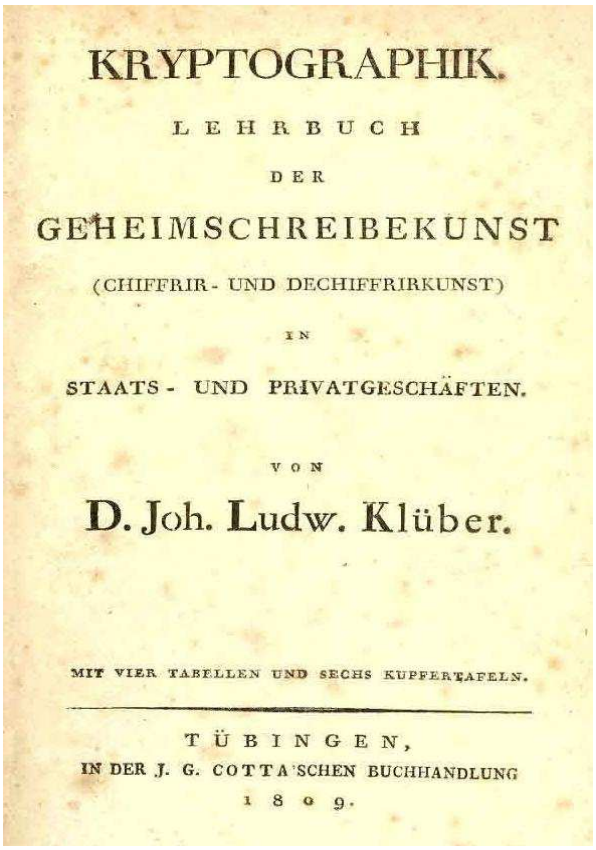
D. Joh. Ludw. Klüber.

Mit vier Tabellen und sechs Kupfertafeln.

Tübingen.

In der J.G. Cotta'schen Buchhandlung
1809.

Figure 2: First page of Cryptography Record



KRYPTOGRAPHIK.

LEHRBUCH

DER

GEHEIMSCHREIBEKUNST

(CHIFFRIR- UND DECHIFFRIRKUNST)

IN

STAATS- UND PRIVATGESCHÄFTEN.

VON

D. Joh. Ludw. Klüber.

MIT VIER TABELLEN UND SECHS KUPFERTAFELN.

TÜBINGEN,
IN DER J. G. COTTA'SCHEN BUCHHANDLUNG
1809.

Figure 3: First page of Klüber Book

Most of the cryptography record consists of typed excerpts from different sections of the Klüber book. These excerpts include:

- the bibliography
- the overview (table of contents)
- sections of the body of the Klüber book

In the cryptography record:

- Single pages (Figure 4) generally contain the content of multiple pages from the Klüber book (Figure 5), with notations showing the page number of the book where that information may be found.
- Footnotes from the book were not included.
- There are some hand-written typographical corrections, as well as small vertical lines showing page breaks.
- There are some modernized spelling changes from the original text in the Klüber book.

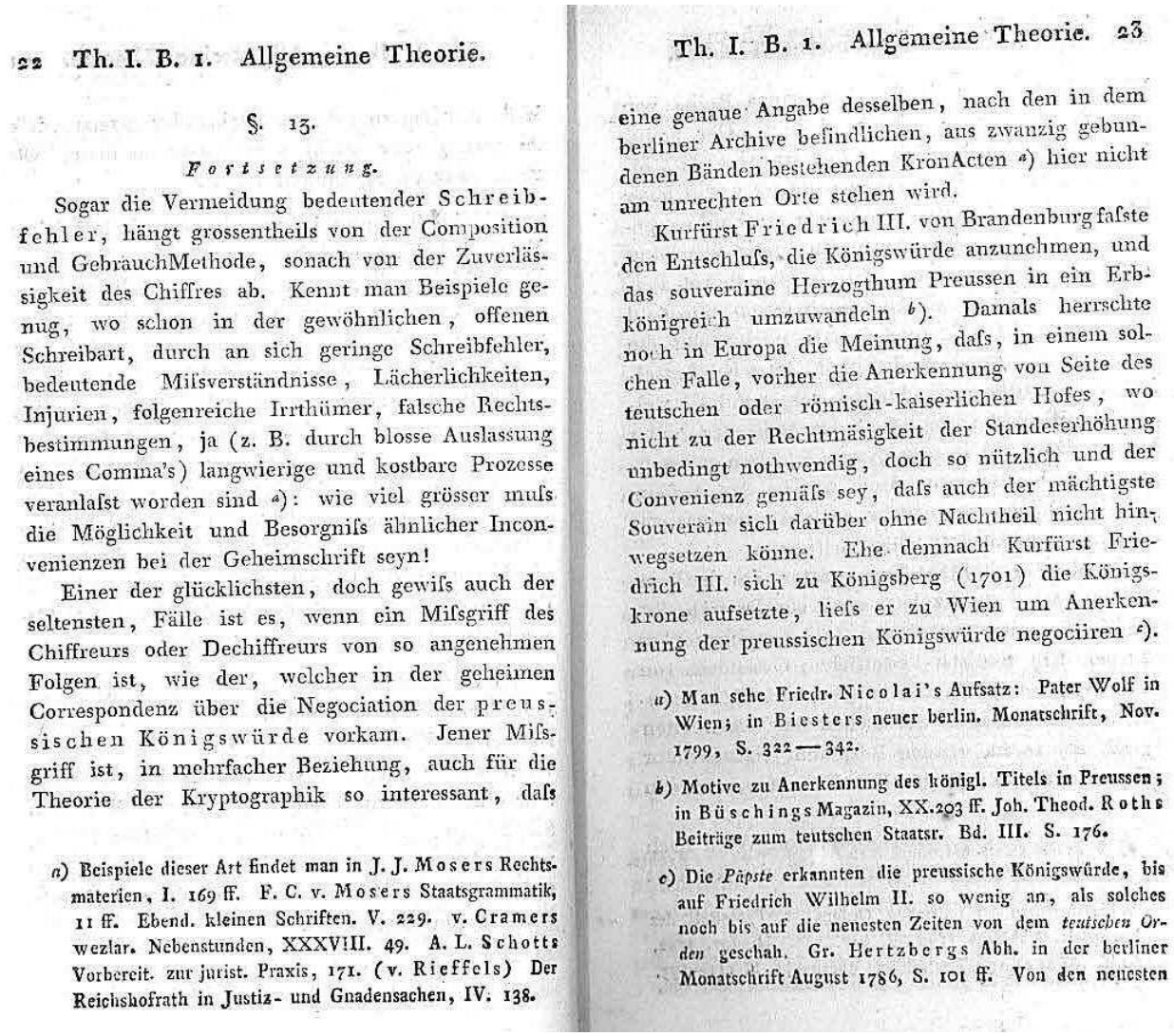
Joh. Lüder.

Aus Klüber : Kryptographik; Tübingen 1809.

Seite 22 Einer der glücklichsten, doch gewiß auch der seltensten, Fälle ist es, wenn ein Mißgriff des Chiffreurs oder Dechiffreurs von so angenehmen Folgen ist, wie der, welcher in der geheimen Korrespondenz über die Negociation der preussischen Königswürde vorkam. Jener Mißgriff ist, in mehrfacher Beziehung, auch für die Theorie der Kryptographik
Seite 23 so interessant, daß eine genaue Angabe desselben, nach den in dem Berliner Archive befindlichen, aus zwanzig gebundenen Bänden bestehenden KronActen hier nicht am unrechten Orte stehen wird.

Kurfürst F r i e d r i c h III, von Brandenburg, faßte den Entschluß, die Königswürde anzunehmen, und das souveraine Herzogtum Preußen in ein Erbkönigreich umzuwandeln. Damals herrschte noch in Europa die Meinung, daß, in einem solchen Falle, vorher die Anerkennung von Seiten des teutschen oder römisch-kaiserlichen Hofes, wo nicht zu der Rechtmäßigkeit der Standeserhöhung unbedingt notwendig, doch so nützlich und der Konvenienz gemäß sei, daß auch der mächtigste Souverain sich darüber ohne Nachteil nicht hinwegsetzen könne. Ehe demnach Kurfürst Friedrich III. sich zu Königsberg (1701) die Königskrone aufsetzte, ließ er zu Wien um Anerkennung der preussischen Königswürde negocii-
Seite 24 ren. Diese Negociation fand, eine ganze Reihe von Jahren,

Figure 4: Partial page of the Cryptography Record



22 Th. I. B. 1. Allgemeine Theorie.

§. 13.

Fortsetzung.

Sogar die Vermeidung bedeutender Schreibfehler, hängt grossentheils von der Composition und GebrauchMethode, sonach von der Zuverlässigkeit des Chiffres ab. Kennt man Beispiele genug, wo schon in der gewöhnlichen, offenen Schreibart, durch an sich geringe Schreibfehler, bedeutende Mifsverständnisse, Lächerlichkeiten, Injurien, folgenreiche Irrthümer, falsche Rechtsbestimmungen, ja (z. B. durch blosse Auslassung eines Comma's) langwierige und kostbare Prozesse veranlafst worden sind *a*): wie viel grösser mufs die Möglichkeit und Besorgnifs ähnlicher Inconvenienzen bei der Geheimschrift seyn!

Einer der glücklichsten, doch gewifs auch der seltensten, Fälle ist es, wenn ein Mifsgriff des Chiffreurs oder Dechiffreurs von so angenehmen Folgen ist, wie der, welcher in der geheimen Correspondenz über die Negociation der preussischen Königswürde vorkam. Jener Mifsgriff ist, in mehrfacher Beziehung, auch für die Theorie der Kryptographik so interessant, dafs

a) Beispiele dieser Art findet man in J. J. Mosers Rechtsmaterien, I. 169 ff. F. C. v. Mosers Staatsgrammatik, 11 ff. Ebend. kleinen Schriften. V. 229. v. Cramers wezlar. Nebenstunden, XXXVIII. 49. A. L. Schotts Vorbereit. zur jurist. Praxis, 171. (v. Rieffels) Der Reichshofrath in Justiz- und Gnadensachen, IV. 138.

Th. I. B. 1. Allgemeine Theorie. 23

eine genaue Angabe desselben, nach den in dem berliner Archive befindlichen, aus zwanzig gebundenen Bänden bestehenden KronActen *a*) hier nicht am unrechten Orte stehen wird.

Kurfürst Friedrich III. von Brandenburg fafste den Entschlufs, die Königswürde anzunehmen, und das souveraine Herzogthum Preussen in ein Erbkönigreich umzuwandeln *b*). Damals herrschte noch in Europa die Meinung, dafs, in einem solchen Falle, vorher die Anerkennung von Seite des teutschen oder römisch-kaiserlichen Hofes, wo nicht zu der Rechtmäsigkeit der Standeserhöhung unbedingt nothwendig, doch so nützlich und der Convenienz gemäfs sey, dafs auch der mächtigste Souverain sich darüber ohne Nachtheil nicht hinwegsetzen könne. Ehe demnach Kurfürst Friedrich III. sich zu Königsberg (1701) die Königskrone aufsetzte, liefs er zu Wien um Anerkennung der preussischen Königswürde negociiren *c*).

a) Man sehe Friedr. Nicolai's Aufsatz: Pater Wolf in Wien; in Biesters neuer berlin. Monatschrift, Nov. 1799, S. 322—342.

b) Motive zu Anerkennung des königl. Titels in Preussen; in Büschings Magazin, XX. 293 ff. Joh. Theod. Roths Beiträge zum teutschen Staatsr. Bd. III. S. 176.

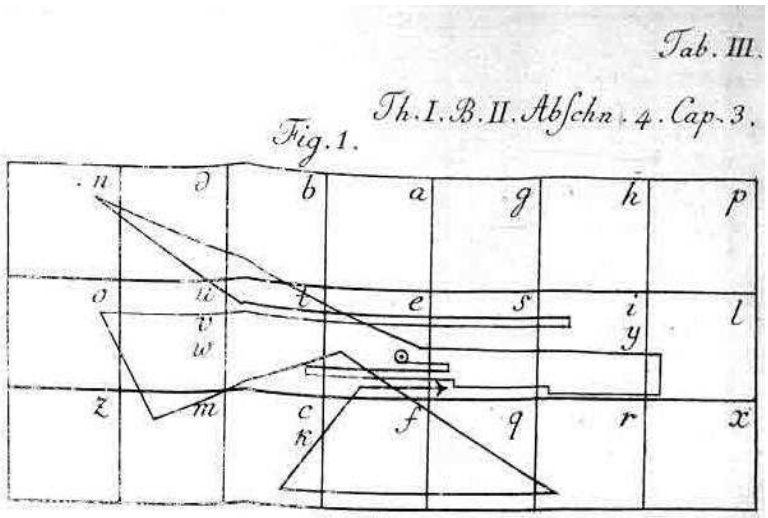
c) Die *Päpste* erkannten die preussische Königswürde, bis auf Friedrich Wilhelm II. so wenig an, als solches noch bis auf die neuesten Zeiten von dem *teutschen Orden* geschah. Gr. Hertzbergs Abh. in der berliner Monatschrift August 1786, S. 101 ff. Von den neuesten

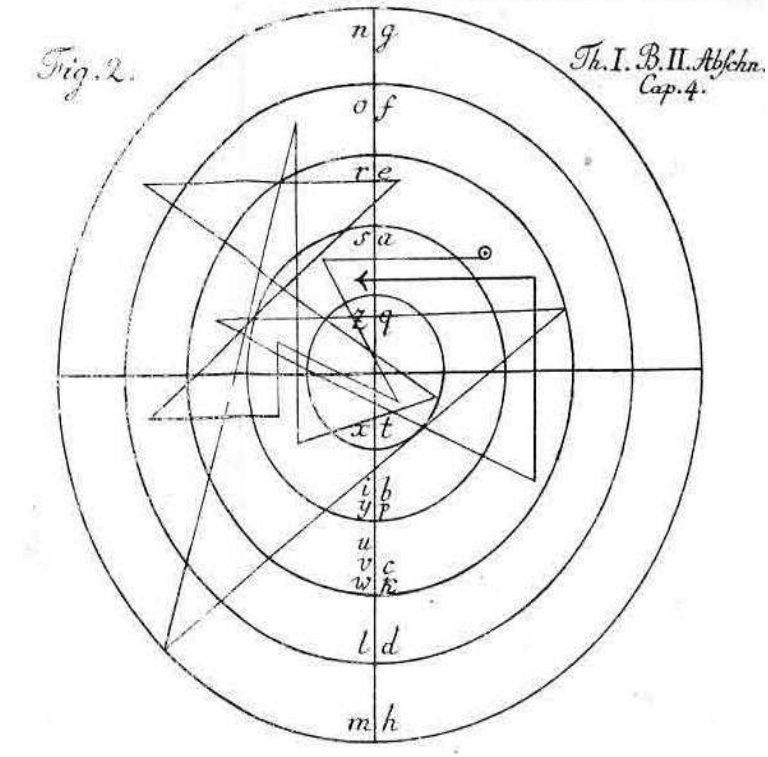
Figure 5: Pages 22 – 23 of the Klüber book

The most interesting part of this cryptography record is the hand-written cryptography example at the end. The things to look for are:

- The Klüber book includes examples of line scripts using a rectangle, circle and a series of embedded circles. (Figure 6) For each example:
  - The letters of the alphabet (excluding the letter "j") were inscribed within the shapes.
  - In some cases, multiple letters of the alphabet are contained in the same cell. In these cases, the person decrypting the message may need to figure out from the context which letter was more likely in the original message.

- A small circle is drawn showing where the line begins and then lines are drawn in the table from one letter of the message to the next. A small arrow shows the end of the message.
- The pattern made by those lines would apparently be sent as the encrypted message, which the recipient would decrypt by laying that pattern on the same table and reading the letters off from the beginning circle to the concluding arrow. An example in the rectangle is shown using the Latin phrase: EST SILENTIO MERCES.





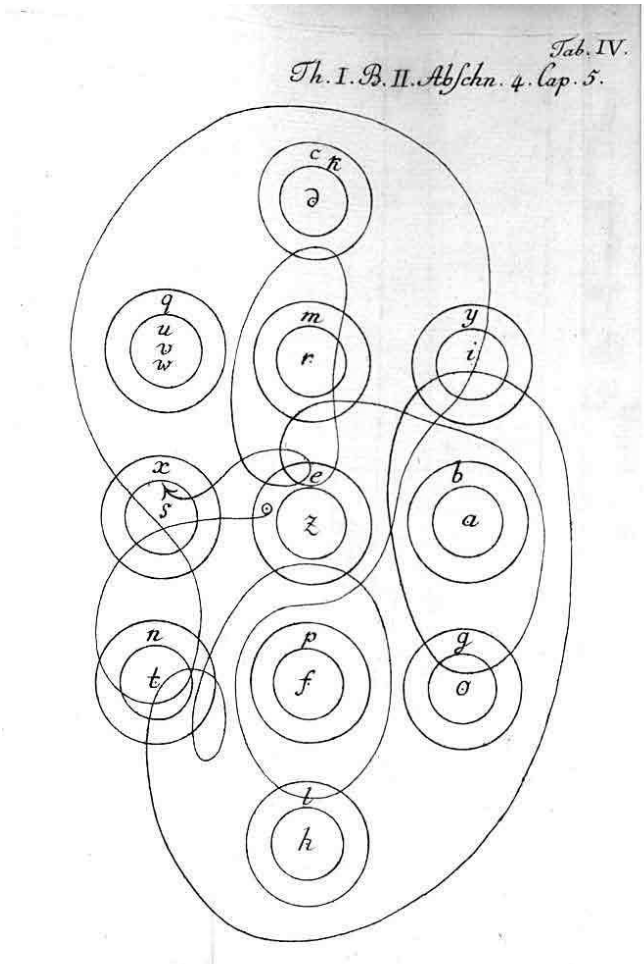


Figure 6: Line script examples from the Klüber book

In the hand-written example in the cryptography record, the author:

- applied that technique using a square table with 5 rows and 5 columns in which the letters of the alphabet were inscribed (again excluding the letter “j”) and included a version of the table without a line script and an example of the table with a line script example using what appears to be the German phrase: DIES IST DIE SOGENANNTE QUADRATSCHRIFT. (Figure 7)
- interestingly, did not include the section of the Klüber book (pages 285 – 289) addressing the line script examples

Quadratschrift.

k	y	b	x	g
ü	a	s	f	v
h	o	c	r	d
i	u	e	l	w
p	t	m	z	q

Gehört nach den Angaben in Klüber, Kryptographik (1809), Teil I, Buch II, Abschn. IV, Kap. 3.

Der Text auf Pauspapier lautet: „Das ist die sogenannte Quadratschrift."

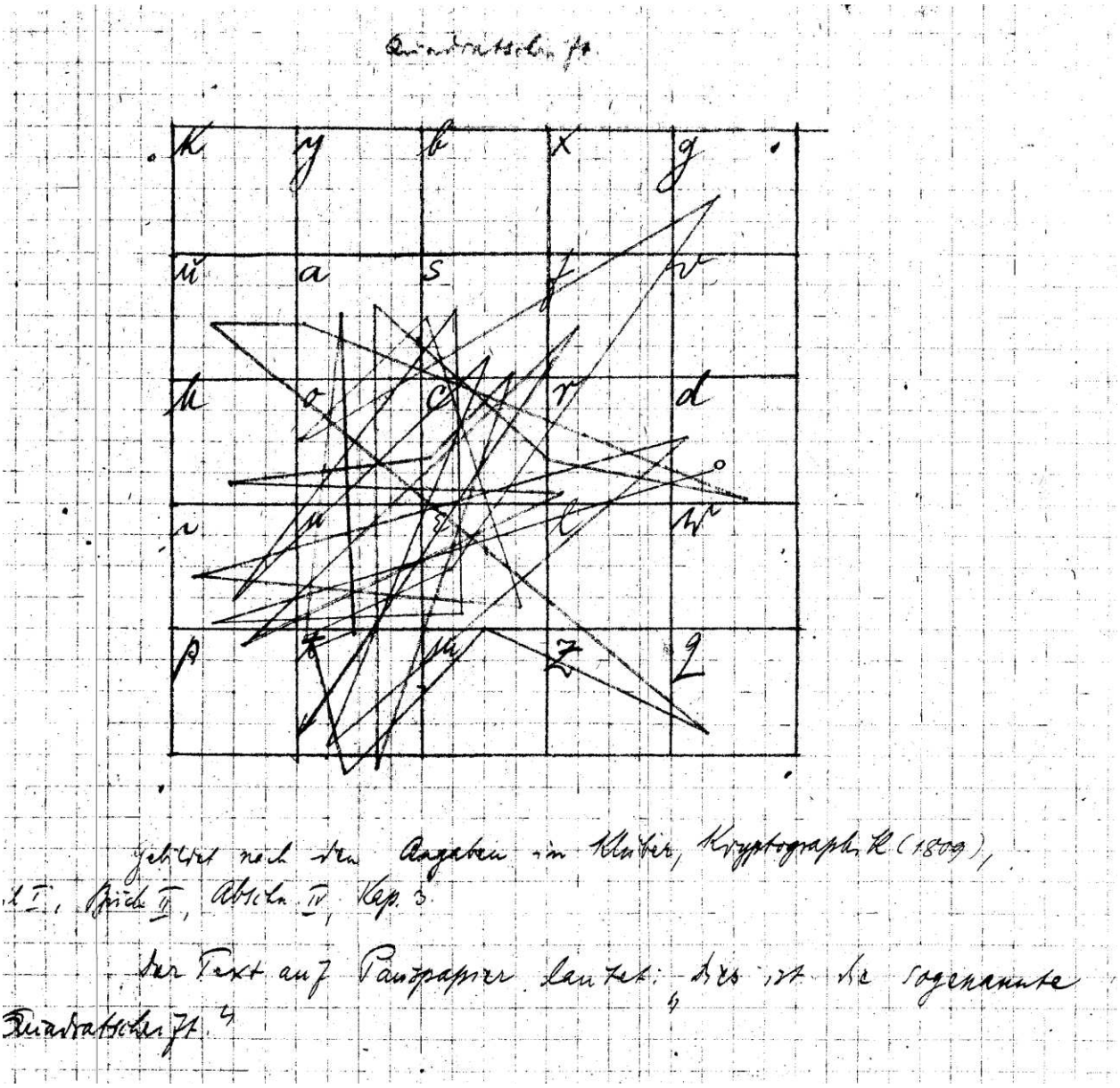


Figure 7: Line script example from the Cryptography Record

<u>Does this German document have permanent historical value for the U.S.?</u>

Yes. It is an example of the cryptographic materials recovered under the TICOM effort. It is also important for modern cryptographers studying the systems of our country's adversaries in that developers of new cryptographic systems frequently recycle principles of systems used years earlier.

How was the context of this record determined?

The June 2011 press release on this record did not provide the context of this declassified historical record. Given that the first page of the record contains the same information as the title page of the Klüber book, it may have initially appeared to the public that this record was the Klüber book. Fortunately an early edition of the Klüber book is available in the National Cryptologic Museum as part of a collection of materials donated to the National Cryptologic Museum Foundation by the historian Dr. David Kahn. By comparing the record to the book, it was apparent that while the record contained information from the book, it was not actually part of the book.

Several people with experience in cryptanalysis and German, from both the U.S. and U.K. in another example of cooperation, worked together to identify the content of the record. Because the hand-written square line script example actually has the line script misaligned on the table, the message can be recovered accurately by copying the line script and applying it to the table without script on the adjacent page. (Figure 7)

All these efforts assisted in determining the context of this record. While NSA may never know for certain when this cryptographic record was created, what its specific purpose was, or who the author was, this reconstruction provides the best possible explanation given the information available.

For other related information, go to www.nsa.gov.