# A French cipher from the late $19^{\text {th }}$ century 

Rémi Géraud-Stewart and David Naccache<br>Information Security Group, Département d'informatique de l'ÉNS, École normale supérieure, CNRS, PSL Research University, Paris, France. first_name.family_name@ens.fr

## ARTICLE HISTORY

Compiled April 6, 2020


#### Abstract

The Franco-Prussian war (1870-1871) was the first major European conflict during which extensive telegraph use enabled fast communication across large distances. Field officers would therefore have to learn how to use secret codes. But training officers also raises the probability that defectors would reveal these codes to the enemy. Practically all known secret codes at the time could be broken if the enemy knew how they worked.

Under Kerckhoffs' impulsion, the French military thus developed new codes, meant to resist even if the adversary knew the encoding and decoding algorithms, but simple enough to be explained and taught to military personnel.

Many of these codes were lost to history. One of the designs however, due to Major H. D. Josse, has been recovered and this article describes the features, history, and role of this particular construction. Josse's code was considered for field deployment and underwent some experimental tests in the late 1800s, the result of which were condensed in a short handwritten report. During World War II, German forces got hold of documents describing Josse's work, and brought them to Berlin to be analyzed. A few years later these documents moved to Russia, where they have resided since.


## KEYWORDS

Historical cipher, French cryptography, Hippolyte D. Josse

## 1. Introduction

Since Kerckhoffs' works [Ker83], it has become almost common sense to design, evaluate and implement cryptography in a transparent way, not merely for scientific but for very pragmatic reasons. But before this celebrated principle made its way into the mainstream, security by obscurity was the norm. As a result, early relics of cryptographic work are hard to unearth: They often lay in the shadows of military archive bunkers, despite the fact that most of the techniques described there were never implemented, let alone used in the field, and are in any case obsolete by today's standards.
It is thus very lucky, in a sense, that Major Josse's system attracted enough attention for the German army to take notice of it, and bring descriptions to Berlin for cryptanalysis. In hindsight this is itself a mystery: at the time the Germans seized documents, these were already more than 30 years old; and we have no evidence that this particular code was ever used at all. It is unclear then what exactly was their motivation; it may have been part of a systematic effort to search for and analyze every technique they could lay their hands on. Whether they picked this code in particular, or it was part of
a bundle, we do not know.
When East Germany fell to the Soviet army, documents relative to the Josse system were sent to Moscow, probably to undergo analysis as well. They have resided there until recently, when documents were brought back to France.

In this paper we analyse the corpus of documents that has been recovered, from a historical and cryptographic standpoint. Amongst these, only a few can be attributed with relative certainty to Major Josse's efforts, and constitute a credible cryptographic system which, although obsoleted by modern techniques, could very well have been of use in the late 1800s.

## 2. The corpus

Because of its tortured history, being moved from one archiving place to the next across countries, it comes at some surprise that all documents in the bundle are in an excellent state, showing no more than stains due to aging paper and some degradation related to manipulation. This may indicate that these documents were not handled very much or only with extreme care.

As we discuss below, the bundle itself consists in several pages, the origin of which we investigate.

### 2.1. Description of the corpus

The corpus consists in 17 unnumbered manuscript pages, including title pages and appendices. They were handwritten in French. The corpus, reproduced in appendix, is composed of several documents:
(1) A main document, entitled "Projet de Cryptographie Militaire n ${ }^{\circ} 3$ " (Military Cryptography Project Nr. 3). This document describes a cryptosystem's design goals, encryption and decryption procedures, and makes additional remarks on how to teach it. We will henceforth refer to this cryptosystem as Josse's system. This document appears twice (1a and 1b).
(2) A second document, probably meant to follow the first one, entitled "Système cryptographique $\mathrm{n}^{\circ} 3$ " (Cryptographic system Nr. 3). This document contains the result of training exercises with several officers on Josse's code, where accuracy and speed were recorded.
(3) A newspaper article draft, which praises a "New cryptographic system" (without explicitly mentioning Josse's system).
(4) An appendix to the main document (two copies, corresponding to the two versions), containing subtraction tables ( 4 a and 4 b ).
(5) A letter, signed by "S. Mounier" (or possibly Munier?) and dated June 29, 1889, addressed to Major Josse, mentioning the successfully copied version of the original draft. Indeed the first and second documents each appear in two versions: a draft version, with visible crossing-outs and additions; and a clean version. In all probability the clean version is the one mentioned by $\mathrm{M}(\mathrm{o})$ unier.
(6) A leaflet, entitled "Méthode stéganographique Josse" (Josse steganographic method) followed by a poem.

We will refer to these documents by the numbers $1 \mathrm{a}, 1 \mathrm{~b}, 2,3,4 \mathrm{a}, 4 \mathrm{~b}, 5$, and 6 in the following discussion. Note that all pages except the poem are of standard format (A3 double pages, or A4 single pages). The poem paper is lighter and of lesser quality, possibly removed from a notebook.

### 2.2. Handwriting analysis

It is possible to use forensic handwriting analysis techniques on the documents to gather information about their authorship [ENF15]. In this context, there is no suspicion of simulation and we may assume that clear differences in writing correspond to different authors.

This analysis relies on identifying characteristic features of handwriting, such as letter shapes, word spacing, presence and nature of ligatures, connecting strokes, and line form (which indicates pressure). We are helped in this endeavor by the documents' length, and the relatively regular handwriting under scrutiny.

Analysis, summarized in Table 1, reveals that eight authors contributed to the corpus. In particular, the absence of stroke-through text and mistakes in Document 1b seems to indicate that it was copied after 1a (and similarly, 4 b was probably copied from 4a). We mention in this table the key features that enable to distinguish one author from all the others.

Amongst these features we mention the writing style, when recognizable, used by the author. Indeed, official French documents were expected to be written in either of three authorised styles: ronde, coulée, and italienne-bâtarde [Gre15, Mor09]. A middle ground is the copperplate style, considered more readable and therefore appropriate for formal exchanges in restricted circles. ${ }^{1}$ The use of other styles (or failure to adhere to a well-known calligraphic style) is then indication that the document was not meant for official communication. ${ }^{2}$

Some documents (1b, 2, and 4b) are written in different calligraphic styles. This alone does not guarantee that they were written by different persons. However we take the conservative approach to give these authors different names. Document 6 is written in a style reminiscent of 1 a, but exhibits key differences and is probably the work of an unrelated author.

## 3. Content analysis

### 3.1. Overview of inter-document relationships

Handwriting analysis (Section 2.2) already gives some information about how the different documents are related. We completed this analysis by an in-depth examination of the corpus' contents and consistency. An overview of the relationships between documents is illustrated in Figure 1 and detailed hereafter.

In particular, documents 3 and 6 do not seem to be related to the cryptographic system described in documents $1,2,4,5$. Document 6 bears a mention of Josse, and is thus not completely unrelated. However document 3 does not, and seems to be completely independent from the other documents.

[^0]Table 1. Handwriting analysis on the corpus.

| Doc. | Author(s) | Style | Distinguishing features | Comments |
| :---: | :---: | :---: | :---: | :---: |
| 1 a | $\mathrm{A} 1+\mathrm{A} 2$ | - | Connecting stroke in que, $t$, st, capital $S$ and $P$, digit 3 | A1 wrote the title page only. |
| 1b | A3 | Danish ronde | Capital $M$ and $G$, ff ligature, $s$ and $b$, line form | Including the title page. |
| 2 | A4 | Copperplate | Ligatures and final $s$ | - |
| 3 | A5 | - | Capital $L, f, p$, and $f f$, disconnected $q u$ | Dated 188... |
| 4 a | A2 | - | Digits | - |
| 4 b | A3 | Danish ronde | Digits | - |
| 5 | A6 | - | Capital $M, R$, and $S$, line form, character height-towidth ratio, spacing | Signed S. Mounier. <br> Dated 29 Jun 1889. |
| 6 | A7 + A8 | - | Trailing letters $e, s, t$, slant, final $e z$ digraph. Disconnected $p h$, capital $J$. | A8 wrote on the back only. A7 bears some similarity to A2. |



Figure 1. Relationships between the documents. A thick arrow indicates that a document mentions another. A dotted line indicates that a document was used as source for another.

### 3.2. The poem (document 6)

Let's start with a description and analysis of the ancillary documents, because their relationship to the cryptographic system is unclear and they can be treated independently.

While the leaflet bears the inscription "Méthode stéganographique Josse", the poem written on this page and reproduced in Appendix A was widely known at the time. Indeed, the poem was quoted more or less in its entirety in several books published before Josse's death. We found an early mention in "Amusements philologiques ou variétés en tous genres" by Gabriel Peignot ${ }^{3}$ in 1808 [Pei08, p. 40], although there might be even earlier sources. According to Peignot,

[^1]"These letters first present a meaning, when read as usual; but if we read the first line, the third, the fifth, etc. that is, every other line, we shall find a meaning opposite to the one a first reading suggested. ${ }^{4}$ "
In other terms, while the entire poem makes sense as it is, reading the even-numbered lines only (and skipping over the odd-numbered lines) reveals a message that completely contradicts it.

Peignot mentions several other examples of vers brisés (broken verses) in French literature, including the poem's continuation.

As such, the text itself seems to be an exercise in literary entertainment rather than a military steganographic method, and there is no mention of it in any of the other documents. The leaflet is not signed nor dated, and the different paper grade and format seem to indicate that it was not part of the original bundle.

Since the document is handwritten, the possibility remains that there is hidden information in the way words are written, in the placement of words on the paper, or non-word symbols (e.g. dots), or invisible ink.

Comparison to Peignot's version rules out steganography based on altering words. It is unlikely that inter-word spacing was engineered, and a quick statistical hypothesis test on a digital copy is consistent with a Gaussian distribution.

A German-style dot-based steganography is possible: the placement of dots and punctuation sign is rather free, and there are enough such marks (around 75) to encode a short message if using for instance a grid.

Inspection of the document under visible and near-UV light did not reveal nor indicate the use of special ink.

### 3.3. The newspaper article (document 3)

The newspaper draft, written on Revue de Cavalerie Militaire letterhead and unsigned, praises the benefits of a "new cryptographic system" not otherwise made precise. The exact date of writing, or possible publication, is not written. We couldn't find a mention of a published version of this article in the École Militaire's Milindex document archive, which seems to start around 1892. Since the Revue was created in 1885 and the letterhead indicates $188 \ldots$ we can suspect that the draft was written during this period: 1885-1889, and most likely not before 1880 . Since the draft refers to a previous issue ${ }^{5}$ we may assume that the author already wrote for the Revue before, in March of the same year.

A thorough read raises doubts on the idea that the cryptographic system mentioned in this draft is really Josse's. Indeed, it insists on the usage of two cryptographic keys (Josse's system, as we will see, only has one), and on the immunity of ciphertexts to alterations ${ }^{6}$ that seem to break ciphertexts generated by Josse's method. The encryption procedure seems different from Josse's ${ }^{7}$, but is not described in enough details to be decisive.

Finally, the author admits that the system's security relies not on the key, or the

[^2]encryption grid, but on the cryptosystem's principle ${ }^{8}$ - a blatant violation of Kerckhoffs' design recommendations. As we shall see, this is at odds with Josse's system, which does not assume security by obscurity. In fact, as noted by Kahn [Kah67], Josse was a fond admirer of Kerckhoffs:
"Josse quoted Kerckhoffs so often that he felt it necessary to insert an apologetic 'M. Kerckhoffs, whose name recurs so often in cryptography' after an especially heavy flurry of references."

Altogether, these elements seem to rule document 3 out, as a possibly contemporary account otherwise unrelated to Josse's system.

### 3.4. Core documents

The remainder of the documents forms a densely connected and consistent set. Document 1a describes a cryptographic scheme, and is supplemented by Document 4a. Document 5 mentions that a copy was performed, which seems to refer to documents 1 b and 4 b . Finally, Document 2 relates field experiments (timing measurements) based on the cryptosystem.

If we are to believe Document 5, the cryptosystem under consideration was engineered by Josse, and Documents 1a and 4a would bear his very own writing.

## 4. Josse's cryptographic system

### 4.1. Major Josse

Publicly available information about Josse is only fragmentary.
Hippolyte Désiré Josse was born on July 14, 1852 in Montmartre (Seine) near Paris. ${ }^{9}$ His parents Jean Louis Désiré Josse (born 1820) and Cécile Amélie Denisia Dufeu (born 1832) had another child, Marie Emilie Eugénie (born 1860). Hippolyte Josse graduated from École polytechnique in 1872, and married Alix Amélie Hyvernat (born 1855) in 1881 in Paris.

Fighting in the 1870 war against Prussia, Josse was made Major and later knighted within the Ordre de la Légion d'Honneur (Matricule 61,140) on August 14, 1900.

Originally an artillery officer, Josse is the author of a single book, dedicated to military cryptography and published in 1885 [Jos85a] (from which Kahn's citation is excerpted [Jos85a, p. 695]). The book actually gathers articles published that same year by Josse himself, essentially in the Revue Maritime et Coloniale [Jos85b, Jos85c].

He seems to have taken a prime role in the early organisation of French military cryptography ${ }^{10}$ along with fellow army officers Philippe, Munier, Delanne, Berthaut, Brun, Picquart, Legrand, and Straforello, issuing in particular field manuals related to telegraphic communications [Lau09]. One of these documents, known as the "Dictionnaire $1890^{\prime \prime}$, described a dual system relying on one cipher in wartime and another when in peace. It was amongst the codes that Bazeries broke while still an amateur.

This would be contemporary to the system described here, which seems to have been designed around 1889.

[^3]In 1900 Josse (at that time a colonel) participated in the French Ministry of War official commission on cryptography, along with Jean-Jules Brun, Henry-Marie-Auguste Berthaut, and François Cartier.

According to the records, Josse died on February 10, 1929, at the age of 76.

### 4.2. Description of the cryptosystem

Josse's system works on a restricted subset of the Latin alphabet, without punctuation, numbers or spaces, and does not distinguish between upper and lower case. Interestingly, the letter W is also removed from this alphabet. As was very common at the time, letters are put in correspondence with their index in the alphabet:

$$
\begin{array}{ccccccccccccccccccccccccc}
\text { A } & \text { } & \text { C } & \text { D } & \text { E } & \text { } & \text { G } & \text { H } & \text { I } & \text { J } & \text { K } & \text { L } & \text { M } & \text { N } & \text { O } & \text { P } & \text { Q } & \text { R } & \text { S } & \text { T } & \text { U } & \text { V } & \text { X } & \text { Y } & \text { Z } \\
\hline & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25
\end{array}
$$

Both the plaintext, password, and ciphertext are written using this alphabet, and understood as a sequence of numbers between 1 and 25 . The choice to drop W is not explained, but a possible motivation is that operations modulo 25 are somewhat simpler to perform with pen and paper than modulo 26, and W is a very rare letter in French so that its loss has minimal impact.

- Setup: Both the sender and the recipient agree beforehand on a "seed" $P$, which will be used to generate the substitution table used to both encode and decode messages. $P$ is a short password, written in the alphabet discussed above.
- Key generation: To generate the key, duplicate letters are removed from $P$, which gives $P^{\prime}$ of length $N$. Then $P^{\prime}$ is spelled and put in the first row of a table with $N$ columns. The rest of the letters follow, in alphabetical order. There are thus $\lceil 25 / N\rceil$ rows in the table. The table is then read column-wise to yield a shuffled alphabet, which is the secret key. We write $S(a)$ to denote the position of the letter $a$ in that new alphabet (with the convention that the first element is in position 1).
- Encryption: Let $m=m_{1} \cdots m_{M}$ be a message. If necessary, the message is padded with random letters ${ }^{11}$ so that $M$ is a multiple of 5 . First compute

$$
r_{i}=S\left(m_{i}\right)+r_{i-1} \bmod 25
$$

with the exception of the first, $r_{1}=1-S\left(m_{1}\right) \bmod 25$. The ciphertext is given by $c_{i}=S^{-1}\left(r_{i}\right)$.

- Decryption: Given a ciphertext $c=c_{1} \cdots c_{M}$ we first construct

$$
d_{i}=S\left(c_{i}\right)-S\left(c_{i-1}\right) \bmod 25
$$

with the exception of the first, $d_{1}=1-S\left(c_{1}\right) \bmod 25$. The message is finally recovered as $m_{i}=S^{-1}\left(d_{i}\right)$.

Amongst other seemingly arbitrary tweaks, the different treatment regarding $c_{1}$ is justified by a desire that "the first letter of the ciphertext be different from the first letter of the message".

[^4]Example (key generation). Let us use the secret password $P=$ kANGAROO. Then $P^{\prime}=$ KANGRO with $N=6$. We get a table

| K | A | N | G | R | O |
| :---: | :---: | :---: | :---: | :---: | :---: |
| B | C | D | E | F | H |
| I | J | L | M | P | Q |
| S | T | U | V | X | Y |
| Z |  |  |  |  |  |

which yields the shared secret key: KBISZ ACJTN DLUGE MVRFP XOHQY.

### 4.3. Correctness

First note that $d_{1}=-S\left(c_{1}\right)=-S\left(S^{-1}\left(1-S\left(m_{1}\right)\right)\right)=1-S\left(m_{1}\right)$ so that $S^{-1}\left(d_{1}\right)=$ $S^{-1}\left(S\left(m_{1}\right)\right)=m_{1}$. Then for every $i>1$,

$$
\begin{aligned}
d_{i} & =S\left(c_{i}\right)-S\left(c_{i-1}\right) \\
& =S\left(S^{-1}\left(r_{i}\right)\right)-S\left(S^{-1}\left(r_{i-1}\right)\right) \\
& =r_{i}+1-r_{i-1}-1=r_{i}-r_{i-1} \\
& =S\left(m_{i}\right)
\end{aligned}
$$

so that $S^{-1}\left(d_{i}\right)=m_{i}$.

## 5. Implementation remarks

Josse makes several remarks about the use of his cipher in the field, with details about how computing first $S\left(m_{i}\right)$ and using modular subtraction lookup tables make encryption faster and less error-prone.

Although it is not commented upon, a mistake during encryption causes the rest of the process to fail (which may be a serious concern when the operation is performed manually and on the battlefield).

## 6. Cryptanalysis

Josse's system can essentially be seen as several protection layers added on top of a simple substitution cipher. The protections are threefold ${ }^{12}$ :

- The first letter is encoded in a different way;
- Some form of "error propagation" mechanism is used, anticipating on the modern CBC mode of operation;
- The alphabet is scrambled in a key-dependent way.

A few observations can be made about this design:

- Encryption is linear: assume that we know a rotation of the key, i.e. the letters are in the correct sequence but shifted by an unknown amount $s$. Then during decryption all the $d_{i}$ are correct except $d_{1}$, which is the correct value plus $s$.

[^5]Another consequence of linearity is that it is possible to perform the usual frequency analysis techniques on $c_{i}-c_{i-1}$.

- Encryption is deterministic: a chosen plaintext attack easily recovers the key.
- By design the key size is limited to 25 (after removing duplicate letters), which offers a choice of at most $25!\approx 2^{83}$ keys. Using short passwords $P$, the number of possible keys drops substantially: for instance there are only 53310 keys generated from 5-letter passwords, and multiple passwords generate the same key (e.g. CATCH THE CAT and CATHE). If we consider that there are about 130000 words in French, there are realistically fewer than $2^{17}$ usable keys. This is well within reach of exhaustive search. ${ }^{13}$
- The key derivation mechanism works by transposing an alphabet formed by appending unused letters to the password. If the password is to be short, then in fact most letters are in place. Let's assume for simplicity an empty password i.e. the key is obtained by transposing the plain alphabet using a grid of unknown size $N, 1 \leq N \leq 25$. Each possibility gives a scrambled alphabet. The closest candidate alphabet is only wrong by an offset between actual key letters, which enables recovery of the password length and (by subtracting the offsets) the password itself.


## 7. Conclusion and remaining questions

This paper provides a concrete glimpse into the French military cryptographic universe during the late 1880s and in the early 1890s. As we could see, the proposed method was meant to be simple, as it was essential for officiers to understand it quickly, and to use it efficiently. The design itself builds from simples ideas, some of which have been independently introduced in other cryptographic constructions (such as chaining). Very little else is known about Josse's work in cryptography; this is supposedly his third attempt at a cryptographic design (if we are to believe the documents), but we do not know anything about any previous, or subsequent attempts. The inspirations and influences of this encryption method are also difficult to pinpoint, as Josse does not justify why this particular system was designed the way it was. It may well happen that more of his creations are waiting to be found in unexplored archives.

## References

[ENF15] ENFSI. Best practice manual for the forensic examination of handwriting, ENFSI-BPM-FHX-01, 2015
[Gre15] David C. Greetham. Textual scholarship: An introduction. Routledge, 2015.
[Grö07] B. Gröndal. Handwriting Models: An Icelandic Manual, 1883. Operina LLC, 2007.
[Jos85a] Hippolyte Désiré Josse. La Cryptographie et ses applications à l'art militaire. Librairie Militaire de L. Baudoin \& Cie., 1885.
[Jos85b] Hippolyte Désiré Josse. La cryptographie et ses applications à l'art militaire. Revue Maritime et Coloniale, Lxxxiv:391-432, February 1885.

[^6][Jos85c] Hippolyte Désiré Josse. La cryptographie et ses applications à l'art militaire. Revue Maritime et Coloniale, Lxxxiv:640-699, March 1885.
[Kah67] David Kahn. The Codebreakers: The story of secret writing. MacMillan, 1967.
[Ker83] Auguste Kerckhoffs. La cryptographie militaire. Librairie militaire de L. Baudoin, 1883.
[Lau09] Sébastien-Yves Laurent. Politiques de l'ombre: L'Etat et le renseignement en France. Divers Histoire. Fayard, 2009.
[Mor09] Stanley Morison. Selected Essays Ont the History of Letter-forms in Manuscript and Print. Cambridge University Press, 2009.
[Pei08] Gabriel Peignot. Amusements philologiques: ou, Variétés en tous genres. A.A. Renouard, 1808.

## Appendix A. The poem (document 6) in extenso

We reproduce here the poem, with even lines coloured red, and odd lines coloured blue. The poem can be read in two ways: Either "normally", reading every line; or skipping the odd (red, slanted) lines. The two readings yield opposite meanings.

Mademoiselle,
Je m'empresse de vous écrire pour vous déclarer que vous vous trompez beaucoup si vous croyez que vous êtes celle pour qui je soupire Il est bien vrai que pour vous éprouver je vous ai fait mille aveux. Après quoi vous êtes devenue l'objet de ma raillerie. Ainsi ne doutez plus de ce qui vous dit ici celui qui n'a eu que de l'aversion pour vous et qui aimerait mieux mourir que de se voir obligé de vous épouser, et de changer le dessein qu'il a formé de vous haïr toute sa vie, bien loin de vous aimer, comme il vous l'a déclaré. Soyez donc désabusée, croyez-moi, et si vous êtes encore constante et persuadée que vous êtes aimée vous serez encore plus exposée à la rizée de tout le monde et particulièrement de celui qui n'a jamais été et ne sera jamais

Votre serviteur

## Appendix B. Scan of the corpus

MINISTERE
DELA GUERRE
$\qquad$
ÉTAT-MAJOLI GÉNÉRAL
-ame
Direction
DE
Télégraphie Mrlitaite
colooa
684 amanter
I. as pi waveur der adres

vor comil den procsi veotale .le mise a suex ar orex eyptaín are arpabyontie.

PBegy ctactarsemsent sin one.


qu cthe et bitnicrete, theme celle piecaulon hloft pas indes
qu able, an l'ancenri, been que fotrestem d'un sembbleble do oun
perwade, and Pmin toul dre, l'auter
r'en sereat pers beene coup phes avance'. Some to ind dre,

ala convino 1 an on .

pre the touler bes deriches corrax
le typlame in analo

tanment ainoti par P'menternadiane d'un pett nombe de teriem


Methode Stigariogrop hique fors 18

Onodemaisell
Ye on'exiprese of vaus iorive heaver vaus de claver Gue vaws vows tronjer heavionp t' vow erayez ${ }^{3}$ que vaus its celle pier yer $j^{\prime}$ 'serpire, $\because$ at hien vra' ique pacer vodus eprourer
5 y'vos ai fait mull areux apmis equan. 'rous cter devenue l'abjet et ma raillenier aimi.
7 he dontez pheus de a qu vaus dit ici celui. "fr.'n' à en que de l'aversion-pourvous et

- वpi aimerais miux noverir que de 2 vair abling' t vase ipamer, es de
"Chenger $l$ denwin spiita pormei de vaces bair twote ta wib, bien tain de vous
13 aimer comme it voes, ita do'clane'. Sayp donc diabersie, croyy, masi, eter'van its cneome
is Constonte ct pursuadis que vous हैts aimic Vou, vercy, eneores ples expons i lo tieste
i) d lout $l$ monde et penticulitivenment de aluiquin'a fomais itaं A ne ure fomai;
$\Rightarrow$ Watre-lerivitenr


Expasé de la Meithode
nation de l'Alphabet. Clef. - Sois: "Etal.major Général" La clef adoptie On écrit es mat sur un papier qpadrilli en plasant chayplathe dases un carré. et a $t m \alpha j$ orge $n$ e r al
On upprime les lettres rijuties, en allant de gauche à droite., il vesté e $t$ a m $j 0$ r ${ }^{n} \mathrm{n} l$
On écrit are dessucs les
On écrit oue dessucs, les autres lathes de l'alphabet daus l'onine normal, en allant de, gauche ì droite, ct en formant autant $d$ ligne horizontales qu'il at nicessaire. On thepprime la littre $W$ ! on obtient ains:

On ulive enssicte a, letres par colonne, verticales, en commensant por len Colornce de qauche et lion obtient $l^{\prime}$ alphabet de 25 lettes suivant: e but edv a d $x m \neq y j h \geqslant 0$ i r $k g p h g_{\mathrm{g}} \mathrm{l}$ s que l'on mumérate de gaucho e oroite de maniere à abterier l'alphabet. clef.

iffrement d'un texte clair. - Soit à chiffrer le lexte twivant, arce la clef "etah majorgineral":
"Leney-vous prêt à attaquer l'emmeni demain matin"
In forme le tablean suivant :
tene z rou s p pretà atta querlen ue mi demain mation $\begin{array}{lllllllllllllllllllllllllllllllllllllll}4 & 1 & 22 & 1 & 15 & 6 & 16 & 3 & 25 & 21 & 18 & 1 & 4 & 7 & 7 & 4 & 4 & 7 & 23 & 3 & 1 & 18 & 24 & 1 & 22 & 22 & 1 & 10 & 17 & 8 & 1 & 10 & 7 & 17 & 22 & 10 & 7 & 4 & 17 \\ 4 & 5 & 2 & 3 & 18 & 24 & 15 & 18 & 18 & 14 & 7 & 8 & 12 & 19 & 1 & 5 & 9 & 16 & 14 & 17 & 18 & 11 & 10 & 11 & 8 & 5 & 6 & 16 & 8 & 16 & 17 & 2 & 9 & 1 & 23 & 8 & 15 & 19 & 11 \\ 10\end{array}$

Sa ligne (1) renferme le texte clair ícrit en siparant les letures.
Dand la ligue (2), on iuscrit au dessous de chaqje latse, sa valever numsirique dame l'alphabet_clef.
Oams la ligne (3), on inseriat des noubres abtewns de la manière wivante
Ta 1: lttre $t$, du texte clair at reprisenté porsa valeur 4, dom l'alphabet clef
la 2 leftre e, entreprisentie par ta valeur tam l'alphabet. def, au gmentó della valeur de les lettre pricidents $t=4$. On a done $1+4=5$
Qa 3 lettre $n$, eat uprisentic par la tomus des valuen des lettre purmíbentes et do la verune pripre, dovel 'ubphabet. def: $1+4+22=2 \%$; f'alphabet employi' n' ayant que 25 lettre, Il faut wetrancher 25 de ctte tounue: $27-25=2$. On inserit 2 dans la colonne correspendout- $\frac{1}{2}$ la lethe $n$.

It aiusi de viete, en remarquant of. it ruffit $\partial^{\prime}$ ajouter à la valuer de chayju latire le nombre inserit deye dami la celymme vatricale be ganch, sur la ligne (3) et qui uprinente $l$ vinttat des opiration prricidents.

K'opiration termince, on divise le crypto gramune en groupes uniformes do 5 lettres, en vumensant par la yauche, ct l'on ajoute des leths, wulles, s'il eat b'ens aire, poorcouplíter b derviorgroupe On abtient dinsi, itexte wivant:
tcqur-lzrrh-adyke-cxohi-rfmfd-cvodo-ibxeq-dzkfm:

Afin d'éviter de conmencer le eryptogranume por la meme lutro quo le texte clair, on
 In iuserive done $25-4=21$ c'cstà dire $p$, dom l'alphabet clef, au hèr de $t$, ehle textes lifinitif deviendra:
pctur-lzrrh-adyKe_exohi-rfmfd_cvodo-ibxeq-dzkfm.
e'chiffrement d'un Cryptogramme. - Soit à dichiffrer le texte huivant, icrit avec Pa clef "stat major Génerial".

$$
\operatorname{lqtga-dqvxb-nggse-kgiuk-yools-mihng-qvhte~}
$$

On form le tableau hierant:

Ta ligne (1) renferme le taxte chiffré, c'orit en 10 parant les letres.
Sam la liyne (2), on inserit an dersous d chaque lettre, sa valuer daus l'alphabet-clef Aans la ligue (3), on inscrit de, vombres obtenus de la manière vievante.

On sait que par convention, la prernirere lettre du texte chiffré vait ètre zempla c'e, parcell qui correrpund au compliment de sa valeur à 24 dose $l$ alphabet. clef. $25-24=1$. On p'crìt dunc 1 , à la ligne (3), dans la colomevesticale correspuniouste à la lettrel \& 2: vombre est abtenu en utronchant de la valever de la $2<l_{\text {ettse, } l a}$ valeuer di la lettre qui priside. $23-1=22$.

En appliquant la mime ligle pour la $3:$ lettre, on voit que $l$ 'opération est inppossibles th ajoute en comsiquence 25 an 3 vorubre : $4+25-23=2 g-23=6$

It aini de wite.
Surgue dams le wurant des apirations on rencentre une vorstraction qui dvemerait o pour
 chiffre.

Satraduction cherchic ert:
envoyez d'urgence renforts demandes. $d d z n$
Eegroupe ddzn uprizente de, leters nulles qui unt été ajoutécs pour completeràs, le numbir de, lettres due dervier groupre

Deservations Pratiques.
Pour éviter toule chances d'orreurs dans le chiffrement, il convient de vérifier les mombres obtenus, avant de b, umplacer par le, letre qu" ils représentent.

Ainni, suit à chiffrer, tovjoun avce la méme clef "étal-majer-géveral", lexte nuisant: Partez demain matin. An linpore l tabbau ver $s$ ligues, comme il mit:

Paritezdema i n matinvkc Un forme d'abord les ligues (1) (2) et (3), puien 217184115811071722107447226195 dam la ligue (5) on ericatat bíapivationsa dou 2132125116242510 17 96 | $p$ | $u$ | $p$ | $s$ | $e$ | $o$ | $l$ | $s$ | $m$ | $i$ | $x$ | $v$ | $o$ | o | 5 | $k$ | 0 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $n$ | 0 | $p$ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 21 | 7 | 18 | 4 | 1 | 15 | 8 | 1 | 10 | 7 | 17 | 22 | 10 | 7 | 4 | 17 | 2 | dichiffrendent es $l^{\prime}$ 'on doit vetrouver les doypjops insorits dom la ligne (2).

Cett virification faits, on umploc san, la ligus(L) les nombires, par les littres qjill, rporiventent.
hiffri: tupse-olsmi-xvogto - konop.
afin d'cuites Aonte erreve, il convient D'ajouter le, lettre, vulle, cormplimentaires, autante, clair, et de bes chiffrer counne $l$, autres.

Ig modification à approster à la 1 'letts ne ve fait qu'en dernier lieus.
Ie travail pact, itre facitité por l'empli d'un petil barème des roustractions, umblable a aleri qui est a joint



1111111111111


## 三

 ＂1＂＂＂，＂＂＂＂＂

，，1，，，，，，，
 いいいいいいい＂。島止がなったら
$\stackrel{1}{6}$


## ज なた た が 





 ＂1＂11＂111＂1み＂れ＂＂

 ＂11＂1＂＂1＂＂1＂いい＂




$$
\begin{aligned}
& \text { ※ }
\end{aligned}
$$



Srojer de systenne
Exyplograpphoque
Nrilitaire

Exposé de la Nrzétbode.
Yornalionde Pialphabet. Clef Sout "Etat. Nrajor Ginineal"," Pa clef adoptie
On èrit ces noto snven praqier quadrille' en plaçant chaque lelke dans un carré :
f $t$ a $t$ ma $j 0 \tau g$ i $n e x$ a $l$
On omppinme les lettres repreties, en allant de ganche à droite ; il reste
c! a $m j=\sim$ g $w d$
On çrit an dessons, les ankes lettreo de l'alphabet dans liordre nomal, w allant degancke à draite, et en formant antant de lignes horizontales gnil sot nécessaine on ompprime fa kettre W. Ow obtient ainsi:

$$
\left\{\begin{array}{lllllllll}
c & i & a & j & j & q & n & l \\
l & c & d & f & k & k & p & q & \\
w & v & x & y & z & & &
\end{array}\right.
$$

 it l'an obtiont P Cifpriabet de E 5 Peliries smeant.

que lionmmerito to ganche a droite, de man o obteric l'alphabet Clef.

Cniffenment dim teste chair soit ichiffer le texte smvant, avec la clef "Etat Mbajor General":
"Eenez-sons prét à altaquer l'ernemi demain motion."
On forme lo tablcon omvant:


Sa higne (1)renferme le toate chain ccrit en ocparant les letres.
Dans la ligne (2) on inserit an dessons dechaeqne lettre, sa salem munerigne dans l'alphabet Clef.
Danolakigue (3), on inocrit des nombres obtemus dela manière omvante:
Sa 1 ǐlextre $t$, dn teate dain est requésentée par sa oalen ft, dams l'alphabet Clef.
Sa $2^{2}$-lettre e, estreprésentéc pav sa valeun dans l'alphabet. clef, anginentée de la oalenr de Ra $l_{0}+t r e$ precidente $t=H$. On a donc $1+y=5$.
Sa $3^{2}=$ lettre $n$, est représentée par la somme de valemo des lettires précédentes et de la oicime propre, damo l'alyhabek.clef: $1+4+22=27$.
Solphabot employé $n$ 'ayant que 25 lettres, il fant retromeber 25 de cetter somme $: 27-25=2$ Gninscrit 2 dano la colonne correopondant à la lettre ne
Et ainoi de onite, enremanquant gni il onfit d'ajonter à la valar de choopre lettre, he nombre inocrit doja dans la colome verticale de ganche, on la ligne (3) etqui represente le rionltat de opérations priciédentes.
Sopération terminée, on diaise le coypitogramme en gronper miformes de 5 lettres, en commencant jar la ganclse, et lion ajonte des lettreo milles, oil eot mecessaine pran complitar le demier grouper.
Gn oftient ansu he textermont:

Gfin d'eviter de commencer le enyptogramme par la mêne lettre que le teate clain, on comvient de rempheces cette lettre par cethe quiest repriesentéciprar he complement de sa valem i 25 .
On écriva danc 95- $4=1$, eseot a dive p, dans l'olphaber. CPef, an hien de $t$ ot le kexte définitif deviendua:

Déctoiffrement Jim Crypotogranme... Sait à dectoiffier le teste omisant icrit avec he clef" Btat-Jrajor général."

$$
P_{g t g} g-d q 0 x b-n g g s=-h g i n k-y o o l \text {-...mibnq-qubte. }
$$

On forme $f_{e}$ tablean smivant:

Sa higree (1) enferme be texhe Aiffré, ecrit an séparant hes lettues.
Dano la ligne (2), monit an desons dechaqne hettre, va valen dans lialphabet Clef.
Dano he hgne (3), on inoent des nombres obtems de he mamercemoante:
On sait que prar comvertion, ha in lettre dn teatechifrè doit ĉre remplaceé prar celle gni corregrond an complènent de savalen ì 2 st dans $i$ calphabet Clef.
25-2н = 1 . Oncirit donc 1, i ha higne (3), dans ha colome vertieale conreoprondante ile lettre $l$. Se 2: nombe est obtern en retrancloant de he valen de la 2 : lettre, la saleuv de la lettre qui pricide $23-1=22$.

En applignant la méne kigle pon ha 3 "lettue, on ovit qinel'o peication eot mprassible On ajonte en consequence 25 an 3 nombre: $4+25-23=29-23=6$.
Et ainsi de onite.
Sorsque dams le comant des operzationo on rencontre me sonotraction gmidonmevait o poun réonltat, on remplace 0 par $25 . C^{\prime}$ cot he cas quise prochtit proules 22 : et 23 : hettres dn teate chifree.

Sa tradnction ch hee est:
Envoyez d'magence renforts demandés. Id $z y$.
Se grampe oJ 2 n représenke deo lettues unlles quisut été ajountés prourcompleter à 5 , le nombre des lettres du dermier guampe.

- Oberzations pratignes.

Gonvéviter tontes chances d'erreurs dano le chifpement, il comvient de verifier hes nombres abtems, avant de les remphacer prar les lettres qwilo represontent.
 onioant: Sartez deman matin. On diopose he tablean onv 5 hinneo, comme il onit:


Gfin d'civiter tonte errens, it comient d'ajonter les lettres nolles complénontaires an tesite. clain, et de hos chifrew comme les antres.

Sa madification is apporter e he ser̃ lettre ne oe fait qn'en demer hien.
 celni qui eot crijjaint-

Som nue depectse de phus de qo lettres, on bechifue pravoéves de qo lettres (4 peowperdes feltin)

|  |
| :---: |
|  |




$$
\delta_{1} \ddagger \mathfrak{\infty} \check{\infty}
$$

$$
\begin{aligned}
& \text { N } \\
& 1 \\
& 0 \\
& 11 \\
& 11 \\
& \text { S }
\end{aligned}
$$





$$
\bar{\pi} \bar{\sim} \bar{\sim} \dot{\sim} \in \infty \in \infty
$$

Dystéme cryptographique ne3.
Cinistudtion relotivic à lomplri du systime ne's eet cumica aus officies avce les hainnues f le frapier quabible' neccoscaine LI luer cet remis cogalument la difuche In' a chiffer aree a syeteine
Qhatue No 1 Peudatdergeiatimen.
Gtude di li Sudmuctione.
Omié du chiffermento.


Clombue de lethuses

Sevx dipicher cxactos- Denx dipiches en partié crooniés.
Qupiche ne?


Geni dépichus exachment chiffieis. Ane defriche moncé (bo lethses faunes).

Depriche 12.3. Nauntat des afiowationses
Duncé du Chiffremento
clombue de lettres


3 defichuo exactió - Tdifiche contruant dewx cumese mail restauts compuchmsitle.

Cuphlogiamme Nef Pentrat dooofeñatime.
Amée du dichiffroments


Clombe de letheso -
 3 difichers (acec 3 lethos invoniens) trithers:
1 deficicle dunt la fin at incomfuibicuritle.
Gupthonomme De: 6. Kantrat derspreationue.
Qmeí du dichiffrmento.

clombue de lectuese
 moth faini dames lime dicux.


[^0]:    ${ }^{1} \mathrm{~A}$ variant of the copperplate style was the official style in the British Empire at that time [Grö07].
    ${ }^{2}$ The specificities of these styles, along with their history and some examples, can be found in [Grö07].

[^1]:    ${ }^{3}$ Étienne-Gabriel Peignot 1767-1849.

[^2]:    4"Ces lettres présentent d'abord un sens, étant lues à la manière accoutumée; mais si ensuite on ne lit que la première, la troisième, la cinquième ligne, etc. c'est-à-dire, toutes les lignes impaires, ou (sic!) y trouvera un sens opposé à celui qu'a présenté la première lecture."
    5 "(...) mise en évidence par l'essai publié dans la Revue de Cavalerie (livraison de mars)".
    6 "Un autre avantage particulier du système, c'est qu'il n'est pas troublé par la transposition ou la suppression de quelques lettres (...)".
    7 "(...) on efface chaque ligne au fur et à mesure qu'elle est transcrite (...)".

[^3]:    8 "(...) pour presque toutes les méthodes, le principe est connu (...) pour la méthode nouvelle (...) il faut garder pour soi le principe".
    ${ }^{9}$ Archives nationales, reference LH/1375/17.
    ${ }^{10}$ Service historique de la défense - Archives de la Guerre (henceforth SHD-AG), 1 K 842, p. 5.

[^4]:    ${ }^{11}$ The document is not explicit as to how these letters should be chosen.

[^5]:    ${ }^{12}$ The padding does not really add any security, it is used to fit in a standard format.

[^6]:    ${ }^{13}$ Based on Josse's own experiments a decryption attempt takes fewer than 5 minutes; assuming a clerk works 5 hours a day, this amounts to 60 keys per clerk per day. Therefore using a team of 200 clerks, each one would have to process 655 keys. Given the scheme's simplicity (as the intended audience is field officiers) it should be no issue to find enough people and train them to perform decryption. Thus in 11 days the correct key is sure to be found. It is also likely that computations using related keys (e.g. partially correct keys) speeds up this process substantially.

