#### A French cipher from the late 19<sup>th</sup> century

Rémi Géraud-Stewart and David Naccache

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°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 n°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 (4a and 4b).
- (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 M(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 1a, 1b, 2, 3, 4a, 4b, 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, 4b 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.<sup>1</sup> 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.<sup>2</sup>

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 1a, 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.

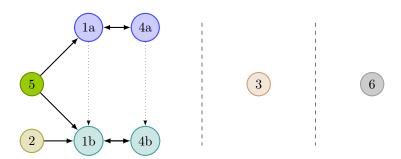
In particular, documents 3 and 6 do not seem to be related to the cryptographic system described in documents 1, 2, 4, 5. Document 6 bears a mention of Josse, and is thus not *completely* unrelated. However document 3 does not, and seems to be completely independent from the other documents.

<sup>&</sup>lt;sup>1</sup>A variant of the copperplate style was the official style in the British Empire at that time [Grö07].

<sup>&</sup>lt;sup>2</sup>The specificities of these styles, along with their history and some examples, can be found in [Grö07].

 ${\bf Table \ 1.} \ \ {\bf Handwriting \ analysis \ on \ the \ corpus.}$ 

Doc.	Author(s)	Style	Distinguishing features	Comments
1a	A1+A2	-	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 $ff$ , disconnected $qu$	Dated 188
4a	A2	-	Digits	-
4b	A3	Danish ronde	Digits	-
5	A6	-	Capital $M$ , $R$ , and $S$ , line form, character height-to-width ratio, spacing	Signed S. Mounier. Dated 29 Jun 1889.
6	A7+A8	-	Trailing letters $e$ , $s$ , $t$ , slant, final $ez$ digraph. Disconnected $ph$ , 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<sup>3</sup> in 1808 [Pei08, p. 40], although there might be even earlier sources. According to Peignot,

 $<sup>^3</sup>$ Étienne-Gabriel Peignot 1767–1849.

"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.<sup>4</sup>"

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... 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<sup>5</sup> 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<sup>6</sup> that seem to break ciphertexts generated by Josse's method. The encryption procedure seems different from Josse's<sup>7</sup>, 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

<sup>&</sup>lt;sup>4</sup>"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."

<sup>5&</sup>quot;(...) mise en évidence par l'essai publié dans la Revue de Cavalerie (livraison de mars)".

<sup>&</sup>lt;sup>6</sup> "Un autre avantage particulier du système, c'est qu'il n'est pas troublé par la transposition ou la suppression de quelques lettres (...)".

<sup>7&</sup>quot;(...) on efface chaque ligne au fur et à mesure qu'elle est transcrite (...)".

encryption grid, but on the cryptosystem's principle<sup>8</sup> – 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 1b and 4b. 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. 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<sup>10</sup> 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", 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.

<sup>8&</sup>quot;(...) pour presque toutes les méthodes, le principe est connu (...) pour la méthode nouvelle (...) il faut garder pour soi le principe".

<sup>&</sup>lt;sup>9</sup>Archives nationales, reference LH/1375/17.

<sup>&</sup>lt;sup>10</sup>Service historique de la défense – Archives de la Guerre (henceforth SHD-AG), 1 K 842, p. 5.

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:

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' of length N. Then P' 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<sup>11</sup> so that M is a multiple of 5. First compute

$$r_i = S(m_i) + r_{i-1} \mod 25$$

with the exception of the first,  $r_1 = 1 - S(m_1) \mod 25$ . The ciphertext is given by  $c_i = S^{-1}(r_i)$ .

• **Decryption:** Given a ciphertext  $c = c_1 \cdots c_M$  we first construct

$$d_i = S(c_i) - S(c_{i-1}) \bmod 25$$

with the exception of the first,  $d_1 = 1 - S(c_1) \mod 25$ . The message is finally recovered as  $m_i = S^{-1}(d_i)$ .

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".

 $<sup>^{11}\</sup>mathrm{The}$  document is not explicit as to how these letters should be chosen.

**Example (key generation).** Let us use the secret password P = KANGAROO. Then P' = KANGRO with N = 6. We get a table

K	Α	N	G	R	О
В	С	D	Е	F	Н
I	J	L	M	Р	Q
S	Т	U	V	X	Y
Z					

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

#### 4.3. Correctness

First note that  $d_1 = -S(c_1) = -S(S^{-1}(1 - S(m_1))) = 1 - S(m_1)$  so that  $S^{-1}(d_1) = S^{-1}(S(m_1)) = m_1$ . Then for every i > 1,

$$d_{i} = S(c_{i}) - S(c_{i-1})$$

$$= S(S^{-1}(r_{i})) - S(S^{-1}(r_{i-1}))$$

$$= r_{i} + 1 - r_{i-1} - 1 = r_{i} - r_{i-1}$$

$$= S(m_{i})$$

so that  $S^{-1}(d_i) = m_i$ .

#### 5. Implementation remarks

Josse makes several remarks about the use of his cipher in the field, with details about how computing first  $S(m_i)$  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<sup>12</sup>:

- 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.

 $<sup>^{12}</sup>$ The padding does not really add any security, it is used to fit in a standard format.

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,  $1 \le N \le 25$ . 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.

<sup>&</sup>lt;sup>13</sup>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.

- [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

ÉTAT-MAJOR GÉNÉRAL

DIRECTION

Télégraphie Militaire ---

Mon Educamdere,

7. ai l'hoaneur de vous adocues l' jour à titre de renseignement, une copie du procis verbal de mise en suri de crota suptime de cryptographie.

Beage thetasemen disone.

A. wowier

5, rue des Beaux-Arts

CAVALERIE

Note our un nouveu procéde oughtographique

of auteur est absolument convaince de l'indéchiffusbillé a de son systems at exoit formamont, judge a preuve du contravu,

gued que bout le nombre de dépietes tombéel entre les mains de l'en la question de la diduffracion n'en servet pas pour cota plus avance

an arentage que no presentent-pas les systèmes à double cleftes pl perfectionned, puisque chaque depiche intercepte augmente la prober

que l'on a de trestuire toutes les autres dépectes duffices d'après la systeme. La gaille même, qui presente tougons un problème alleg and I offer pad cette gunantie mide on dividence par l'essai publice dans la

de Cevalirie (livracion de mand), à tavoir : que si la parmore ligne mene decemberge - de la depiche remastraen claim en mine temps que

toute duffer outre les mans de l'omnemie, il ne venait pas très difficile bornon tout be rate, c'est à dire le ce construire le grille une fois pour t In pour jugge a un corteen pount se randou complet se atte inde bill en songeant que, Band le système, le même ligne de toute de hout the willy chiffide I in nombre on qualque sorte undefiniden queiqu'elle na soit copendant déchiffrable que d'une seule. Et, si lon i on peut choiser ontre as milliers d'orthe graphes différentes, celles qui Saint-Cyn our des clefs de quotre ou cinq lettres, Eli n'ompidoux pas

uns Bepiche wrive tranques amqueles por exemple de ses deux premission light of la sumplus n'en rett per moins livible, chose qui n'amail h'est pas trouble par la tronsposition on la suppression de quelques le conespondent, momo non provonce, de live auser factement dans un letters, eir constance qui rond purque toujours Mishe una Defre che chiffree Dans un system actre que lors simple clef. Paseillement, ti Cooperas Mr autre wanters, particular du système, c'est qu'il frent-the son analogic que daind les chiffraisons par dictionnaire. cas que dans un autre.

from differ on dichiffren, il faut un peu plus de temps que pour

Comme respitate, on ne peut quere too wer mieux. C'est à peure 11,

chiffier on dechiffeer to mime texte sand un systems à remple clef,

qui est secrète; pour la methode nouvelle, l'application n'a aucun tigni. toutes les methodes accommend, le principe est conner, et c'ext l'application fration, mais il faut garden pour soi le principe qui repose sur l'obsern ration d'un fail materiel of unique. Soul est dans la lets du Affreur bond les autris 440 temes, ca mot o'entend du materiel, c'est à dire at the sold than ; sount I settle molecuel qu'une and othe pour levie Il est mai que le systems exige le secret; mais, tambis que, de la defel de l'alphabet, du dictionnaire et de la guille, ici, il resymplique qu'au princère même i on d'autres termes, pour prosque on to mem lettre consepond toujours a la mêma lettre,

qu'elle est transcrute, me ou celle pre coulour n'est per indu ponsable, car l'ennemi, bem que possesseur d'un demblable do cun n'en serout par beau coup plus avance. Pour tout dire, l'auteur a la conviction absolue que ce secret, qui pout être livel, traki, pout on au cun cod the surpoist. C'ort pounquoi, dans de ponsee, un tot systems on degreet pas être utilise dous toutes los despetes couran mais where four la consepondance des quartient-generaux; & for terment sinds par l'intermedraire d'un petet nombre de penerm parfartement two, it deflicrait tooke interception of nothing beinen i Peprune Co patience of la sagacte see plus Robelles Sciriffrance

Méthodo Stigorographique the same strength processed of the State of If not him were your prime where Vary what describes I defect the me the Maria Shaw who he are invested making the state had is some officer to some of realist in the thought desire quite former it may her trule as in this lain at many disabini, orange, mon', obe som its come Conduct of provides on cases the server They leave more plan is horis . To were de lout I monde at frank substances it de The ger is a formain the it so near formani

moderna'selle Je m'empresse de vans verire pair vans doctarer " que vans vous trompey beautoup to vans crayes I que vous êtes celle pour ye'je unfire 11 Il at him was you pour vous sprewer 5 je vaus ai fait mille aven après que 'vous ches devenue l'objet de ma raillerie aine 7 ne doutez plus de a que vaus dit ici celui que n'à cu que de l'aversion pour vous et g qui aimerait mien mouris que el changes I vair ably! I vous spourer, et de " Changer le dessein qu'il a forme de vous hair toute sa vis, bien lain de vaux 13 aimes, comme il vaus l'a diclane. Lays donc disaburie, craye, mui, cheiraus ites encone is constante et premeadie que vaus êtes ainie Nous were enewer plus exports i la risse I de tout to monde et particulièrement de alui qui n'a jamais été ch ne un jamais of Vatre less tens

Trojet de Système ryptographique metaire

```
Enposé de la Méthode
on évrit ces mots sur un papier quadrillé en plaçant chaque lettre dans un carré.
      Et a t maj or generalent de ganche à droite, il reste et a mjor que l'este
     On écrit au dessois, les autres lettres de l'alphabet dans l'ordre normal, en allant de gandre à droite, et en formant autant d'higne horizontales qu'il est nicesaire. On supprime la lettre W. On abtient ainsi:
      e tamiorque
     6 cdf Hikba
     (uvzyz
                         On relive ensuite ces lettres par colonnes verticales, en commençant por la
     Colorne de gauche et l'on obtient l'alphabet de 25 lettres suivant.

e b u t c v a d x m g y j h z o i r k g p n g l s

que l'on numérate de gauche è droite, de manière à aleterier l'alphabet clef.
     Alphabet-elif { et ut c v ad x m f y j h z o i T k g, p n g l s 
 1 2 3 4 5 6 7 8 g 10 11 12 13 14 15 16 17 18 19 28 21 22 23 24 25
iffrement d'un texte clair. - Soit à chiffrer le texte reivant, avec la clef "etal major général".
"Venez-vous prêt à attaquer l'ennemi demain matin"
              On formé le tableau minant:
tenez vous prétà attaquer le nnemi demainmatin
4 1 22 1 15 6 16 3 25 21 19 1 4 7 7 4 4 7 25 3 1 18 24 1 22 22 1 10 17 8 1 10 7 17 22 10 7 4 17 22
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
t c b u r l z r r h á d y k e c x o h i r f m f d c v o d o i b z e q d z k f m
  La ligne (1) renferme le texte clair c'evit en siparant les lettres.
  Danster ligne (2), on inscrit au dessous de chaque lettre sa valeur numérique dans l'alphabet clef.
   Dans la l'épre (3), on inscrit des numbres obtenus de la manière reivante,
        la 1º lettre t, de texte clair est représenté por sa valeur 4, dans l'alphabet clef.
La 2º lettre c, entreprésentée par sa valeur dans l'alphabet clef, au grantée de la valeur de la
        lettre provident t=4. On a done 1+4=5
        La 3' lettre n, ent représentée por la romme des valuers des lettres providents et de la neune
       Jumpne, don't 'alphabet. clef: 1+4+22 = 27.
L'alphabet employé u'ayant que l'o letters, il faut retrancher 25 de cette somme: 27-25=2.
        On inserit ? dans le colombre correspondant à la lettre n.
              It aims de wite, en remarquant ejs it ruffit d'ajouter à la valuer d'chaque lettre, le nombre inscrit dejà
dans la cologne verticale te ganche, sur la l'ope (3) et qui représent l'inttat des opérations précidents.

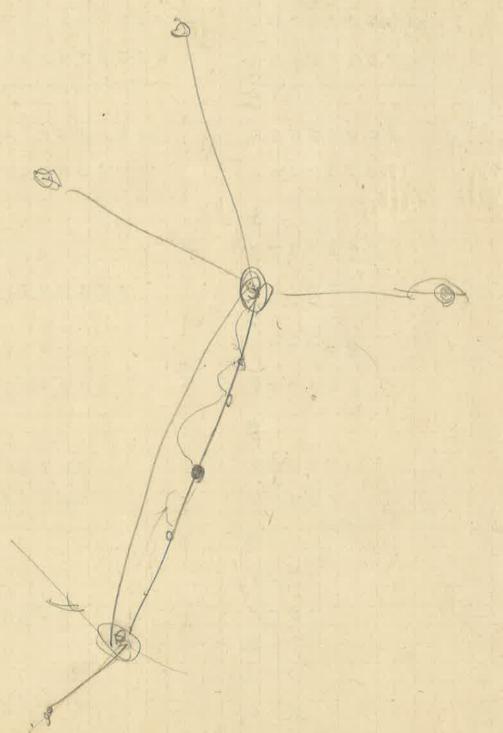
L'opération terminée, on divise le crypto gramme en groupes uniformes de 5 lettres, en vermen sant par la ganche, et l'on a joute des lettres, mulles, s'il est récessaire, pour complétes l'dernier youque
         On obticul dinni, I texte without:
tebur-lzrrh-adyke-cxohi-rfmfd-cvodo-ibxeq-dzkfm.
afin d'éviter de commencer le creptogramme por la même lettre que le teste clair, on convicut de remplocer tette lettre por celle qui est représentée por l'emploment de sa valeur à 25. In inscrire donc 1 25-4 = 21 c'est à dire p, dans l'alphabet cles, au lieu de t, et le teste l'élimité desciendre:
diffinitif deviendre:
pictur-lerrh-adyke-exohi-rfmfd-evodo-ibxeq-dzkfm.
```

Soit à déchiffrer le tente suivant, écrit avec la e'chiffrement d'un Crypto gramme. \_ clif "Stat major général". lgtga-dgvxb-nggse-kgiuk-yools-mihng-qvhte On form le tableau min ant: l q t q a d q v x b n q q s e k q i u k y o o l s m i h n y q v h t e 2425 4 26 7 8 23 6 g 2 22 23 28 25 1 19 20 19 3 19 121 16 16 24 25 10 19 14 22 23 28 6 14 4 1 1 22 6 16 12 1 15 8 3 18 20 1 22 5 1 18 1 22 11 16 18 4 25 8 1 10 9 22 8 1 25 8 8 15 22 lenvoyez dur genceren forts de mandes ddzn la ligne (1) renferme le texte chiffre, c'er it en réparant les tettres. Dans la ligne (2), on inscrit au dérious d'chaque lettre, sa valeur dans l'alphabet - clef Dans la lique (3), un inscrit des nombres obtenus de la manière minante. On soit que por convention, la promière lettre du tente chiffre doit être remplocée sporcell qui correspond au complément de sa valeur à 24 dons l'alphabet. cles. 25-24=1. On évrit donc 1, à la ligne (3), dans la colonne verticale correspondante à la lettre l Le 2º nombre en obtenu en retronchant de la valeur de la 2° lettre, la valeur de la lettre qui précide. 23-1=22. En appliquant la même rigle pour la 3: lettre, on voit que l'opération est impossible. On ajoute en conséquence 25 au 31: Nobelore: 4+25-23=29-23=6 It aimi de wite. Longue dans le courant des apérations on rencontre une voustraction qui donnérait o pour vinultair on uniplace o par 25. C'est le cas qui re produit pour les 22° et 23° lettre, du texte chiffre. La traduction cherchie ert: envoyez d'urgence renforts demandés. ddz n le nombre des lettres du dernier groupe Observations Tratiques. Your d'viter toules chances d'erreurs dans le chiffrement, il convient de vérifier les rombres obtenus, avant de les remplacer par les lettres qu'ils représentent ainsi, soit à chiffrer, toujour avec le mime cles "étal-major-général" l'tente mirant: Partez demain matin. On dispose l'habban un 5 liques, comme il mit. Partezdemainmatinvkc On forme d'abord les liques (1) (2) et (3), pries dans la lique (5) un exicute le apération des du dichiffrendent et l'en doit retrouver les différences. 21 7 18 4 1 15 8 1 10 7 17 22 10 7 4 17 22 6 19 5 21 3 21 25 1 16 24 25 10 17 9 6 16 23 2 19 16 22 16 21 Pupse olsmix vog 6 Konop inscrit dons la liegne (2). Cette Virification faite, on remplos dans la lique (4) (21 7 18 4 1 15 8 1 10 7 17 22 10 7 4 1722 6 19 5 les numbres, par les lettres qu'il, représentent. liffi: tupse-ofsmi-xvog6-konop. a fin d'évites toute enveux, il convient d'ajoutes les lettres rulles complimentaires, cui tente, clais, et de les duffrer commo le, centre,. La modification à apporter à le 1" lettre ne se fait qu'en dernier lieu.

Le travail plant itre facilité por l'emples d'un petit barine des sourractions umblable à alui qui est ci junt
une dépâche un fin la la longue de l'entre chiffre partironifies de 30 lettres (4 groupe de s'entre)
une dépâche un fin la longue de l'entre chiffre partironifies de 30 lettres (4 groupe de s'entres)
une dépâche est seule modifiée, en pronour le compliment de se value par rapport à 25 : les principales de sources de sources de sources de sources de seule modifiée, en pronour le compliment de se value par rapport à 25 : les principales de sources de seule modifiée de sources de sources de seules partires de seule modifiée de sources de seules partires de seules partires de seules de se

かいいいといいといいで dy ny ny my my my my my my 2252525252 222222222 D D H a n n n n n H おいいいいいいるいだ 222222222 10 11 12 11 11 11 11 11 11 11 さる こる こっと こっちょ 22222323 n p n p n n n n 22223 11 11 11 22 624 u n n n u U 32222 2 23 25 6 9 6 6 P 25 27 27 22 23 o n n n 25 24 27

se 11



Projer de système
Cryptogræphique.
Militaire

## Exposé de la Methode.

```
Formation de l'alphabet. Clef. Soit "Étal. Major Général", la clef adoptée
On écrit ces moto sur un papier quadrille en plaçant chaque lettre dans un carré :
             État majorgénéral
            On oupprime les lettres répétées, en allant de ganche à droite ; il reste
             e lamjorgn e
            On évrit an dossous, les antres lettres de l'alphabet dans l'ordre normal, on allant de ganche à droite, et en formant antant de lignes horizontales qu'il est nécessaire. On supprime la
            lettre W. On obtient amoi:
             le tamporgnt
            le c d f h i h p q s
            u v x y z
                  On releve onomte ses lettres par colornes verticales, en commençant par la colonne de ganche
            et l'on obtient l'alphabet de 25 lettres onwant:
             ebuterademfy jbzor: hypny lo
            que l'on numerate de gamelse a droite de man le a obtenu l'alphabet Clef.
            Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s

Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s

Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s

Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s

Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s

Alphabet Clef. { e f n l e v a d x m f y j h z v i z k g p n g f s
  Chispernent d'un texte clair Soit à chisper le texte survant, avec la cles "État Noajor General":
                           "Eenez-sons prêt à altaquer l'ennemi demain matin. "
                           On forme le tableau omeant:
mitenezvonopretä attagner lenne midemainmaten
(2) # 1 20 1 45 6 16 3 36 24 18 1 # 7 7 # 17 23 3 1 18 24 1 20 20 1 10 17 8 1 10 7 17 22 10 7 4 17 28
(3) H 5 2 3 18 24 15 18 18 14 7 8 12 19 1 6 9 16 14 17 18 11 10 11 8 6 6 16 8 16 17 2 9 1 18 8 16 19 11 10
(4) (teburlz rebady he coobir fullovodo i bzegdz k fm
           La home (1) renferme le toate clair écrit en opparant les lettres.
           La higne (1) renserme le toate chair ecent en separant les lettres.
Dans la ligne (2) on inscrit an dessons de chaque lettre, sa valeur munerique dans l'alphabet. Clef.
           Dans la ligne (3), on inscrit des nombres obtenns de la manière onvante:
           La 10 lettre V, du toate dans est representée par sa valeur st, dans l'alphabet Clef.
           La 2º lettre e, est représentée par sa valeur dans l'alphabet. Clef, anginentée de la valeur de la
            lettre précédente 1= H. On a donc 1+ H=5.
           La 3º lettre n, est représentée par la comme des valens des lettres précédentes et de la vienne
            propre, dans l'alphabet Clef: 1+4+ 22=27.
           L'alphabet employe n'ayant que 25 lettres, il fant retrancher 25 de cette somme: 27-25=2
           En inscrit 2 dans la colonne concopondant à la lettre n
Et ainsi de suite, en remarquant qu'il suffit d'ajonter à la valeur de chaque lettre, le
nombre inscrit doja dans la colonne serticale de ganche, sur la ligne (3) et qui représente le
résultat des opérations précédentes.
           L'opération terminée, on divise le cryptogramme en groupes uniformes de 5 lettres, en commencant par la ganche, et l'on ajonte des lettres milles, s'il est nécessaire pour
            complétor le denner groupe.
            On obtient amor le texte onwant:
            t c b u z - lzzz b - ady ke - exobi-zfmfd-cvodo-ibxeg-dzkfm.
```

Cafin d'éviter de commencer le cryptogramme par la même lettre que le texte dair, on convient de remplacer cette lettre par celle qui est représentée par le com-

En ecriva donc 25-H= M, C'est à dire p, dans l'alphabet. Clef, an lien de 1

plement de sa valem à 26.

et le texte definitel deviendre:

le texte sinicant ivit avec la Clef "Etat-snajor General." Soit à décloifier

lgtga-dqvxb-nggse-kgink-yools-mibng-qvbte.

On forme le tablean suivant:

(4) | lgtgadqvæbnggsekginkyoolsmihnggobte.
(1) | 24 23 4 69 8 23 6 9 2 22 23 1025 1 19 10 17 3 19 12 16 16 24 26 10 17 14 22 23 23 6 14 4 1 (3) 1 22 6 16 12 4 16 8 3 18 20 1 22 6 1 18 1 20 11 16 18 4 25 8 1 10 7 30 8 4 26 8 18 15 40 14) (envoyez dur gencer enfortodema in de sodzy

La ligne (1) renservae le texte chispré, cerit en opparant les lettres.

Dans la lique (2), ou mount an dessons de chaque lettre, sa valem dans l'alphabet Clef. Dans le lique (3), on inscrit des mombres obtenno de la manière omvante:

On sait que par convention, la soi lettre du texte chifre doit être remplacee par celle gov correspond an complement de savaleur à 24 dans l'alphabet Clef.

25-24=1. On évrit donc 1, à la higne (3), dans la colonne verticale correspondante à la lettre l. Le 2° nombre est obtern en retrandoant de la valeur de la 2° lettre, la valeur de la lettre

gm precede 23-1=22.

En appliquant la même règle pour la 3º lettre, on ovit que l'opération est impossible On ajonte en consequence 25 an 3º nombre: 4+25-23=29-23=6.

Et anni de omite.

Lorsque dans le consant des operations on rencontre une sonstraction qui donnerait 0 pour resultat, on remplace 0 par 26. C'est le cas qui se producit pour les 22 et 83 : lettres

du texte chifié. La traduction che chée est: Envoyez d'ungence renforts demandés. Il z 9.

Le granpe ddz 5 représente des lettres milles qui ont été ajoutées pour complèter à 5, le nombre des lettres du dernier granpe.

## Obsergations pratiques.

Som éviter toutes chances d'evens dans le chifrement, il convient de verifier les nombres abtenno, avant de les remplacer par les lettres qu'ils representent. Amoi soit à chifrer, tonjours avec la même clef "État-Major General, le texte suisant: Partez demain matin. On dispose le tableau sur 5 hignes, comme il onit:

(1) (Sartozdemainmatinoke (e) 21 7 18 14 1 16 8 1 10 7 17 22 10 7 14 17 22 6 19 5 (3) 11 3 4 25 1 16 24 25 10 17 9 6 16 23 2 19 16 22 16 21 (4) p w p 2 c o l o mix v o q l K o n o p 15) 11 7 18 11 1 15 8 1 10 7 17 22 10 7 11 17 22 6 19 5

On forme d'abord les lignes (1) (1) et (3) puns dans he highe (5) on exeente les operations du dechiper. ment at lon doit retrouver bearon bees inents dans la ligne (2). Cette ven fication faite, on remplace dans he higue (H) les nombres par les letter gril, representent

### Coxtechifie to poe - olomi-xooql-Kanop.

Ofin d'eviter toute even, il convient d'ajonter les lettres milles complémentaires au texte clan, et de les chifrer comme les antres.

La modification à apporter à la 100 lettre ne se fait qu'en dernier lien.

Le travail pent être facilité par l'emploi d'un petet barême des sonstractions, semblable à celni qui est ci joint.

Donn une déposebre de plus de lo lettres, on la chifire parserres de lo lettres (4 groupes de so lettres)

2

# Système cryptographique 1:3.

I wistruction relative à l'emploi du système 11:3 est remise aux officies anc les barêmes y le papur quadrellé nécessaire Il leur est remis également la dépiche 11 à chifur avec ce système

4! 4 de Chotet

Dépiche Nº 1. Résultat des spérations.

Chuse de l'Instruction de 8 91 6

Durés du chiffement 2:55 31 6 Chairm

31 57 Cafriso
31 59 de Bussy

Durei mayame du chiffement - 39' \ 1 à 2 letter far minut

Deux dépiches exactes \_ Deux dépiches en partie erronces.

Depeche Nº 2.	Répultat des opérations.	Commence	Tin	Spéraleure.
	Durée du Chiffrement	2411	216	Chairon
(40)		/	216	Salmi
	, As		31.2	de cholet
			33.10	de Bussel.

Durei moyenne du Chiffrement. 45 là 3 lettres par minut

Cen's dépiche machement chiffier. Une dépiche monée (20 letter fairnes).

Dépêche 11. 3.	Résultat des opérations			
		Commonce ment.	Fin	sperature.
	Durce du Chiffement	331	316	Safour Chavion
		2	3. /2	Chairon
			3. 17	de Cholet de Busny
	Nombre de lettres	- 10/	Ja3 les	thyparmini
	Que' mojenne du chiffument -	45		1 por manier
	3 defeches exaction - 1 depiche con	ntenant o	deux erre	und mail
	restant comprehensible.			
Cryptogramme M!	Kenetat desoférations.		<b>—</b>	
		Commence. _ment.		Operateurs.
	Pure du dechiffemente -	9.18	1437	Chairon A Cholet
	~~		2240	de Cholet
			9h 40	Lafout
	Nombre de Settors		347.	de Bussy
	Nombre de letters ;	100	2014	1 2 4
	Duree moyenne du déchiffrement.	38, ( La	r lettus	hav minite.
	3 depicher (avec 3 letter errone	us) du	rilles;	
	I dépêche dont la fin est inci	mpréhe	with.	
Cryphogramme Nº 6.	Kerultat des operations.	(c.		al.
		Commence -	Fin.	Speriateurs
	Duré du déchiffement	3:11	3433	Chairon
		1	1134	Chairon de Cholet
			3648.	Safour de Bury

Oweimyennede dichiffement 2003 letter /3 farminule.

Les 4 cryptogrammer sout hin déchiffeir, sauf un mote fasse dans four d'en d'en .