"I shall love you up to the death"
(Marie-Antoinette to Axel von Fersen)

Jacques Patarin[1], Valérie Nachef[2]

(1) Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
jacques.patarin@prism.uvsq.fr
(2) CNRS(UMR 8088) et Département de Mathematiques
Université de Cergy-Pontoise
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
valerie.nachef@u-cergy.fr

Abstract

In this paper, we explain the encryption algorithm used by the Queen of France, Marie-Antoinette, to send letters to Axel von Fersen during the French Revolution. We give the complete deciphering of some letters for which we found differences with the text taken from historical books. We also provide the deciphering of one letter that seems to be unknown so far. The results we get bring new proofs on Marie-Antoinette's deep affection for Fersen. Finally, we mention some open questions about Marie-Antoinette's correspondence with Axel von Fersen.

Key words: secret key cryptography, polyalphabetic system, Porta ciphers, Marie-Antoinette encrypted letters.

1 Introduction

In this paper, we study some letters sent by the Queen of France, Marie-Antoinette (1755-1793), to Count Axel von Fersen between 1791 and 1792. After the failure of the escape to Varennes, the royal family is taken back to the Tuileries and is under serious guard. In spite of this situation, Marie-Antoinette succeeds to send letters to Fersen. Some of them are enciphered; others are plaintext or written with invisible ink. Most of the time, these letters show that Marie-Antoinette is trying to find alliances with foreign countries in order to restore the Monarchy in France. But some parts of her letters are devoted to expressing her love for the count. A French TV channel asked us to explain Marie-Antoinette's encryption algorithm. This led us to the study of some letters. There are very few letters written by the queen which are still available. Most of them were destroyed. Fersen kept the letters he received and deciphered, and also the letters he wrote himself to Marie-Antoinette. These archives were kept by his nephews and great-nephews. In 1877, Baron von Klinckowström published all the letters, but some parts were missing or crossed out. In 1982, some descendants of Baron von Klinckowström auctioned letters that were supposedly destroyed, and the French Historical Archives bought them.

It is surprising to notice that on one hand, historians who published Marie-Antoinette's letters always chose the deciphered version published by Baron von Klinckowström and on the other hand, cryptographers who were interested in the encryption algorithm never tried to verify the decryption when it was possible to have both the plaintext and the ciphertext.

In this article, we explain how the letters were enciphered, and we give some examples where there are differences between the deciphered text and the text published by historians. We also found a letter we think was not published in deciphered mode since we did not find it in historical books.

2   Historians and cryptographers' point of view

Many books containing letters written by Marie-Antoinette to Fersen but also to her family and counselors before or during the French Revolution have been published (see for example [4] or [5]). Some of these letters are also available on the Internet (http://axelvonfersen.free.fr/reine.php or http://www.freewebs.com/vonfersen/indexeng.htm). We always find more or less the same versions. We can notice that some parts in the encrypted letters are missing and have been replaced by suspension points (...). Is it due to a loss of the text or to a dissimulation? It is surprising to remark that historians did not try to study the encryption algorithm or the enciphered texts. Also in books on historical cryptography, there are few details on this encryption algorithm. It is only explained that it is a polyalphabetic system, and the three first lines of the encoding table are given. But again there is no attempt to compare, when it is possible, the plaintext and the ciphertext. Yet it could be interesting to obtain new development on this disturbed period.

According to Marie-Antoinette, this work of copying and enciphering was tedious, and she complained about it in a letter to Fersen dated November 2, 1791, [4] p.662: "Farewell, I am getting tired of ciphering; this is not my usual occupation and I am always afraid of making mistakes."

3   The polyalphabetic system

Historical books of cryptography ([1, 3]) explain that Marie-Antoinette and Fersen used a polyalphabetic system. Such an encoding was considered practically unbreakable at that time. The opinion of these books is that Marie-Antoinette employed a very strong encryption algorithm. Also, she did not suffer from any cryptanalysis of her letters (unlike the Queen Mary Stuart in England during the 16th century).

The polyalphabetic system needs two different keys: an enciphering table which is fixed and a keyword which changes with each message.

Fersen's enciphering table

It seems that Fersen used the same enciphering table with all his partners. Only the first three lines of the table are given in books of historical cryptography (see [1, 3]). While we were deciphering some of Marie-Antoinette's letters, we calculated other lines of this table. We found at the French National library the complete table published by Y. Gylden [2] in "La revue de criminalistique" in 1931, thanks to a reference from [3]. The table (see Table 2 below) was found in Fersen's private papers. One can wonder how Marie-Antoinette had hidden this table. Is there a simple way to remember it?

The use of the keyword

We repeat the keyword under the cleartext as many times as needed. For example, if the keyword is *hello* and the cleartext is "greetings from the king", we will need to repeat the keyword four times as shown below (see Table 1).

Table 1: The use of the keyword

g	r	e	e	t	i	n	g	s	f	r	o	m	t	h	e	k	i	n	g
h	e	l	l	o	h	e	l	l	o	h	e	l	l	o	h	e	l	l	o

Notice that the spaces between the words of the cleartext are not taken into account in the ciphering process. This means that the person who will decipher the message has to put back the spaces.

Then the letter of the keyword is found in the first column of the table. On the row determined by this letter, there are pairs of letters. The plaintext letter is sought in this row, and the cipher letter is the other letter of the pair. In our example, in order to cipher "g", we take the letter "h" of hello that is under g, and in the table we get the pair "GH". Thus the encryption of g is H. In Section 5, we will provide more detailed examples.

Remarks

1. In Y. Gylden's paper, it is also explained that besides the encoding table, Fersen had a list of letters where the names of important persons were represented by one letter. For example, for the king it was N, for the queen the letter was O and so on. It does not seem that this list was used in the letters that we studied.

2. Marie-Antoinette's encryption algorithm was a Porta-like system, but here the order of the letter does not show any logical progression.

Table 2: Fersen's encoding table

A	AB	CD	EF	GH	IK	LM	NO	PQ	RS	TU	XY	Z&
B	AC	BK	DU	EI	FL	GN	HO	MY	PS	QX	RT	Z&
C	AD	BG	CZ	EK	FM	HT	IX	LR	NP	OQ	S&	UY
D	AE	BZ	CT	DK	FI	GS	HY	LQ	MX	NR	O&	PU
E	AF	BL	CI	DH	EU	GK	MT	NQ	OR	P&	SX	YZ
F	AH	BF	CL	DG	EQ	IY	KP	MU	NS	O&	RX	TZ
G	AG	BI	CL	DN	ER	FP	HT	KU	M&	OX	QY	SZ
H	AI	BT	CS	DO	EL	F&	GH	KM	NQ	PR	UY	XZ
I	AK	BT	CS	DX	EI	FL	GZ	HY	M&	NP	OQ	RU
K	AL	BO	CP	DG	ER	FS	HU	IX	KY	MZ	N&	QT
L	AM	BZ	CD	EG	FI	HK	LN	OR	PS	QU	TY	X&
M	AN	BO	CP	DQ	ER	FS	GT	HU	IX	KY	LZ	M&
N	AO	BC	DM	EP	FS	GN	HY	IU	KT	LQ	R&	XZ
O	AP	BL	CK	DQ	ES	FU	GX	HZ	I&	MO	NR	TY
P	AQ	BX	CU	DZ	ES	FO	GY	HT	IN	KR	L&	MP
Q	AR	BZ	CT	DH	EU	FQ	GO	IL	KN	MP	SY	X&
R	AS	BN	CQ	DT	EU	FY	G&	HO	IP	KR	LX	MZ
S	AT	BP	CQ	DR	E&	FS	GU	HX	IY	KZ	LN	MO
T	AU	BY	CM	DX	E&	FH	GQ	IR	KZ	LS	NP	OT
U	AX	BL	CO	DQ	ES	FU	GT	HY	IN	KZ	M&	PR
X	AY	B&	CZ	DE	FX	GU	HI	KT	LS	MR	NP	OQ
Y	AZ	BU	CG	DH	EX	FY	IO	K&	LN	MP	QS	RT

4 The letters found at the French Historical Archives

On one hand, we had the letters published in historical books, and on the other hand we had hints on the encryption algorithm. At the French Historical Archives, we found some encrypted letters on which the keyword was written. We were able to compare what we obtained, once we had decrypted them, with the texts taken from historical books. We produce here two examples. The first one (Figure 1) is an extract of a letter that Marie-Antoinette wrote to Axel von Fersen on July 8, 1791. We have the ciphertext, the keyword "*courage*" (courage) written under it and above the cleartext we obtained. In Figure 2, this is a letter written by Axel of Fersen. Here we have the plaintext and the keyword "*autres*" (others) written under the cleartext. We did not find the corresponding encrypted letter. Here we can notice that some parts of the text had been crossed out.

Figure 1: Extract of one of Marie-Antoinette's letters to Fersen on which we added the cleartext - July 8, 1791

Bruxelle ce dix oct=

me voila enfin de retour

...

vous plains d'avoir été forcé de sanctionner
mais je sens votre position elle est affreuse et
d'n'y avoir pas d'autre parti j'ai d'ailleurs la
consolation que quelques gens raisonnables sont
du meme avis, mais qu'allez vous faire, tout
espoir est il perdu s'il en reste ne vous laisses
vous abbatre. et si vous voules etre aidé j'envoie

Figure 2: Letter of Fersen to Marie-Antoinette - October 10, 1791

5 First example - First surprise

On one hand, we found at the French Historical Archives some encrypted letters with keyword; on the other hand, we found in historical books the plaintext. Since the dates were written in cleartext on the cipher letters, we could form the plaintext-ciphertext pairs together with the keyword. Thus we were able to study the encoding method more precisely. We could check that it was effectively a polyalphabetic system. Surprisingly, we noticed that apart from the letter of June 28, 1791, only one letter in two was encrypted in the texts. This was not mentioned in books of historical cryptography (actually we discovered later that Y. Gylden mentioned this fact in "La revue de criminalistique" [2]). Marie-Antoinette's good reputation for encryption algorithm is weakened. Today, the modern cryptanalysis can retrieve the cleartext when only one letter in two is encrypted.

Let us give an example. We consider the letter written by Marie-Antoinette to Fersen on June 29, 1791. The keyword is "*depuis*" (since).

Table 3: Example of deciphering

Ciphertext	L	&	C	F	E	B	P	S	R	&	E	B	T	&	R	E	Q	E	E
Keyword	-	s	-	d	-	e	-	p	-	u	-	i	-	s	-	d	-	e	-
Cleartext	l	e	c	i	e	l	p	e	r	m	e	t	t	e	r	a	q	u	e

Ciphertext	U	E	B	L	I	C	I	V	&	U	X	A	K	R	N	V	E
Keyword	p	-	u	-	i	-	s	-	d	-	e	-	p	-	u	-	i
Cleartext	c	e	l	l	e	c	i	v	o	u	s	a	r	r	i	v	e

This sentence means: " May heaven grant that this letter reaches you."
To study this letter we have the cleartext-ciphertext pair together with the keyword. In order to decipher the text, we write the keyword under the ciphertext but we use only one letter in two of the ciphertext. We use lower-case letters for the cleartext and capital letters for the ciphertext. We notice that when we have the letter "d" in the keyword, if there is the letter "i" in the cleartext, it becomes "F" in the ciphertext. Also, with "d" in the keyword "f" becomes "T". Similarly, when we have the letter "p" in the keyword, the letter "r" is encrypted with "K". Encryption and decryption are symmetric processes. We need to have the encoding table in order to know which substitution to apply. In the encoding table, in the row corresponding to a letter of the keyword, letters are written by pairs. Since when we have a letter in the cleartext, the other letter of the pair is the enciphered letter and conversely.

Without knowing the complete table, we are able with the help of several pairs of plaintext-ciphertext together with the keyword (for example: courage, depuis, vertu) to find the substitutions corresponding to the following letters in the keyword: A, C, E, G, I, O, P, R, T, U and we got partial information for the letters D and S. As we explained in Section 3, we got later the whole table from [2]. Thus this table was fixed once and for all and it was found first in Fersen's private papers.

We can also notice from the table that "i" and "j" are enciphered with the same letter. This is also true for "u" and "v". The letter "w" does not appear in the alphabet used for the keyword.

As we can see on the examples of Figures 1 and 2, one has to get used to the calligraphy of the 18th century.

Table 4: The substitution corresponding to the letter E in the keyword

E	AF	BL	CI	DH	EU	GK	MT	NQ	OR	p&	SX	YZ

6   New results

The total deciphering of all the letters for which we had the ciphertext allowed us to complete some of them. We give them in chronological order.

6.1   Letter of June 28, 1791

In this letter that we suppose is addressed to Fersen all the letters are encrypted. This is the only example of that kind that we have. Here we find some differences between the text taken from historical books and the deciphered letter.

The following text is taken from [5] page 125 or [4] page 544:

"Do not worry about us. It seems that the chiefs of the Assembly want to behave more softly. Talk to my parents about foreign approaches (unreadable). If they are afraid it is necessary to come to compromise with them."

When we decrypted this letter with the keyword "*vertu*", (virtue), we get:

"Do not worry about us. It seems that the chiefs of the Assembly want to behave more softly. Talk to my parents about foreign approaches(6 encrypted letters). If they are afraid it is necessary to come to compromise with them. **Burn all that is (10 encrypted letters) and send the remainder of the letter to M. von Fersen. He is with the king of Sweden**."

One may ask the following question: Who is the addressee of this letter? We could not decrypt several words even after several shifts of the letters of the keyword.

6.2   Letter of June 28, 1791

Here is the text we got from the historical books [5] page 126 or [4] page 545:

"I am alive......Oh, how anxious I have been for you, and how sorry I am about all you must have suffered in having no news from us. May heaven grant that this letter reaches you. Do not write to me, this would compromise all of us and above all do not return under any circumstances. It is known that it was you who helped us to get away from here and all would be lost if you should show yourself. We are guarded day and night, I do not care...Do not be troubled on my account, nothing will happen to me. The National Assemble will show leniency. Farewell... I cannot write any more."

When we decrypt this letter with the keyword "*depuis*" (since), we get:

"I am alive **here my beloved for the reason to adore you**. Oh, how anxious I have been for you, and how sorry I am about all you must have suffered in having no news from us. May heaven grant that this letter reaches you. Do not write to me, this would compromise all of us and above all do not return under any circumstances. It is known that it was you who helped us to get away from here and all would be lost if you should show yourself. We are guarded day and night, I do not care. **You are not here.** Do not be troubled on my account, nothing will happen to me. The National Assemble will show leniency. Farewell **the most loved of men. Be quiet if you can. Take care of yourself for myself**. I cannot write any more **but nothing in the world could stop me to adore you up to the death**"

Here we think that the differences between the text taken from historical books and the decrypted text we get are due to the fact that the persons who published the letters wanted to conceal Marie-Antoinette's deep affection for Fersen.

6.3   Letter of July 8, 1791

Here is another letter for which we have more information:

In this long letter Marie-Antoinette informs Fersen about the king's ideas concerning the political situation. In historical books [5] page 127 or [4] page 548, we have this passage:

"There is no doubt that a foreign power could get into France, but the armed people would flee the borders and the troops from outside. Then they would make use of their weapons against their fellow citizens that they have been considering as enemies for two years in our trip and especially... The king thinks that a full unlimited power as it composed even by dating it on June 20th, would be dangerous in its current state."

When deciphering with the keyword "*courage*" (courage), we get:

"There is no doubt that a foreign power could get into France, but the armed people would flee the borders and the troops from outside. Then they would make use of their weapons against their fellow citizens that they have been considering as enemies for two years. In our trip and especially **since our return we have made every day the sad experiment to be considered as enemies**. The king thinks that a full unlimited power as it composed even by dating it on June 20th, would be dangerous in its current state."

In this letter, we have the encrypted text, and the keyword is repeated under the ciphertext but using one letter in two. The person (Fersen or his secretary) who decrypted it had committed a mistake: he/she inserted two spaces instead of one between two letters of the key. Thus, the end of the section could not be correctly decrypted and was replaced by suspension points. At the beginning of each new paragraph, the encoding begins with the first letter of the keyword even though the previous paragraph has stopped before the end of the keyword. That is the reason why the next section beginning with "The king thinks..." was correctly decrypted.

6.4   Letter of July 9, 1792

Now we present a letter that we decrypted with the keyword "*depuis*" (since) that seems to be unknown so far. We did not find it any historical book:

"Here is a large report I wrote on the ideas of the king. It is certain that the force will do only damage. We have to give way to the storm. We would not have time to be rescued. Give this report to M. de Mercy in order he takes care of it; the opinions of my brothers and those to whom it would be necessary to talk. I wish that you do not go to Vienna, you stay near the king and that you will be the least visible. In all of this, believe me, my gentle friend, I would like to owe you every thing, I have strong reasons to make this request. Our happiness depends on it, since we would have no more happiness if we were separated for ever. Farewell. Feel sorry for me. Love me. Above all do not judge me in all what you will see me doing before you hear me. I would die if I was for a moment disapproved by the one I adore and I will never stop adoring him. The Lameth's and their associates seem to want to serve us in good faith. I take advantage of this situation but I trust them with caution. Farewell."

7   Signs of love in the letters between Marie-Antoinette and Fersen

Before we decrypted the previous letters, there was probably only one known letter (see below) that showed there were signs of love between Marie-Antoinette and Fersen. So some people had doubts about the authenticity of this letter. In her book devoted to Marie-Antoinette's correspondence, [4] page 545, E. Lever presents the following love letter dated July 29, 1791 which is not the same letter that we studied in Section 6. She explains that this letter was decrypted and published for the first time by Lucien Maury in "La revue Bleue" in 1907. There is no other trace of this letter in the literature. Here is the letter:

"I can tell you that I love you and indeed that is all I have time for. I am well. Do not worry about me. I hope you to be well too. Write me cipher letters and send them by mail to Mrs Brown's address, in a double envelope to Mr. de Gougens. Send the letters by your manservant. Tell me to whom I should send the letters I could write you. I cannot live without that. Farewell, the most loved and the most loving of men. I kiss you with all my heart."

In "La revue bleue" [6], Lucien Maury in 1907 gave an extract of this letter. He said that he was authorized to publish this extract by Baron von Klinckowström. In 1877, the father of Baron von Klinckowström had published all the letters kept by Fersen except this one. L. Maury did not give any detail on the decryption. Moreover he pointed out this letter was written in September either 1791 or 1792. There are some articles on the Internet that have doubts about the authenticity of this letter (http://teaattrianon.blogspot.com/2007/06/fersen-legend-part-2.html). We could not find the corresponding ciphertext.

8   Crossed out letters

Finally, we did not find the ciphertext corresponding to crossed out letters. These letters were sent by Fersen to Marie-Antoinette, and the encrypted letters which were received by Marie-Antoinette were probably lost.

9   Conclusion and open questions

9.1   Summary

Here is the summary of what we found above:

1. Marie-Antoinette used to encode one letter in two of the text. This was not reported in classical cryptography books. Clearly, this weakens the safety of her encryption method. This restrains the enthusiasm shown by many historians about her encoding technique.

2. At that time, it would have been possible for a cryptographer to decipher at least partially many letters. This would have brought proofs of Marie-Antoinette's complicity with some foreign countries, and there would have been real proofs to condemn her. In fact her trial was lost in advance and the revolutionary court condemned her without any proof. This might explain that it was useless to make cryptanalysis efforts in order to find proofs.

3. Unlike Marie-Antoinette, Madame Elizabeth, the sister of Louis XVI, did not encrypt the letters she wrote to get help from foreign armies. So the Revolutionary tribunal had proofs to condemn her.

4. Some passages were deleted in order to dissimulate Marie-Antoinette's affection to Fersen. By deciphering the cipher letters we uncovered some of them. Thus, now the letter of Section 7 published by E. Lever (see [4]) is not the only one of that kind. This may give arguments for its authenticity. It appears that Marie-Antoinette had a deep affection for Fersen. This is not really a surprise, and it is very likely (due to the epoch) that this was a platonic love.

5. We were also able to decipher some encrypted letters that had not been deciphered due to decryption mistakes.

9.2   Open questions

Several questions are still open:

1. How did Marie-Antoinette dissimulate the encoding table? Did she memorize it?

2. Fersen and Marie-Antoinette used very simple words as keywords (depuis, vertu, autres, ...). How did they agree on the keyword that changed with each letter?

3. Would it be possible in the future to read the crossed out passages, for example by using scientific police techniques or techniques employed to examine the different layers of paintings?

4. Would it be possible to find other encrypted letters?

References

[1] Friedrich Ludwig Bauer, *Decrypted Secret: Methods and Maxims of Cryptology*, Springer 1997.

[2] Yves Gylden, *Le chiffre particulier de Louis XVI et Marie-Antoinette lors de la fuite Varennes*, Revue internationale de criminalistique, III, (1931), 248-256.

[3] David Kahn, *The Code-Breakers*, Scribner 1996.

[4] Evelyne Lever, *Marie-Antoinette Correspondance (1770-1793)*, Taillandier 2005.

[5] *Marie-Antoinette Correspondance - Tome II 1788-1793*, Sources de l'Histoire de France, Paleo 2004.

[6] Lucien Maury, *Revue littéraire et politique - Revue bleue*, Numéro 17, 5ème série, Tome VII, Avril 1907, 236-239.

Jaques Patarin is Professor at the University of Versailles - France. He is the author of lots of papers in many areas of cryptography (secret key cryptography, multivariate cryptography, historical cryptography,...)

Valérie Nachef is Associate Professor at the University of Cergy-Pontoise - France. Her research interests are the study of block ciphers based schemes and historical cryptography.