

“Je vous aimerai jusqu’à la mort” (Marie-Antoinette à Axel de Fersen)

Jacques Patarin¹, Valérie Nacheff²

(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 Mathématiques
Université de Cergy-Pontoise
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
valerie.nacheff@u-cergy.fr

1 Introduction

Dans cet article, nous nous intéressons aux lettres échangées entre la reine Marie-Antoinette et le comte Axel de Fersen durant les années 1791-1792. Après l’échec de la fuite à Varennes dont Fersen fut l’un des organisateurs, la famille royale est ramenée aux Tuileries et reste sous surveillance. Malgré cela, Marie-Antoinette parvient à envoyer des lettres à Axel de Fersen. Certaines sont codées, d’autres sont rédigées en clair ou écrites à l’encre sympathique. Dans ces lettres, Marie-Antoinette essaye la plupart du temps de trouver des alliances avec les puissances étrangères pour restaurer la monarchie. Certains passages montrent aussi ses sentiments envers Axel de Fersen. A la demande de France 2 pour une émission sur Marie-Antoinette, nous avons étudié les lettres chiffrées de Marie-Antoinette. Il reste très peu de lettres écrites par la reine. Fersen avait gardé les lettres reçues, déchiffrées et celles qu’il avait écrites. Ces archives furent conservées par ses neveux et arrière-neveux et en 1877, le baron de Klinckowström publia l’ensemble de la correspondance, mais certains passages étaient manquants ou raturés. En 1982, des descendants du baron de Klinckowström mirent aux enchères des lettres que l’on croyait détruites et qui furent achetées par les archives nationales.

Il semble que d’une part, les historiens qui ont publié les lettres de Marie-Antoinette aient utilisé les versions déchiffrées données par le baron de Klinckowström et que d’autre part, les cryptographes qui se sont intéressés au mode de chiffrement n’aient pas cherché à vérifier les lettres quand cela était possible à l’aide du texte clair et du texte chiffré pour le même document.

Nous expliquons ici le mode de chiffrement et donnons quelques exemples où il y a des différences entre le déchiffrement obtenu et le texte publié par les historiens. Nous donnons également un extrait d’une lettre que nous avons déchiffrée et que nous n’avons pas trouvée dans les ouvrages historiques.

2 Le point de vue des historiens et des cryptologues

Plusieurs ouvrages donnant les lettres de Marie-Antoinette, non seulement au comte de Fersen mais aussi à sa famille et ses conseillers avant et pendant la révolution ont été publiés (voir par exemple [4, 5]). Certaines lettres de Marie-Antoinette sont également disponibles sur internet. Dans tous ces documents, on retrouve à peu près les mêmes textes. Il faut remarquer que dans certains passages des points de suspension remplacent le texte sans que l’on sache si le texte manquant est dû à une dissimulation ou à

une perte du texte. Une historienne contactée pour avoir travaillé sur cette période nous a dit ne pas s'être intéressée au côté scientifique et cryptographique pour l'étude des lettres.

Egalement, dans les ouvrages sur l'histoire de la cryptographie, peu de détails sont donnés sur le mode de chiffrement. La plupart du temps, il est expliqué qu'il s'agit d'un chiffrement poly-alphabétique et les premières lignes de la table de chiffrement sont données. Du côté de la cryptographie, on s'intéresse au mode de chiffrement mais il n'y a pas de recherche pour comparer les textes clairs et chiffrés et ainsi obtenir des nouveaux éléments sur cette période troublée.

Pour Marie-Antoinette, ce travail de chiffrement et de copies est fastidieux. Elle s'en plaint au comte de Fersen dans une lettre datée du 2 Novembre 1791 [4] p.662 : "Adieu, je suis fatiguée à force d'écritures; jamais je n'ai fait tel métier, et je crains toujours d'oublier, ou de mettre quelques bêtises."

3 Le chiffrement poly-alphabétique

Les livres de cryptographie historique, comme [1, 3], disent que Marie-Antoinette et Fersen utilisaient un chiffrement poly-alphabétique. Un tel chiffrement était réputé pratiquement indéchiffrable à l'époque et l'opinion de ces livres de cryptographie est donc que Marie-Antoinette (contrairement à Marie-Stuart par exemple, une autre reine célèbre mais d'une autre époque) utilisait une excellente méthode pour son temps. D'ailleurs elle n'a jamais eu à souffrir (contrairement à Marie Stuart) de la cryptanalyse de ses ennemis sur ses lettres.

Le chiffrement poly-alphabétique utilise deux clés : une table de chiffrement et un mot clé, qui change en général à chaque message.

La table de chiffrement utilisée par Fersen

Il semble que Fersen ait utilisé tout le temps la même table avec ses divers interlocuteurs. Dans différents ouvrages de cryptographie historiques comme [1, 3], les trois premières lignes de la table sont données. En déchiffrant quelques messages de Marie-Antoinette, nous avons progressivement trouvé plusieurs autres lignes. Mais finalement, une visite à la BNF suite à une note de [3] nous indique que la totalité de la table de chiffrement est connue. Elle est publiée par Y. Gylden dans la revue de criminalistique [2] en 1931. Elle a été trouvée dans les papiers de Fersen. Nous donnons ici l'intégralité de cette table dont nous avons retrouvé des parties.

On peut se demander comment Marie-Antoinette pouvait dissimuler cette table. Y a-t-il un moyen mnémotechnique pour retrouver cette table à l'aide d'un moyen simple à mémoriser ?

L'utilisation du mot clé

Le système est simple. Le mot clé sera répété autant de fois qu'il faut sous le message clair, puis la table de chiffrement détermine chaque lettre du message correspondant au couple de lettres du message clair et du mot clé. Nous allons en voir des exemples dans les sections suivantes.

Remarques

1. Dans l'article de Y.Gylden, il est également expliqué qu'en plus de la table de chiffrement, Fersen utilisait une liste dans laquelle les noms des personnages importants étaient donnés par une seule lettre de l'alphabet. Par exemple, pour le roi la lettre N, pour la reine le lettre O, pour le roi de Suède la lettre D... Cette liste ne semble pas avoir été utilisée dans les lettres que nous avons étudiées.
2. La méthode de substitution poly-alphabétique est inspirée de la méthode de Porta, mais présente l'avantage que l'ordre des lettres accouplées est brouillé par la table dechiffrement et ne présente pas de progression régulière.

4 Les lettres des archives nationales

Nous avons d'une part les lettres publiées dans les ouvrages historiques et d'autre part des éléments sur le mode de chiffrement. Pour l'émission de France 2, une première visite aux archives nationales s'impose. Sur un microfilm, il faut trouver les lettres en question. Si la bande défile trop vite, il faut recommencer

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	KN	M&	OX	QY	SZ
H	AI	BT	CS	DO	EL	F&	GH	KM	NQ	PR	SZ	UY
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	FO	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	GN	HI	KT	LS	MR	NP	OQ
Y	AZ	BU	CG	DH	EX	FY	IO	K&	LN	MP	QS	RT

au départ. Enfin après avoir trouvé des lettres chiffrées, il faut aller faire les photocopies. Comme il n’y a pas de repère sur le microfilm, il faut tout faire redéfinir et les photocopies sortent parfois difficilement. Nous donnons deux exemples de lettres trouvées aux archives nationales. La première (Figure 1) est un extrait d’une lettre de Marie-Antoinette à Axel de Fersen datée du 8 Juillet 1791. Elle montre comment s’effectue le chiffrement et le déchiffrement à l’aide du mot clé *courage*. La deuxième (Figure 2) est une lettre de Fersen à Marie-Antoinette datée du 10 Octobre 1791. Il s’agit uniquement du texte clair et les premières lignes ont été raturées. Le mot clé *autres* est indiqué sous le texte. A partir de cela, le texte chiffré était conçu et expédié.

7 25 1791

le 8 juillet 1791

Le roi pense que l'apprise n'est que le
 c-o-u-r-a-g-e-i-c-o-u-r-a-g-e-i-c-o-u-
 est net et en vult l'at de de on adoti on to fa po d
 u sur t un y e p l o t s t c e n e k r d o p t n o b t t u t g l r u :
 r - e - g - e - c - o - u - r - a - g - e - c - o - u - r - a - g - e -
 passim a a port e a a o x a u t e c e n n d i s b a i s
 a e s = i l a = a g o e t u c : r a n o k a c t f u r l l c i r k n b a n s
 - o - u - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 a n t i p l u s e x e n c e t a u c u m a c t e g u e l c o n d e
 a o t f l e s : k a r o e k a l c k u f c h e d u s l g o o q k e
 - a - g - e - c - o - u - r - a - g - e - c - o - u - r - a - g -
 s h a e s s x g o o n k d u s : a u d i s e a b c f s r t o a p
 - e - o - u - r - a - g - e - c - a - u - r - a - g - e - e -
 e r e p o u r q u i m o i t h e s o i n d e l e z i t l i q u e r
 s r e p h u s g k i b o g i y b s h i o d i l u x u l d g f i k
 o - u - r - a - g - e - c - o - u - r - a - g - e - c - o - u - r -
 i g y .
 d y .

Le roi pense que c'est par la voie des
 e n o u p u r e y u a c k s y p x r x a t o q e h e d
 - o - u - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 n e g o c i a t i o n s s e u l e q u e l e u r p e c o u r
 i s g c c p a u i x n a s k u b e d a u l f u e s u c q u a
 - a - u - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 p o u r r a i t e t r e u t i l e a l u i e t a s o n n o
 ' c u k r u i k e m k u y i b e s t i r t f f s q u a n o
 u - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 y a u m e q u e l a d i e m o n s t r e b t b o g d k s i a o p
 h a e m f g k e b a : a e o o i s d r b t b o g d k s i a o p
 - a - u - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 c e s n e d o i t e t r e q u e s e a n d a i n e t s i
 c u s o e n o c t : k t u e d u u s f c a n h a x r s e g o p
 - r - a - g - e - c - o - u - r - a - g - e - c - o - u -
 l' o n p e n e f u i s o i t f i c i a t o u t e v o y e d e h
 l u u z e o e m a e o n t p c x a h o e t k v m y s d u n
 - a - g - e - c - o - u - r - a - g - e - c - o - u -
 e g o c i a t i o n
 f g a c c a h i m u .
 - g - e - c - o - u -



FIGURE 1 – Extrait d’une lettre de Marie-Antoinette à Fersen sur laquelle nous avons ajouté le texte clair correspondant- 8 Juillet 1791

5 Premier exemple - Première surprise

Nous sommes maintenant en possession des textes chiffrés de certaines lettres et du texte clair trouvé sur internet ou dans les ouvrages [4, 5]. Nous pouvons commencer à étudier le mode de chiffrement. Il s'agit donc d'un chiffrement poly-alphabétique à l'aide d'une clé. Notre première surprise est de constater qu'à part le premier texte du 28 Juin 1791, il n'y a qu'une lettre sur deux qui est chiffrée dans les textes. Ce fait n'était pas signalé dans les livres classiques d'histoire de la cryptographie (comme [1, 3]). (Nous découvrirons plus tard que ce fait était signalé dans l'article de Y.Gylden de la revue de criminalistique déjà citée). La réputation de Marie-Antoinette comme étant une personne ayant utilisé un excellent algorithme pour l'époque en prend un peu un coup. (En fait en cryptographie moderne, on sait retrouver un texte à partir d'une lettre sur deux même si ce n'est pas toujours facile).

Donnons un exemple. Nous considérons ici la lettre de Marie-Antoinette au comte de Fersen datée du 29 Juin 1791. Le mot clé est *depuis*.

Texte chiffré	L	&	C	F	E	B	P	S	R	&	E	B	T	&	R	E	Q	E	E
Clé	-	s	-	d	-	e	-	p	-	u	-	i	-	s	-	d	-	e	-
Texte clair	l	e	c	i	e	l	p	e	r	m	e	t	t	e	r	a	q	u	e
Texte chiffré	U	E	B	L	I	C	I	V	&	U	X	A	K	R	N	V	E		
Clé	p	-	u	-	i	-	s	-	d	-	e	-	p	-	u	-	i		
Texte clair	c	e	l	l	e	c	i	v	o	u	s	a	r	r	i	v	e		

Pour cette lettre, nous avons le texte clair et le texte chiffré. Pour le déchiffrement par exemple, on écrit le mot clé, ici *depuis* sous le texte chiffré en n'utilisant qu'une lettre sur deux. On voit donc que quand on a la lettre "d" dans la clé, le **i** est remplacé par la lettre **F**. Quand on a la lettre "p" dans la clé, le **r** est remplacé par la lettre **K**, et ainsi de suite. Les opérations de chiffrement et de déchiffrement sont donc symétriques. Il faut avoir la table de chiffrement, c'est à dire connaître la substitution à opérer pour chaque lettre de l'alphabet. On remarque que dans ces substitutions, par exemple si on a la lettre de "d" dans la clé, le **i** est changé en **F** et le **f** est changé en **I**. Puisque nous avons plusieurs couples clair-chiffré de certaines lettres avec des mot-clés différents, il a été possible de commencer à établir une partie de la table de chiffrement. Par exemple, pour la lettre E, nous avons les substitutions suivantes où nous regroupons les lettres échangées deux par deux :

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

Il faut aussi noter que les lettres i et j sont cryptées de la même manière ainsi que les lettres u et v et que la lettre w n'est pas dans l'alphabet. Il faut également s'habituer à la calligraphie des lettres qui diffère de ce que l'on utilise actuellement.

Après une première étude les résultats sont les suivants :

Tout d'abord, nous avons établi, à l'aide de plusieurs lettres pour lesquelles on avait le texte clair, le texte chiffré et quelques mots clés (*depuis - courage - paroitra - vertu*) les substitutions utilisées avec les lettres A,C,E,G,I,O,P,R,T,U, et des indications partielles pour les lettres D et S. Comme nous l'avons signalé Section 3, nous avons vu ensuite que toute la table de chiffrement utilisée par Fersen était connue et fixe.

6 Nouveaux résultats

Le déchiffrement complet et systématique de toutes les lettres pour lesquelles nous possédions les textes chiffrés nous a permis de compléter certaines d'entre elles. Nous donnons par ordre chronologique celles pour lesquelles nous avons obtenu quelques résultats nouveaux.

6.1 Lettre du 28 Juin 1791

Dans cette lettre du 28 Juin 1791 qui est dite adressée au comte de Fersen, toutes les lettres sont chiffrées et non pas une sur deux. Ici, nous avons une différence entre le texte trouvé dans les ouvrages historiques et le déchiffrement.

Texte trouvé dans les ouvrages historiques [5] page 125 ou [4] page 544 :

“Rassurez-vous sur nous. Nous vivons. Les chefs de l’Assemblée ont l’air de vouloir mettre de la douceur dans leur conduite. Parlez à mes parents de démarches du dehors (illisible). S’ils ont peur, il faut composer avec eux.”

Par déchiffrement avec le mot clé *vertu*, nous obtenons :

“Rassurez-vous sur nous. Nous vivons. Les chefs de l’Assemblée ont l’air de vouloir mettre de la douceur dans leur conduite. Parlez à mes parents de démarches du dehors (6 lettres non déchiffrées). S’ils ont peur, il faut composer avec eux. **Brûle tout ce qui est (10 lettres non déchiffrées) et envoie le reste de la lettre à m de Fersen. Il est avec le roi de Suède.**”

On peut se poser la question sur le véritable destinataire de cette lettre. Il y a eu un décalage de la clé. Malgré les essais de différents décalages, certains passages n’ont pas été déchiffrés.

6.2 Lettre du 29 Juin 1791

Texte trouvé dans les ouvrages historiques [5] page 126 ou [4] page 545 (version légèrement différente) :

“J’existe ... Que j’ai été bien inquiète de vous, et que je vous plains de tout ce que vous souffrez de n’avoir point de nos nouvelles. Le ciel permettra que celle-ci vous arrive. Ne m’écrivez pas, ce serait nous exposer, et surtout ne revenez pas ici sous aucun prétexte. On sait que c’est vous qui nous avez fait sortir d’ici ; tout serait perdu si vous paraissiez. Nous sommes gardés à vue jour et nuit ; cela m’est égal... Soyez tranquille, il ne nous arrivera rien. L’Assemblée veut nous traiter avec douceur. Adieu...Je ne pourrai plus vous écrire.”

Texte obtenu après déchiffrement où le mot clé est *depuis*

“J’existe **mon bien aimé et c’est pour vous adorer**. Que j’ai été bien inquiète de vous, et que je vous plains de tout ce que vous souffrez de n’avoir point de nos nouvelles. Le ciel permettra que celle-ci vous arrive. Ne m’écrivez pas, ce serait nous exposer, et surtout ne revenez pas ici sous aucun prétexte. On sait que c’est vous qui nous avez fait sortir d’ici ; tout serait perdu si vous paraissiez. Nous sommes gardés à vue jour et nuit ; cela m’est égal. **Vous n’êtes pas ici**. Soyez tranquille, il ne m’arrivera rien. L’Assemblée veut nous traiter avec douceur. Adieu **le plus aimé des hommes. Calmez-vous si vous pouvez. Ménagez-vous pour moi**. Je ne pourrais plus vous écrire **mais rien au monde ne pourra m’empêcher de vous adorer jusqu’à la mort.**”

Ici les différences entre le texte connu et le texte réel viennent vraisemblablement du fait que l’on a voulu masquer les sentiments de Marie-Antoinette pour Fersen.

6.3 Lettre du 8 Juillet 1791

Voici une autre lettre pour laquelle nous avons obtenu un supplément d’information :

Dans cette longue lettre, Marie-Antoinette décrit à Fersen les pensées du roi sur la situation présente. Dans les textes historiques [5] page 127 ou [4] page 548, nous avons ce passage :

“Il n’ y a pas de doute qu’une force étrangère ne parvienne à entrer en France, mais le peuple armé, comme il l’est, en fuyant les frontières et les troupes du dehors, se servirait à l’instant de leurs armes contre ceux de leurs concitoyens, que depuis deux ans on ne cesse de leur faire regarder comme leurs ennemis dans notre voyage et surtout ... Le roi pense qu’un plein pouvoir illimité, tel qu’il est composé, même en le datant du 20 de juin, serait dangereux dans l’état où il se trouve.”

Par déchiffrement avec le mot clé *courage*, nous obtenons :

“Il n’ y a pas de doute qu’une force étrangère ne parvienne à entrer en France, mais le peuple armé, comme il l’est, en fuyant les frontières et les troupes du dehors, se servirait à l’instant de leurs armes contre ceux de leurs concitoyens, que depuis deux ans on ne cesse de leur faire regarder comme leurs ennemis. Dans notre voyage et surtout **depuis notre retour, nous en avons chaque jour la triste expérience.** Le roi pense qu’un plein pouvoir illimité, tel qu’il est composé, même en le datant du 20 de juin, serait dangereux dans l’état où il se trouve.”

Dans cette lettre, nous avons le texte chiffré et la clé est répétée sous le texte une lettre sur deux. La personne qui s’est occupée du déchiffrement (Fersen ou son secrétaire) a laissé deux blancs sous le texte chiffré à un endroit et plus loin en a oublié un. A chaque nouveau paragraphe, on repart avec le début du mot clé *courage*. C’est pourquoi, pour le paragraphe commençant par “le roi pense”, il n’y a pas de problème de déchiffrement.

6.4 Lettre du 9 Juillet 1792

Voici enfin ce que nous avons déchiffré (le mot clé est *depuis*) sur une lettre chiffrée de Marie-Antoinette au comte de Fersen datée du 9 Juillet 1792 et qui ne semble pas être connue (elle n’est pas dans les ouvrages que nous avons consultés) :

“Voici un grand mémoire que j’ai rédigé sur les idées du roi. Il est certain que la force ne fera que du mal. Il faut céder à l’orage. Nous n’aurions pas le temps d’être secourus. Donnez ce mémoire à M. de Mercy. Que ce soit lui qui s’en charge. Les avis de mes frères et de ceux à qui il faudra en parler. Je désire que vous n’alliez pas à Vienne, que vous restiez auprès de roi et qu’en tout vous paraissiez le moins possible. Dans tout ceci, croyez-moi mon tendre ami, moi qui voudrais tout vous devoir, j’ai de fortes raisons de vous faire cette prière. Notre bonheur en dépend car il n’y en aurait plus pour nous si nous étions séparés à jamais. Adieu. Plaignez-moi. Aimez-moi. Surtout ne me jugez dans tout ce que vous me verrez faire qu’après m’avoir entendu. Je mourrai si j’étais un moment désapprouvée par le très que j’adore et que je ne cesserai jamais d’adorer. Les Lameth et leurs associés ont l’air de vouloir nous servir de bonne foi. J’en profite mais ne m’y fie qu’autant qu’il faut. Adieu.”

7 Signes écrits d’amour de Marie-Antoinette à Fersen

Avant le déchiffrement des passages que nous venons d’indiquer, il existait peut-être un seul passage écrit connu de signes d’amour de Marie-Antoinette à Fersen, ce qui permettait à certains de mettre en doute l’authenticité de ce passage. Dans son livre sur la correspondance de Marie-Antoinette [4] page 545, E. Lever donne en effet une lettre d’amour de Marie-Antoinette datée du 29 Juin 1791 différente de celle citée précédemment en disant que cette lettre a été déchiffrée et publiée pour la première fois par Lucien Maury dans la Revue Bleue. Il n’y a pas d’autre trace de cette lettre dans la littérature. Nous la

reproduisons ici :

“Je puis vous dire que je vous aime et n’ai même le temps que de cela. Je me porte bien. Ne soyez pas inquiet pour moi. Je voudrais bien vous savoir de même. Ecrivez-moi en chiffre par la poste à l’adresse de Mme Brown, dans une enveloppe double pour M. de Gougens. Envoyez les lettres par votre valet de chambre. Mandez-moi à qui je dois adresser celles que je pourrai vous écrire, car je ne peux vivre sans cela. Adieu, le plus aimé et le plus aimant des hommes. Je vous embrasse de tout mon coeur.”

Dans la revue bleue [6], que nous avons trouvée à la BNF, Lucien Maury en 1907, donne un fragment de cette lettre de Marie-Antoinette à Fersen qui est celui cité précédemment. Il précise qu’il a eu l’autorisation de copier ce passage par le baron de Klinckowström dont le père avait publié les lettres gardées par Fersen. Il ne donne pas de détails sur le déchiffrement. De plus, il précise que ce message n’a pas de date mais le situe vers septembre 1791 ou 1792. L’authenticité de ce message est mise en doute, par exemple, dans certains articles sur internet (<http://teaattrianon.blogspot.com/2007/06/fersen-legend-part-2.html>). Nous n’avons pas le texte chiffré correspondant à cette lettre.

8 Lettres raturées

Finalement, aux archives, nous n’avons pas trouvé de texte chiffré correspondant aux lettres raturées. La plupart de temps, ce sont des lettres envoyées par Fersen à Marie-Antoinette et les lettres chiffrées qui sont arrivées chez Marie-Antoinette ont dû disparaître.

9 Conclusion et questions toujours ouvertes

Les principaux résultats nouveaux que nous avons découverts sont les suivants :

1. Marie-Antoinette en général ne chiffrait qu’une lettre sur deux, ce qui étrangement n’est pas signalé dans les livres de cryptographie classique. Clairement ceci rend son algorithme de cryptographie beaucoup moins sûr et oblige à modérer quelque peu l’enthousiasme des certains historiens sur la “solidité” des techniques de cryptographie utilisées par Marie-Antoinette.
2. Ainsi, un cryptologue de l’époque aurait probablement pu, en quelques jours, déchiffrer partiellement de nombreuses lettres de Marie-Antoinette. Ceci aurait pu fournir des preuves de la complicité de Marie-Antoinette avec certaines puissances étrangères, et donc fournir des preuves valides pour la condamner. En fait, le procès était perdu d’avance pour Marie-Antoinette et le tribunal révolutionnaire la condamnera à mort sans aucune preuve, ce qui pourra expliquer le fait qu’il était inutile de toutes façons de faire beaucoup d’effort de cryptanalyse pour en trouver.
3. Certains passages ont été supprimés pour dissimuler l’affection de Marie-Antoinette pour Fersen. A partir des textes chiffrés, nous avons pu en retrouver certains. De ce fait, le texte du 29 Juin 1791 n’est désormais plus un texte isolé de cette affection, et son authenticité peut s’en trouver renforcée. Il apparait désormais certain que Marie-Antoinette avait de forts sentiments pour Fersen. Ce n’est d’ailleurs pas vraiment une surprise historique. Par contre il est bien sûr fort possible (et même probable, compte-tenu de l’époque) que cet amour soit resté peut-être platonique.
4. Nous avons également pu déchiffrer des passages qui n’avaient jamais pu être déchiffrés du fait d’erreurs de déchiffrement.

Plusieurs questions restent cependant naturellement ouvertes. Par exemple :

1. Comment Marie-Antoinette avait-elle caché la table de chiffrement de Fersen ? Dans le “meuble à serrure” dont l’existence historique ne semble pas être prouvée ? L’avait-elle mémorisée ?
2. Comment Marie-Antoinette et Fersen se mettaient-ils d’accord sur le mot clé ?

3. Sera-t-il un jour possible de lire les ratures, par exemple en utilisant les méthodes de police scientifique ou des techniques analogues aux procédés permettant de voir les différentes couches de peinture d'un tableau ?
4. Serait-il possible d'obtenir d'autres lettres chiffrées ?

Références

- [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 à 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.