

Comment Marie-Antoinette chiffrait-elle ses lettres ?

Pour qu'elles ne puissent pas être interceptées, Marie-Antoinette chiffrait ses lettres. La méthode qu'elle utilisait était a priori excellente... mais avec une erreur majeure : elle ne chiffrait qu'une lettre sur deux.

Marie-Antoinette chiffrait ses lettres par **substitution poly-alphabétique**. Pour cela, elle disposait d'une table de chiffrement par destinataire. En voici une :

Tout le monde

AB	A	B	C	D	E	F	G	H	I	L	M
	O	P	Q	R	S	T	V	X	Y	Z	N
CD	M	A	B	C	D	E	F	G	H	I	L
	Z	N	O	P	Q	R	S	T	V	X	Y
EF	L	M	A	B	C	D	E	F	G	H	I
	N	O	P	Q	R	S	T	V	X	Y	Z
GH	I	L	M	A	B	C	D	E	F	G	H
	N	O	P	Q	R	S	T	V	X	Y	Z
IL	H	I	L	M	A	B	C	D	E	F	G
	N	O	P	Q	R	S	T	V	X	Y	Z
MN	G	H	I	L	M	A	B	C	D	E	F
	N	O	P	Q	R	S	T	V	X	Y	Z
OP	F	G	H	I	L	M	A	B	C	D	E
	N	O	P	Q	R	S	T	V	X	Y	Z
QR	E	F	G	H	I	L	M	A	B	C	D
	N	O	P	Q	R	S	T	V	X	Y	Z
ST	D	E	F	G	H	I	L	M	A	B	C
	N	O	P	Q	R	S	T	V	X	Y	Z
VX	C	D	E	F	G	H	I	L	M	A	B
	N	O	P	Q	R	S	T	V	X	Y	Z
YZ	B	C	D	E	F	G	H	I	L	M	A
	N	O	P	Q	R	S	T	V	X	Y	Z

CHIFFRE
DE S. M. MARIE ANTOINETTE,

Un des tableaux de chiffrement de Marie-Antoinette @ Archives nationales

On notera que ce tableau ne contient que 22 lettres, les lettres manquantes sont J, K, U et W, ce qui correspond à un usage venant du latin où I et J d'un côté, U et V de l'autre sont confondues. K peut être remplacé par C et W par V.

Clef de chiffrement

L'utilisation de cette table pour chiffrer demande une clef secrète qu'on partage avec le destinataire. Par exemple, si la clef est *sel*, pour chiffrer la première lettre, on utilise la ligne dont la première colonne est ST, D est alors changé en N (et N en D), E en O, etc. Pour chiffrer la seconde, on utilise la ligne dont la première colonne est EF.

Du 12 août 1791. 13/8/1791

à Comte de Fersen.

du Comte de Fersen.

+ m a dit
e - d - i



qu'une reposé toujours qu'on attend les
reposes des autres cours ou est sur de
celle de druse ~~abjection~~ m = De. Bischofs
verder qui est iet que son maître est prêt
à marcher et qu'il prene fort l'Empereur
d'agir ou mesure qu'il va se faire une
alliance entre eux ou attend les reposes
d'Espagne et de Russie avant de les avoir
l'Empereur ne se décidera pas ou craint
beaucoup l'Angleterre je suis qu'il en est
arrivé une repose dont on ne parle
pas, elle ne contient qu'une assurance
très vague de ne pas se mêler des affaires
affaires de France il paroit qu'on
si en est pas content et qu'on voudroit
quelque chose de plus positif j'attends
avec grande impatience de vos
nouvelles elles décideront toute cette

Travail de chiffrement d'une lettre au comte de Fersen où l'on voit que Marie-Antoinette ne chiffrait qu'une lettre sur deux. @ Archives nationales

Utilisation correcte

Pour chiffrer une phrase comme "*je vous aime*", on peut construire un tableau à 10 lignes et 3 colonnes :

J	E	V	O	U	S	A	I	M	E
S	E	L	S	E	L	S	E	L	S
S	T	D	E	F	B	X	Z	Q	O

Le message chiffré est donc "*stdefbxzqo*". Si vous essayez de chiffrer une lettre ainsi, vous verrez la difficulté d'éviter les erreurs. C'est pour cela que, on ne sait quel cryptologue avait conseillé à Marie-Antoinette de ne chiffrer qu'une lettre sur deux ce qui, en fournissant des repères, simplifie grandement le chiffrement mais l'affaiblit tout aussi grandement. Nous allons voir pourquoi.

Utilisation par Marie-Antoinette

Le tableau devient ainsi :

J	E	V	O	U	S	A	I	M	E
	S		E		L		S		E
J	O	V	M	U	B	A	S	M	T

Le message chiffré est maintenant "*jovmubasmt*". On peut examiner des lettres chiffrées ainsi par Marie-Antoinette aux Archives nationales, comme celle présentée ci-dessus.

Décryptement

Le décryptement sans connaître la clef est ainsi facilité, surtout si on connaît le tableau de chiffrement. C'est ici que des talents de cruciverbiste sont utiles. En effet, on peut deviner un mot si on en connaît une lettre sur deux comme ici J-V-U-A-M, qui est transparent pour tout amateur de mots croisés. Ensuite, on sait que la première lettre de la clef transforme E en O ce qui ne se produit que pour ST, en continuant ainsi, on décrypte le message quel que soit sa longueur.