TD 1 : Les chiffrements historiques

Christina Boura

1 La scytale

Le message suivant a été chiffré à l'aide d'une scytale.

`lunlaessatsadueatebamtmeuiaalfsqieonuncrooaht`

1. Quel est le diamètre (nombre de lettres par tour) de la scytale ?
2. Quel est le message clair ?

Chiffrer le message suivant en utilisant la même technique et la même clé, c.-à-d. le diamètre (ne pas oublier d'enlever les espaces) : `Repos pour demain`

2 Renforcer la sécurité d'un chiffrement par substitution

On souhaite renforcer la sécurité d'un chiffrement par substitution mono-alphabétique en effectuant d'abord un chiffrement par décalage puis un chiffrement par substitution sur le résultat du chiffrement par décalage. Qu'en pensez-vous de la sécurité de ce nouveau système ? Justifier.

3 Le chiffrement ADFGVX

Le chiffre ADFGVX est un système de chiffrement allemand inventé par le colonel Fritz Nebel et introduit à la fin de la Première Guerre mondiale afin de sécuriser les communications radiophoniques lors de l'offensive sur Paris. Il a été cassé par le lieutenant Georges Painvin début juin 1918, donnant un avantage crucial à l'armée française.

Son originalité réside dans l'union d'une substitution inspirée du carré de Polybe et d'une transposition. Le nom du chiffre provient des coordonnées des lettres dans le carré. Les chiffres du carré de Polybe sont en effet remplacés par les lettres A, D, F, G, V et X, choisies en raison de leur codes morse très différents les uns des autres, de façon à éviter les erreurs de transmission radio.

Ici on utilise des tableaux de taille 6 permettant de coder l'ensemble des lettres de l'alphabet (non accentuées) et les 10 chiffres. Une première clé secrète consiste en la disposition des caractères dans le tableau. Une deuxième clé est représentée par une permutation permettant de mélanger le texte chiffré après application du principe de Polybe.

Par exemple, on suppose que le tableau est donné par :

	A	**D**	**F**	**G**	**V**	**X**
A	c	1	o	f	w	j
D	y	m	t	5	b	4
F	i	7	a	2	8	s
G	p	3	0	q	h	x
V	k	e	u	ℓ	6	d
X	v	r	g	z	n	9

Dans une première étape, on codera donc le mot `attaque` par `FF|DF|DF|FF|GG|VF|VD`. Dans une seconde étape, on va transposer (permuter) les lettres que nous venons d'obtenir selon une permutation secrète π ayant une longueur également secrète. Supposons par exemple que la permutation π est de longueur $n = 4$ et qu'elle est donnée par $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. On dispose alors le texte codé en lignes successives de n lettres et on complète les lignes par des caractères aléatoires (ne modifiant pas le message, `XX` ici) :

```
FFDF
DFFF
GGVF
VDXX
```

Le texte chiffré sera le résultat de la permutation par π des colonnes :

```
FDFF
FFDF
GVGF
DXVX
```

et la lecture des caractères de haut en bas et de gauche vers la droite. Finalement on obtient le chiffré : `FFGD|DFVX|FDGV|FFFX`.

1. Chiffrer le texte `attaquesurparisle12janvier` à l'aide du même tableau et de la permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$.
2. Déchiffrer le texte `GFFFV FFDFF DDFXG FVDVV XFVVF GXGAD AXDGV FGVFX FFVAF FVV` qui a été chiffré à l'aide du même tableau et de la permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 2 & 5 & 4 \end{pmatrix}$.

4 Sécurité des mots de passe

Pour chacun des schémas de mots de passe suivants, indiquer le nombre de combinaisons qu'une attaque par force brute (effectuée par quelqu'un qui connaîtrait le schéma) devra tester pour être certaine de trouver le mot de passe.

— On impose exactement 8 caractères minuscules.
— On impose exactement 8 caractères minuscules, mais les lettres ne doivent pas se répéter.
— On impose des lettres minuscules ou majuscules pour les 5 premiers caractères et des chiffres pour les 3 derniers caractères.
— On impose exactement 7 caractères minuscules ou majuscules et exactement 2 caractères spéciaux (15 possibilités)
— On impose de 6 à 10 caractères composés uniquement de minuscules, majuscules ou chiffres.
— On impose exactement 8 caractères minuscules, majuscules ou caractères spéciaux, où le nombre de caractères spéciaux est au plus 2.

5 Chiffre de Vigenère

1. Chiffrer à l'aide du carré de Vigenère et du mot-clé "citron" le message "*Attaquons Versailles*".
2. Le message chiffré

   `tfuefknfmtfuekaakbskaehnejmifg`

   a été obtenu en utilisant le chiffre de Vigenère. Retrouver le message clair écrit en anglais. Pour vous aider, les lettres les plus fréquentes de la langue anglaise sont par ordre décroissant `e, t, a, o, i, n, s, h` et `r`.

6 Se familiariser avec les ordres de grandeur

1. Évaluer le nombre moyen de secondes dans une année.
2. On suppose que l'on connaît un couple texte clair/texte chiffré, et le système cryptographique utilisé. Le texte est chiffré avec une clé de 128 bits. Le nombre d'opérations pour un chiffrement est estimé à environ 1000 instructions. Considérons que notre PC (Intel Core i7 5960x) peut effectuer environ 300000 millions d'instructions par seconde (MIPs). Estimer le temps demandé pour une recherche de la clé par force brute.
3. Répéter le même calcul pour en algorithme utilisant une clé de 56 bits. Combien d'années l'attaque va prendre si on suppose qu'on possède 100 ordinateurs du même type ?

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