Université de khenchela
Faculté des sciences et Technologies L3 ISIL

TD 2 :Cryptographie classique

1 Exercice

Pour protéger des données confidentielles, on utilise un système de chiffrement dit de César (qui consiste à décaler les lettres de l'alphabet d'une constante). Montrer qu'il est très aisé de déchiffrer le message suivant (écrit en français) : ZSGASHWSFGRWBHSFBSH.

2 Exercice

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de César sur un texte en langue française dans lequel les espaces ont été supprimées :

```
zsqvwttfsasbhrsqsgofsghibacrsrsqvwttfsasbhdofgipghwhihwcbwzbs acrwtws
rcbqdogzotfseisbqsroddofwhwcbrsgzshhfsgzozshhfszodzig tfseisbhsrobgibhs
lhstfobqowgshobhzss
```

3 Exercice

Imaginons une généralisation du code de césar avec une clé (3, 15, 21, 12, 5). de tel sorte que la lettre qui remplace la lettre en clair est prise alternativement dans la première ligne du tableau suivant (clé 3), puis dans la deuxième (clé 15), puis dans la suivante (clé 21) ? et ainsi de suite. Quand on arrive à la sixième lettre à coder, on reprend la clé 3.

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
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
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
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
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
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

FIGURE 1 – Code de César avec une clé de 5 positions

- Coder le text suivant : VIVE LE MONDE DES RESEAUX

4 Exercice

On considère un système de chiffrement symétrique avec une clé de 64 bits. Vous cherchez à casser le système sans aucune connaissance de la clé : vous essayez de manière exhaustive toutes les clés. On suppose que vous avez à votre disposition un ordinateur puissant capable de tester une clé (et de dire si c'est la bonne !) en une picoseconde (1 ps = 10^{-12} s).

1. Combien de clés y a-t-il ? Combien de clés en moyenne essaierez-vous ?

2. Combien de temps en moyenne vous faudra-t-il pour trouver la bonne clé ?
3. Quelles solutions préconisez-vous pour lutter contre la cryptanalyse par force brute ?
4. Quelle est la période conseillée de changer la clé dans ce cas ?

5 Exercice

Vous avez intercepté le message suivant :

```
KAZUIVZYTJZXFPDIFFJCZQXWQZXQHRJYRHCOEKXIJZXLBVSNQTMQSYDTMSWJIH
TOSCUWRCYQQOTNCZHAVGYRBIQALTIFIDGMUAHG
```

Vous cherchez à le déchiffrer. Votre indice : il s'agit d'un code de substitution et la clé est de longueur 5.

6 Exercice

Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaire à son exécution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. Nous allons approximer la puissance d'un PC actuel à environ 2000 Mips (millions d'instructions par seconde). Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires. On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute, c'est-à-dire en testant toutes les clés les unes après les autres. Une clé est constituée d'un mot de 128 bits. On suppose que toutes les clés sont équiprobables.

1. En combien de temps une machine de 2000 Mips teste-t-elle une clé ?
2. Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
3. A quel temps moyen de calcul cela correspond-il si on suppose qu'un seul PC effectue la recherche ? Si les 1 milliard de PC de l'Internet sont mobilisés à cette tâche ?
4. Que devient le temps de calcul moyen si on minimise la taille des clés à 32 bits ?