

Fiche de Td No 1

Exercice No 1

1. Evaluer le nombre moyenne 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 clef de 128 bits. Le nombre d'opérations pour le chiffrement est estimé à environ 1000 instructions. Un PC actuel (processeur intel E8400, 10/2008)) peut effectuer environ 26 000 millions d'instructions par seconde (MIPs). Estimer le temps demandé pour une recherche de la clef par force brute.

Si vous utilisez la commande bc, pensez à la lancer avec « bc -l ». La fonction ln (log népérien) s'appelle l. On peut calculer un log en base 10 par : $\ln(x)/\ln(10)$, un log en base 2 par $\ln(x)/\ln(2)$.

Cf <http://www.unixprogram.com/bc.pdf>

Exercice No 2

Pour évaluer la sécurité d'un chiffrement symétrique, on essaye d'estimer le temps et l'investissement financier nécessaire pour retrouver la clef connaissant un couple (texte clair, texte chiffré), suffisamment long pour déterminer la clef de façon unique (attaque "texte clair connu"). Pour beaucoup des chiffrements modernes, il s'agit du temps nécessaire pour retrouver la clef par recherche exhaustive (attaque "force brute"). Quand c'est le cas on définit un *niveau de sécurité* qui est la longueur de la clef si l'attaque par force brute est la seule possible, et qui est estimée en fonction des faiblesses du chiffrement dans les autres cas. Ces attaques sont hautement parallélisables, on peut s'attendre à diviser le temps par deux en doublant les moyens financiers. Le code DES (niveau de sécurité et clef de 56 bits) a été cassé en 1998, en 56 heures et pour un coût de 250 000 \$, en construisant une machine spécifique. En adaptant la loi de Moore à la situation on a :

Loi de Moore *Le coût d'une attaque donnée est divisé par 2 tous les 18 mois.*

Même si c'est assez subjectif, on pense que le niveau de sécurité de 56 bits était suffisant en 1982.

1. En utilisant ces données, estimer l'année limite de protection en fonction du niveau de sécurité (supérieur à 56) et la fonction réciproque donnant la taille minimale de clef en fonction de l'année. L'année limite est celle où votre protection sera équivalente à celle du DES 56 bits en 1982.
2. Application: calculer l'année limite de protection pour un niveau de sécurité de 80 bits, 112 bits (triple DES à deux clefs), de 128 bits, le niveau de sécurité nécessaire pour une protection jusqu'en 2008, puis jusqu'en 2027.

Ces estimations sont subjectives et elles ne prennent pas en compte des progrès éventuels des techniques de cryptanalyse, des révolutions techniques inattendues. Elles n'ont pas grand sens sur une durée trop longue, au delà de quelques dizaines d'années. Les longueurs de clefs des chiffrements symétriques actuels comme AES (128 ou 256 bits) sont largement au delà des limites de validité de ces estimations.

Exercice No 3 permutation alphabétique

Chiffrez le texte 'salut les tepos' en utilisant la permutation alphabétique suivante :

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

Quelle est la clef de notre algorithme de chiffrement ?

Exercice No 4

On vous fournit un fichier sur <http://www.ibisc.fr/~petit/Enseignement/Chiffrement-compression/> chiffré par permutation alphabétique. Déchiffrez le. Quelques outils à votre disposition :

- la commande `tr` qui permet de réaliser une substitution. Exemple: `tr 'ABE' 'ety' fichier > fichier2` remplace A par e, B par t, E par y dans le fichier et sauve le résultat dans fichier2. On peut évidemment utiliser des chaîne de taille inférieure ou supérieure à 3 caractères.
- La commande `frequence-caracteres.sh` est dans `/home/petit/bin`. Elle vous fournit la fréquence de chaque caractère présent dans un fichier. Utilisation: `frequence-caracteres.sh nomFichier`

Exercice No 5

- Chiffrer avec le chiffre de Vigenère le texte suivant : « cryptographierulez » en utilisant comme clef le mot « crypto » ;
- Déchiffrez le texte chiffré suivant « URJJMZGJRTICU » sachant qu'il a été chiffré avec la clef « crypto »
- Pour le même texte en clair on obtient le texte chiffré suivant « EVQIEOVRUHLKIJNWEO ». Quelle est la clef ? Pourra-t-on déchiffrer d'autres textes transmis avec la même clef ?
- Memes questions avec le texte chiffré suivant : « CJPIR IPYGQ USMFJ OIR ».

Sources:

- <http://www.pps.jussieu.fr/~roziere/crypto/tp1/tp1.html>
- <http://www.di.ens.fr/~bresson/P12-M1/>
- article de Arjen K. Lenstra sur la solidité des clefs: http://cm.bell-labs.com/who/akl/key_lengths.pdf.

Annexes

Table de vigenère :

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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