Fiche de Td No 1

Exercice No 1

1. Evaluer le nombre moyende secondes dans une année.

Éléments de correction :
365.25*24*3600 =31557600.00 car 24 heures par jour et 3600 secondes par heure

2. On suppose que l'on connait 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.

Éléments de correction:

Le pc teste 26 000 millions / 1000= 26 millions de clef par seconde

2^128/26000000= 13087783343113017825514407978144.93120984615384615384 secondes

soit 4147268278675506954113 87 années soit de l'ordre de 4 10^23

avec une clef de 56 bits, on trouve 87 ans.

2 remarques:

- ***on peut répartir les choses sur plusieurs machines et ainsi diviser encore le temps nécessaire. Exemple: 100 processeurs => 0,87 ans pour casser une clef des 56 bits***
- ***une attaque partielle peut avoir un certain pourcentage de chances de trouver la clef :***
  - ***chercher 5 ans s'il en faut 87 donne 5/87% de chances de trouver le clef soit 5,8% ce qui peut être inacceptable***
  - **chercher 5 ans pour une clef de 128bits donne 10^{-21} % de chance de trouver la clef ce qui est négligeable.**

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

Éléments de correction:

en 1982, 56 bits sont suffisants

en 1982+a, 56+p bits sont suffisants. On écrit a=f(p) et on cherche f.

- ***f(O)= 0***
- ***f(1)=1,5 (pour info)***
- ***f(p+1)= f(p)+1.5***
- ***Donc a=f(p)=p*1.5=p*3/2***

dans l'autre sens: p=g(a)= a/1,5=a*2/3

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 juqu'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.

éléments de correction :

- ***f(80-56)=(80-56)*3/2=36 années => 1982+36=2018***
- ***(112-56)*3/2 =84 => 2066***
- ***(128-56)*3/2=108 ans => 2090***
- ***(2008-1982)*2/3=17.33 bits donc 18 bits soit au total 56+18=74 bits***
- ***(2027-1982)*2/3=30 bits donc 86 bits***

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 ?

Éléments de correction: tbura uxt axqpt

la clef, c'est le tableau

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 apr 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`*

Éléments de correction :

Exercice No 5

- Chiffrer avec le chiffre de Vigenère le texte suivant : « cryptographierulez » en utilisant comme clef le mot « tepos » ;

Éléments de correction :

```
cryptographierulez
tepostepostepostep
------------------
VVNDLHKGOHAMTFMEIO
```

- Déchiffrez le texte chiffré suivant « URJJMZGJRTICU » sachant qu'il a été chiffré avec la clef « crypto »

Éléments de correction :

```
SALUTLESTEPOS
cryptocryptoc
-------------
URJJMZGJRTICU
```

- Pour le même texte en clair on obtient le texte chiffré suivant «UEDNELTSNWTQW». Quelle est la clef ? Pourra-t-on déchiffrer d'autres textes transmis avec la même clef ?

```
SALUTLESTEPOS
cestlapausece
-------------
UEDNELTSNWTQW
```

- Memes questions avec le texte chiffré suivant : « CJPIR IPYGQ USMFJ OIR ».

```
SALUTLESTEPOS
KJEOYXLGNMFEU
---------------
CJPIRIPYGQUSM
```

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