Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Exercice 1 : Chiffrement

1. Que représente l'acronyme CIA en sécurité informatique ?
2. Classer ces attaques en deux catégories : active et passive
   a) Rejeu
   b) collecte d'information sur Facebook et twitter
   c) Déni de service
   c) interception de message
3. Le cryptogramme suivant a été chiffré avec l'algorithme "autochiffrement" et la clé "teamo". Déchiffrer le message et donner le texte en clair (écrit en anglais).

BAIEV AKUWI GRKAP IOBPS FWPXA SLFMP TETVL

Exercice 2 : Chiffrement

Le message suivant a été chiffré avec l'algorithme de transposition en zig-zag de niveau 4. Donner le nom de l'algorithme de chiffrement et déchiffrer le cryptogramme suivant :

ENNOE LARTR TEDOR CMNND ASRER RIARE ETRTI EMOTN MRRTE ARNIR NEREE EEPEE

Exercice 3 : Stéganographie

La stéganographie est la science qui s'intéresse à la manière de cacher une information à l'intérieur d'une autre information, afin que sa transmission n'éveille pas les soupçons.
George Sand, maîtrisant parfaitement l'écriture, écrivait des poèmes à Alfred de Musset:

> Cher ami,
>
> Je suis toute émue de vous dire que j'ai bien compris l'autre jour que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et en amis franchement je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde, comme la plus étroite amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon où je …
>
> Votre poupée

Trouver le message caché dans ce texte.

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Exercice 4 : Services de sécurité

Alice (resp. Bob) utilisent également un système symétrique avec K_{AB} comme secret partagé. Quels sont les services des sécurités correctement fournis par les opérations suivantes, dans lesquelles E signifie "algorithme de chiffrement" et H "fonction de hachage" :

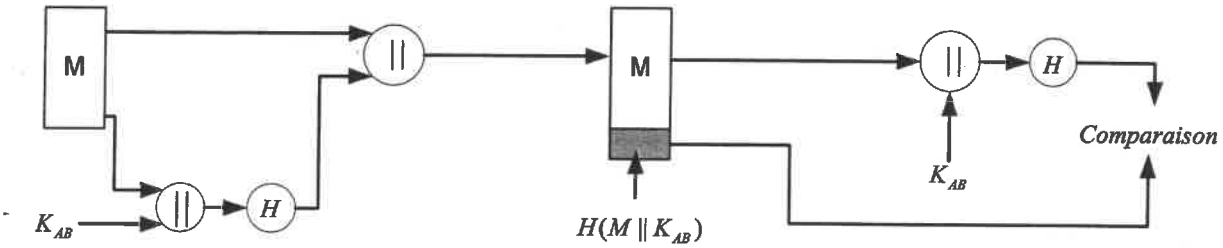
a) $E_{k_{AB}}[M]$

b) $M \| H(M)$

c) $E_{k_{AB}}[M \| H(M)]$

d) $M \| E_{k_{AB}}[H(M)]$

e)



Exercice 5: Authentification

Alice et *Bob* sont deux correspondants se partageant un secret *K*. Ils utilisent le mécanisme suivant : *Alice* envoie son identité accompagnée d'un nombre aléatoire N_A à *Bob*, qui renvoie en retour son identité, un nombre aléatoire N_B et le nombre envoyé par *Alice* chiffré avec la clé partagée *K*. *Alice* renvoie enfin à *Bob* le nombre N_B chiffré avec la clé partagée *K*.

a) *A* et *B* sont-ils mutuellement certains de leurs identités respectives ?

b) Soit un attaquant *C* placé entre *Alice* et *Bob*, interceptant le trafic et se faisant passer pour *Alice* auprès de *Bob* et pour *Bob* auprès de *Alice*. *C* peut-il pénétrer les communications entre *A* et *B* dans le cas de l'échange du a) ?

Exercice 6 : cryptanalyse

Le texte suivant a été chiffré avec l'algorithme de Vigenère et une clé de longueur 2 (2 caractères). Sachant que le texte en clair est écrit en Français, trouver le texte lisible et donner la clé. Expliquer clairement la démarche suivie pour trouver la clé et pour déchiffrer.

```
HUZPVUKBZEEMVDZRVCVQLIVSKAIRZVV
```

Exercice 7 : cryptanalyse

Vous avez intercepté le message suivant :

```
RRMWU SZYHT GVMHK TGYIJ KZYJX KANAO HEYHK ZRAPA DRHSX UVNHR
KFXXY ZVHRZ OBHHY UPCPR KFHTV KHPTT ZRNGK LBHSK KFKJK YHLAA
                    ZVFXZ KPIBS AAY
```

Sachant que le texte en clair est écrit en français, et l'algorithme de chiffrement est Vigenère, et que la longueur de la clé est 5. Déchiffrer ce message en expliquant la démarche. (Le résultat du déchiffrement sans la démarche sera considéré faux)

Université Paris Descartes – UFR de mathématiques et Informatique

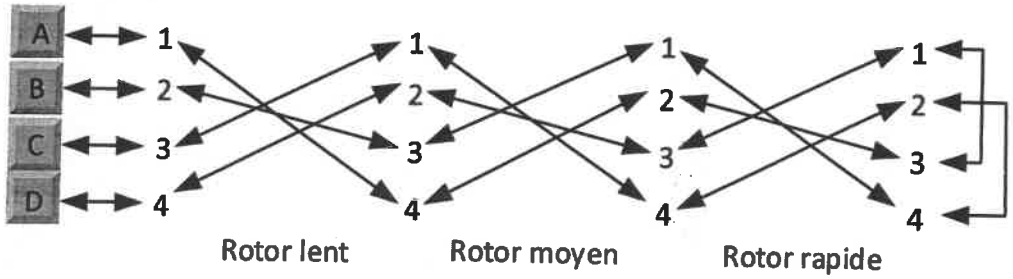
L3 – Sécurité et Réseaux

TD/TP n°2

Le classement des lettres selon leur fréquence d'apparition en français : E S A I T N R U L O D C P M V Q F B G H J X Y Z W K. Le tableau Vigenère est donné en annexe pour vous aider.

Exercice 8 : Enigma

"Enigma" est le nom de la machine de cryptographie utilisée durant la seconde guerre mondiale par l'Allemagne nazie et ses alliés.



Donner le résultat du chiffrement de la séquence "AABAAA" par le modèle simplifié donné par le schéma précédent.

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Annexe :

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

Tableau I : Table de Vigenère