Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

Exercice 1 : Chiffrement de Vigenère

Vous avez intercepté ce message chiffré avec l'algorithme de Vigenère. Déchiffrer le message sachant que la clé est ″RPS″ :

CXFKTFKXGEKSLIDVUSZI

Exercice 2 : Auto-chiffrement

Déchiffrer le message texte suivant, sachant qu'il est chiffré avec l'algorithme d'auto chiffrement et que la clé utilisée est ″RPS″.

CPUCYRKYCTLLSPCKXPSKEDVWHGUCRKCGNRDYFEEYW

Exercice 8 : Auto-chiffrement

Déchiffrer le message texte suivant, sachant qu'il est chiffré avec l'algorithme d'auto-chiffrement et que la clé utilisée est ″RPS″.

CPUCYRKYCTLLSPCKXPSKEDVWHGUCRKCGNRDYFEEYW

Texte en claire : LA CRYPTANALYSE EST L'ART DE DECRYPTER UN MESSAGE

Exercice 9 : Auto-chiffrement

Déchiffrer le message suivant, sachant qu'il est chiffré avec l'algorithme d'auto-chiffrement, et qu'il y a eu une indiscrétion (clé de chiffrement: ″DESCARTES″) :

OEKVEXTRGRRSILOERGZUEUHQVIHTVWJRQEEEEJUYLVZEHWRIYXNZWMFAAXUE

DESCARTES

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

O14	*E*	*K10*	*V21*	*E4*	*X23*	*T*	*R17*	*G6*	*R17*
D3	*E*	*S18*	*C2*	*A0*	*R17*	*T*	*E4*	*S18*	*L11*
L	*A*	*S*	*T*	*E*	*G*	*A*	*N*	*O*	*G*
R17	*S*	*I8*	*L11*	*O*	*E*	*R*	*G*	*Z*	*U*
A	*S*	*T19*	*E4*	*G*	*A*	*N*	*O*		
R	*A*	*P*	*H*	*I*	*E*	*E*	*S*	*T*	

LA STEGANOGRAPHIE EST DE FAIRE PASSER INAPERCU UN MESSAGE DANS UN AUTRE

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

Exercice 10 : Chiffrement de PlayFair (4pts) => 133/133

Soit un système polyalphabétique qui utilise une matrice 5x5 avec un *mot-clé* suivi des autres lettres de l'alphabet (avec W et X dans la même case). Chaque groupe de 2 lettres est codé par la lettre à l'intersection de la ligne de la première et la colonne de la seconde puis à l'intersection de la ligne de la seconde et de la colonne de la première. Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de droite (avec rotation circulaire) ; Si les deux lettres tombent sur la même colonne, on remplace chacune par celle de dessous (avec rotation circulaire). En cas de lettre double et en cas de lettre unique (nombre total de lettres impair), une lettre ″parasite″ est insérée (W).

Déchiffrer le message suivant :

La clé était caché dans le sujets. Comme s'appelle cette technique ? sauriez-vous retrouver la clé ?

IL OP IL NI IZ NE QP YO IQ XI IL FS LA TY

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

IL =LE
OP =SO
IL = LE
NI= IL
IZ=LU
NE =IT
QP=PO
YO=UR
IQ=TO
XI =UT
IL =LE
FS=MO
LA=ND
TY=EW

LE SOLEIL LUIT POUR TOUT LE MONDE

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

Exercice 5 : Chiffrement de Rail Fence

Rail Fence est une forme de transposition qui consiste à écrire les lettres en "Zig-Zag". Déchiffrer le message suivant, sachant que la clé est 3 (niveau=3).

LOSSTERLEEXRS EHMENISNEDMUETIRSTGUEDOT SMAETENBEANI =49 lettres

13 cases ou 13 lettres sur la première ligne

La ligne 2 : 24 cases

La ligne 3 : 12 cases

L				**o**				**s**		
	e		**h**		**m**		**e**		**n**	
		S				**M**				**A**

	s				**t**				**e**				**r**				**L**
i		**s**		**n**		**e**		**d**		**m**		**u**		**e**		**T**	
			E				**T**				**E**				**N**		

			e				e				x				r				s
I		R		S		T		G		U		E		D		O		T	
	B				E				A				N				I		

Les hommes naissent et demeurent libres et egaux en Droits

Exercice 6 : Chiffrement via transposition de la matrice (0.5)

L'exemple ci-dessous utilise un système de chiffrement avec transposition de colonnes pour protéger des données confidentielles :

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

MGCDE CSSFT SENN EEOEL EATII*

Étant donné qu'il y a eu une indiscrétion, vous connaissez la clé 31542.
Déchiffrez le message : pour le chiffrement, on écrit le message en ligne et on le lit en colonnes.

Etape 1 : il faudra trouver le nombre des lignes
Nombre total des caractères : 25 = 5colonnes x X lignes

3	1	5	4	2
M	C	S	E	E
G	S	E	E	A
C	S	N	O	T
D	F	N	E	I
E	T	*	L	I

Remettre les colonnes dans l'ordre :

1	2	3	4	5
C	E	M	E	S
S	A	G	E	E
S	T	C	O	N
F	I	D	E	N
T	I	E	L	*

CE MESSAGE EST CONFIDENTIEL

Exemple de clarification sur le fonctionnement :
Arvin est le plus intelligent
E 645231 ==== > R 645231

1	2	3	4	5	6
A	R	V	I	N	E
S	T	L	E	P	L
U	S	I	N	T	E
L	L	I	G	E	N
T	*	*	*	*	*

Permutation des colonnes

6	4	5	2	3	1
E	I	N	R	V	A
L	E	P	T	L	S
E	N	T	S	I	U

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

N	G	E	L	I	L
*	*	*	*	*	T

ELEN*IENG*NPTE*RTSL*VLII*ASULT
Par substitution
Par transposition

Exercice 5 : Authentification : prouver l'identité (email+mdp)

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) *Alice (Aicha)* et *Bob (Brahim)* sont-ils mutuellement certains de leurs identités respectives ?

Oui, tous les deux ont fournis leur identité et une preuve via le chiffrement du nombre aléatoire avec la clé

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) ?

1- Oui, en volant la session et en arrêtant la retransmission des messages à Alice

2- Oui, en écoutant passivement

Exercice 6 : cryptanalyse

Le test suivant a été chiffré ave c 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.

```
HU=QU
ZP=IP
VU=EU
KB=TB
ZE=IE
EM=NM
VD=ED
ZR=IR
VC=EC
VQ=EQ
LI=UI
VS=ES
KA=TA
IR=RR
ZV=IV
V=E

QUI PEUT BIEN ME DIRE CE QUI EST ARRIVE
```

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

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
```

LES HOMMES NAISSENT ET DEMEUR ENT LIBRES ET EGAUX EN DROITS LES DISTINCTIONS SOCIALES NE PEUVENT ETRE FONDEES QUESUR LUTILITE COMMUNE

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)
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 9 : Enigma

AABAAA=> DBCBCD

Carte => ubuntu => backtrack 1 => 4
Backtrack => kali (debian)
@ip : 192.168.1.105

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°2

@MAC : ether 08:00:27:aa:3c:d5

Ping 192.168.1.103
arp -an

Telnet 23, FTP 21, SSH 22, http 80, HTTPS 443, DNS 53, SMTP 25, IMAP 143, SNMP 161

netstat -natp | grep 23
apt install wireshark

selectionner un paquet telent, clique droite, suivre Flux TCP => j'ai retrouvé login et mdp et commandes et commandes et le contenu du ficher
le numero de port est 23, le protocole de transport est TCP