Correction détaillée du TD1-2-3 :

Table des matières

TD1 :

EXERCICE 1 :

DÉFINITION :

- Authentification : il s'agit de la possibilité de validé l'identité d'une personne. (Identité + preuve).
- Identité : c'est ce qui représente la personne. (login par exemple).
- Mécanisme d'authentification : reconnaissance faciale/clé/empreinte/reconnaissance fessière(chine).
- 3 sortes de mécanisme : qu'on connait , qu'on possède (carte à puce) ou qu'on est (empreinte, faciale).
- Attaque MITM (Man In The Middle) : écoute et analyse les trafics du réseau via l'outil Wireshark.

Question 1 :

Le but de l'exercice est de trouver les différentes failles aux systèmes de sécurité utilisés pour savoir si Alice peut se faire Usurper son identité par Trudy.

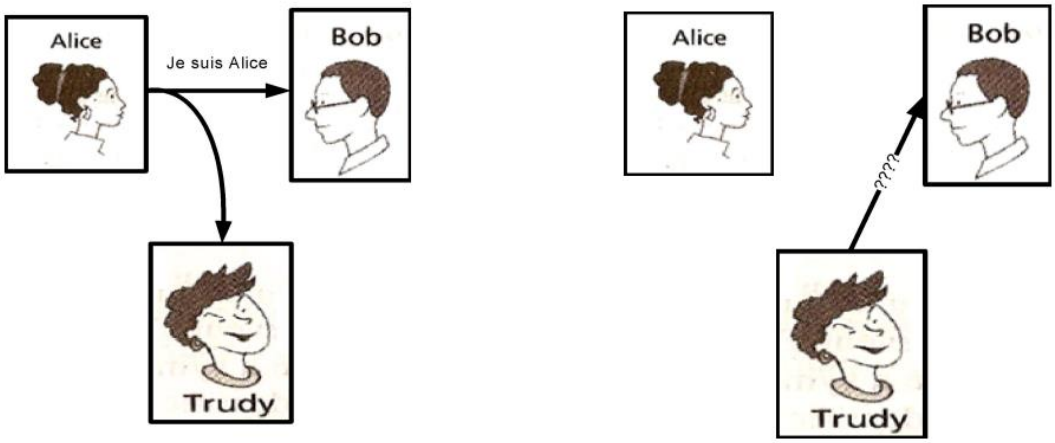


Figure 1 : Protocole d'authentification pda 1.0

Dans cet exemple, il s'agit de l'utilisation de la méthode ARP Poisoning, ici il y a une faille car Trudy pourra dire à Bob « Je suis Alice », car il suffit de validé l'identité sans preuve.

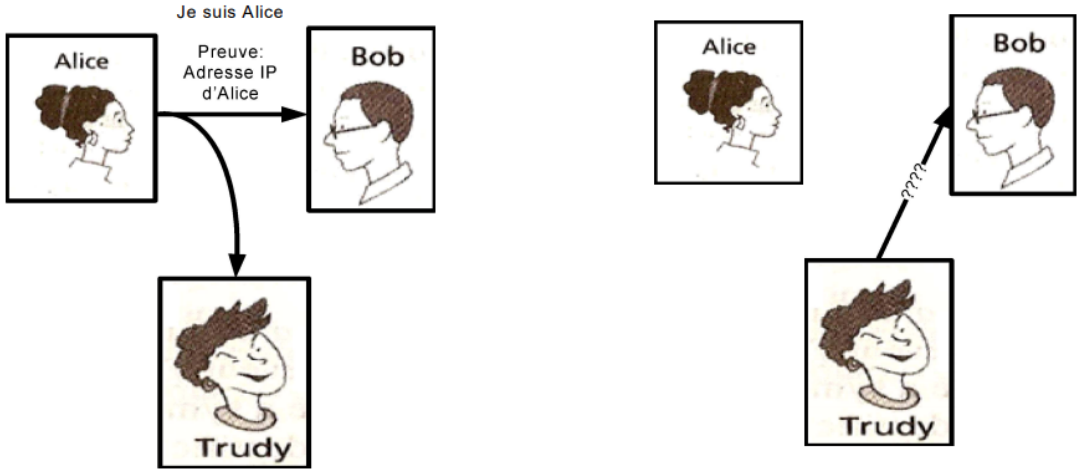


Figure 2 : Protocole d'authentification pda 2.0

Dans cet exemple, Oui, car elle peut dire « je suis Alice » et spoofer (retrouver son adresse IP) son IP à l'aide du logiciel Wireshark. -> Usurper son identité.

Figure 3 : Protocole d'authentification pda 3.0

Dans cette exemple, l'authentification (validation de l'identité par une preuve) seras intercepté par Trudy et donc pourras le réutiliser pour usurper son identité.

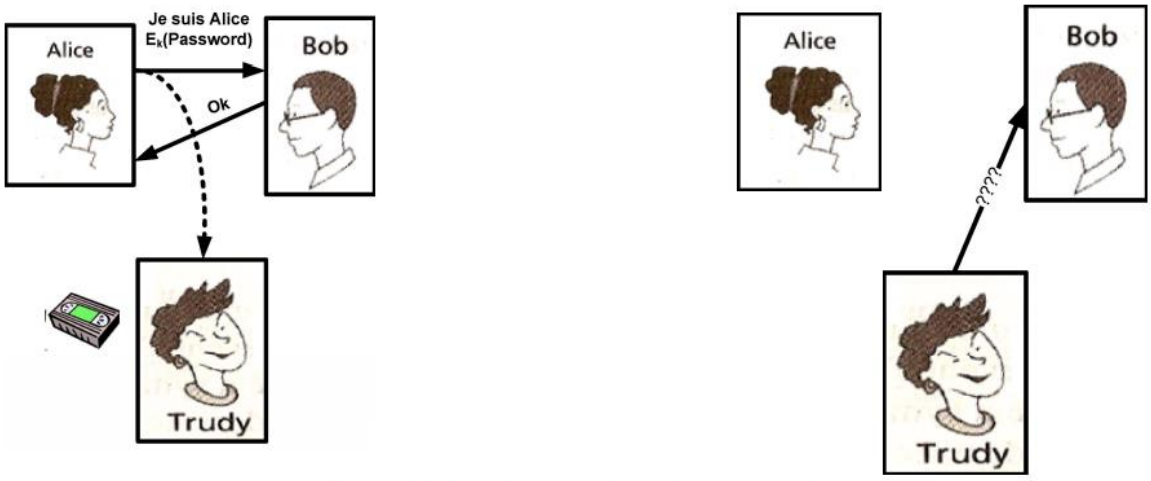


Figure 4 : Protocole d'authentification pda 4.0

Dans cette exemple, Trudy peut usurper l'identité d'Alice, car bien que le mot de passe soit chiffré, Trudy peut l'envoyer chiffré sans avoir besoin de le dechiffré.

Figure 5 : Protocole d'authentification pda 5.0

Ici Trudy ne peut pas usurper l'identité d'Alice car il y a un défi et que pour pouvoir déchiffrer le mot de passe il faut posséder la clé. Par contre il peut y avoir un vol de session.

Il n'est pas possible d'essayer de trouver le Nonce, car par définition un Nonce est un nombre destiné à une seul utilisation, ainsi même si Trudy l'intercepte elle ne peut pas l'utiliser pour une autre fois.

Chose à connaitre : E() -> fonction qui va permettre de crypter.

EXERCICE 2 :

DÉFINITION :

CIA : Confidentialité, Intégrité et Disponibilité.
Authentification : Permettre de valider l'identité de quelqu'un à l'aide d'une preuve.
Confidentialité : Rendre le message compréhensible seulement par l'émetteur et le récepteur.
Intégrité : Permet de savoir qu'une information n'as pas été modifier pendant son transfert.
Non-répudiation : Empêche à une personne de pouvoir nié une action commise (pas ce semestre).
Disponibilité : Accessible en temp défini.

Corrigé :

Confidentialité : Envoyer un message privé.
Intégrité : Message arrivé intact.
Autorisation : Mot de passe.
Authentification : Être sûr de l'origine du message.
Non répudiation : L'action ne peut plus être nié une fois effectuer.
Contrôle d'accès : Vérifier le privilège de modifier un fichier.

EXERCICE 3 : CHIFFREMENT PAR SUBSTITUTION :

Inconveniant : les lettres de l'alphabet couramment utilisés seront apercu et ainsi on peut déchiffrer.

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

Dans l'exo il a oublié de mettre la lettre V, qui correspond à E.
Méthode pour chiffrer un contenu : il suffit de prendre les lettres dans la première ligne et de les associer avec la lettre qui est en dessous.
S E C U R I T E R E S E A U X
T C N P I W G C I C T C R P V

On peut observer que par exemple dans le tableau la lettre S (rouge) correspond à la lettre T (méthode chiffrement).

A présent pour déchiffrer, il suffit de prendre le message, de retrouver les lettres du message dans la ligne 2 et de voir à quoi elle corresponde dans la ligne 1.
Exemple la premier lettre P (en vert correspond à U).

PX GWCXT ERPG ZWCPV SPC YCPV GP ORPIRT

UN TIENS VAUT MIEUX QUE DEUX TU LAURAS.

EXERCICE 4 :

Le chiffrement de césar est simple d'utilisation, il suffit d'effectuer un Chiffrement par substitution (exo 3) mais pour remplir les lettres qui remplace celle de l'alphabet on effectue un décalage des lettres de l'alphabet, dans notre exercice il y a un décalage de 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

Pour chiffrer (avec décalage de 3) :
Prendre la première lettre ici B (en rouge) et faire le décalage : B(2) + 3 = 5 = E.
Une fois qu'on à celui pour B on peut soit remplir le tableau manuellement (conseiller) à partir de B ou le faire à chaque fois.

Ex :
BENJAMIN

EHQMDPLQ

CORRECTION :

On utilise une analyse fréquentielle :

Ici, il y a un décalage de 4, pour trouver le décalage il faut prendre le chiffre qui apparait le plus de fois dans la séquence :

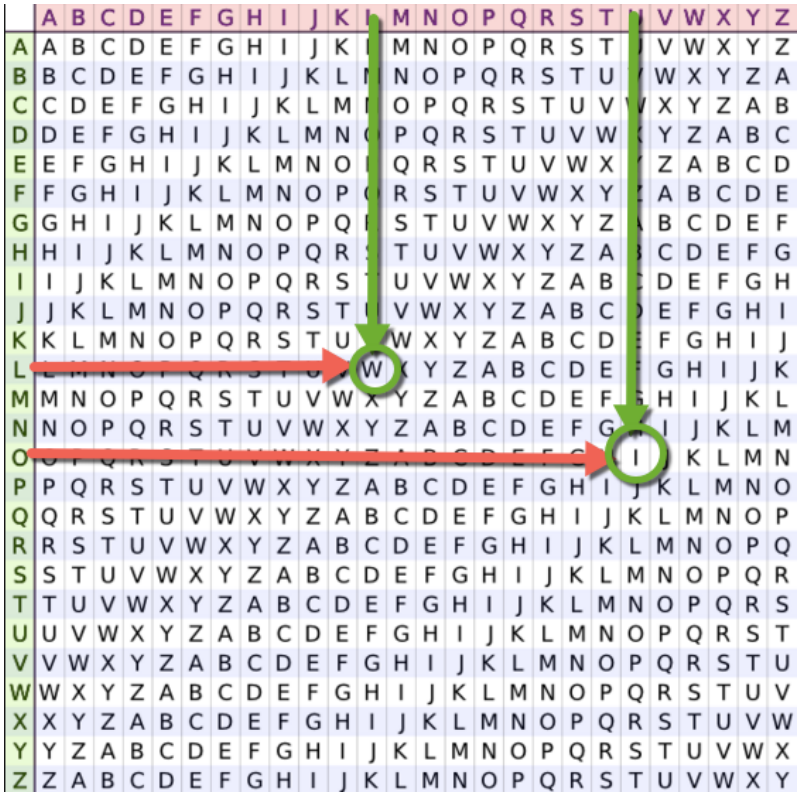
P I N I Y R I Z E Y X T E W P E G L E R H I P P I

5 fois I : On décale le tableau de 5 et on obtient E (5^{e} lettre de l'alphabet) = A (1ere lettre décalé de 5). C'est la méthode Al-Kindi.

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

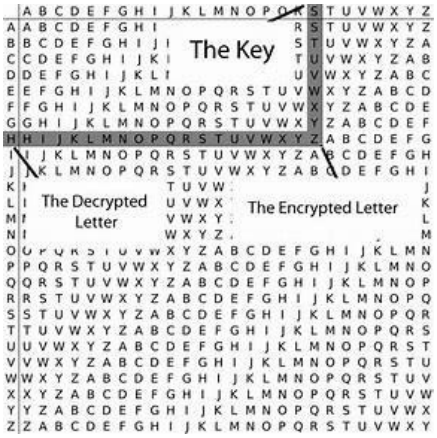
EXERCICE 7 : CHIFFREMENT DE VIGENERE:

Vigenere s'inspire de César, mais relève un problème, c'est qu'on peut déchiffrer le message grâce à l'analyse fréquentielle, il propose ainsi de déchiffrer le message à l'aide de son tableau :



- Pour chiffrer : On prend le message sur la ligne du haut et on utilise la clef sur la colonne à gauche, dans l'exemple de ce tableau la clé est LO et le message est IN, ainsi on lie la clef avec le message et on entre l'intersection.

- Pour déchiffrer : On utilise la clef et on repère la première lettre chiffre avec cette lettre de la clef, une fois sur cette lettre on remonte la lettre appartenant à cette intersection :
Exemple :



Correction :

Le message Crypte(illisible) avec VIGENERE : C X F K T F K X G E K S L I D V U S Z I
La clé : RPS. R P S R P S R P S R P S R P S R P S R P

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Pour la première lettre je prends R dans la colonne de gauche et je vais remonter dans la ligne de R jusqu'à trouver C, puis quand je suis à C je remonte la colonne et je trouve L, et ainsi de suite je trouve :

C X F K T F K X G E K S L I D V U S Z I
R P S R P S R P S R P S R P S R P S R P

Déchiffré : L I N T E N T I O N V A U T L E F A I T.

EXERCICE 8 : Auto-Chiffrement :

Il faut pour cet exercice, chiffrer à partir de la clé le message :
RPS : clé.
CPUCYRKYCTLLSPCKXPSKEDVWHGUCRKCGNRDYFEEYW : Message crypté.

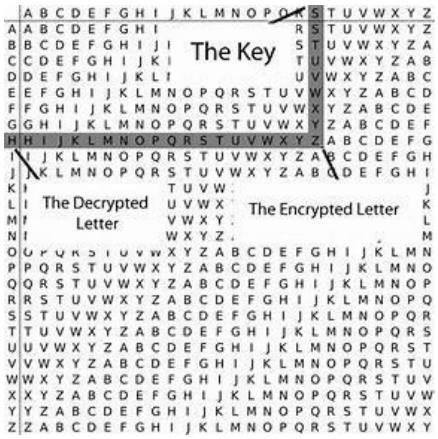
LA CRYPTANALYSE EST LART DE DECHIFFRER UN MESSAGE : Message décrypté.

CORRECTION :

L'algorithme d'auto-chiffrement est inspiré de l'algorithme de Vigenere.
Pour déchiffrer un message à l'aide de la clé, on procède de la manière suivante :

On utilise le tableau de Vigenere pour cela, on fait pour la première lettre je prends R dans la colonne de gauche et je vais remonter dans la ligne de R jusqu'à trouver C, puis quand je suis à C je remonte la colonne et je trouve la lettre L, je fais ça pour chaque lettre et je trouve :

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



EXERCICE 9 : MEME PRINCIPE :

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

L A S T E G A N O G R A P H I E E S T D E F A I R E P A S S E R I N A P E R C U U N M E S S A G E D A N S U N A U T R E

EXERCICE 10 : PLAYFAIR :

Cle: INTELLIGENT.

Il faut faire une matrice 5x5 à l'aide de la clé sans mettre de doublons, et ensuite une fois que la clé est insérée mettre l'alphabet sans répéter les lettres déjà présentes dans la clé, il y aura deux lettres qui seront dans la même case ce sont des lettres dites « parasites », ici c'est XW :

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

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

Pour chiffrer :

- Bleu c'est les lettres chiffrer ; Vert sont les lettres Déchiffrer.
- Si les deux lettres tombent sur la même colonne, on remplace chacune par celle de dessous (avec rotation circulaire).
- Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de droite (avec rotation circulaire).
- 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.

Pour déchiffrer :

- Bleu c'est les lettres chiffrer ; Vert sont les lettres Déchiffrer.
- Si les deux lettres tombent sur la même colonne, on remplace chacune par celle au-dessus (avec rotation circulaire).
- Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de gauche (avec rotation circulaire).
- 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.

EXERCICE 11 : RAIL FANCE (ZIG_ZAG) : TRANSPOSITION.

Algorithme de transposition : changer les places des lettres du messages.

Méthode pour chiffrer : Mettre la phrase en zigzag en fonction des niveaux et ensuite lire le message ligne par ligne.

BENJAMIN sur 3 niveaux.
Chiffré : BA EJMN NI

B				A			
	E		J		M		N
		N				I	

Pour déchiffrer : Compter le nombre de lettres présent dans le message et simuler le zig-zag, puis le remplir en fonction du message chiffrer ligne par ligne, puis assembler le messages en zig-zag une fois le tableau remplit :

1 = B				5 = A			
	2 = E		4 = J		6 = M		8 = N
		3 = N				7 = I	

Correction : *LESHOMMESNAISSENTETDEMEURENTLIBRESETEGAUXENDROIT*

LOSST ERLEE XRSEH MENIS NEDMU ETIRS TGUED OTSMA ETENB EANI

1 L				*5 O*				*9 S*				*13 S*				*17 T*			
	2 E		*4 H*		*6 M*		*8 E*		*10 N*		*12 I*		*14 S*		*16 N*		*18 E*		*20 D*
		3 S				*7 M*				*11 A*				*15 E*				*19 T*	

21 E				*25 R*				*29 L*				*33 E*				*37 E*			
	22 M		*24 U*		*26 E*		*28 T*		*30 I*		*32 R*		*34 S*		*36 T*		*38 G*		*40 U*
		23 E				*27 N*				*31 B*				*35 E*				*39 A*	

41X				*45R*				*49S*

	42 E		*44 D*		*46 O*		*48 T*	
		43 N				*47 I*		

EXERCICE 12 : Chiffrement par transposition de colonne :

Pour chiffrer : On écrit le message en ligne, puis on coupe le message par ordre de colonne, dans notre exercice il on utilise 31542, EX :

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	*

MGCDE CSSFT SENN EEOEL EATII = CE MESSAGE EST CONFIDENTIEL.*

Pour Déchiffrer le message, il suffit de compter le nombre de lettres, puis de le diviser par le nombre de colonnes (que tu connais grâce à la clé), et de remplir les colonnes en fonction de l'ordre qu'ils ont donné, ici il y avait 25 lettres soit 5 lettres par colonnes, et l'ordre était le suivant, 31541, ainsi j'ai :

3 : MGCDE

1 : CSSFT

5 : SENN*

4 : EEOEL

2 : EATII

Il reste plus qu'à les remettes dans l'ordre et lire le message par ligne comme dans l'exemple cités en haut.

TD2 :

EXERCICE 1 :

Question 1 :

CIA : Confidentialité, Intégrité, Disponibilité.

Question 2 :

a) Rejeu : MITM : intercepter des paquets de données (Trudy exo 1) et les rejouer.
b) Collecte d'informations type Facebook et Twitter : Collecte des données pour créer des trakers en fonction de nos envies.
c) Déni de service (DoS) : Envoyer en abondance des requêtes erronés afin que le serveur informatique soit paralysé où perturber.
d) Interception de message : MITM pour décoder des discussions….

Question 3 :

Clé : teamo.
Message chiffré : BAIEV AKUWI GRKAP IOBPS FWPXA SLFMP TETVL

Rappel, utilise le tableau de Vigenere pour décoder.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Clé : teamo.
Message chiffré : BAIEV AKUWI GRKAP IOBPS FWPXA SLFMP TETVL
TEAMO TEAMO TEAMO TEAMO TEAMO TEAMO TEAMO

Message déchiffré : I WISH…

EXERCICE 2 :

ENNOE LART R TEDOR CMNND ASRER RI ARE ETRITI EMOTN MRRTE ARNIR NEREE EEPEE

Je me suis tromper j'ai insérer 5 lettres en trop mais voilà l'idée.

60 Lettres, avec niveau = 4.

1 E						7 N						13 N						19 N						25 O					
	2 R				6 T		8 E				12 D		14 O				18 R		20 C				24 M		26 N				30 N
		3 A		5 R				9 E		11 E				15 T		17 R				21 I		23 T				27 I		29 E	
			4 A						10 R						16 N						22 I						28 R		

31 E						37 L						43 A						49 R						55 T					
	32 N				36 D		38 A				42 S		44 R				48 E		50 R				54 R		56 I				60 A
		33 M		35 O				39 T		41 N				45 M		47 R				51 R		53 R				57 T		59 E	
			34 N						40 E						46 R						52 E						58 E		

EXERCICE 3:

Stéganographie c'est l'art de cache des messages dans un texte ou un fichier…, ici le contenu est trop hard pour que le prof fasse la correction, pour les curieux il faut lire 1 ligne sur 2.

EXERCICE 4 :

Question A)

$Ek_{AB}[M]$:

Confidentialité : Oui, car le message est crypté.
Intégrité : Non, car il peut modifier le message.
Authentification : Oui, car il y a la cle K_{ab}.
Non-répudiation : Ce semestre toujours mettre nan et gagne ¼ des points sur ça.

Question B)

M || H(M) :

Confidentialité : Non, car il peut voir le message et le digest.
Intégrité : Non, car il peut modifier le message, même si l'empreinte vas changer.
Authentification : Nan, car il n'y a pas de preuve.
Non-répudiation : Ce semestre toujours mettre nan et gagne ¼ des points sur ça.

Question C)

$Ek_{AB}[M \,||\, H(M)]$:

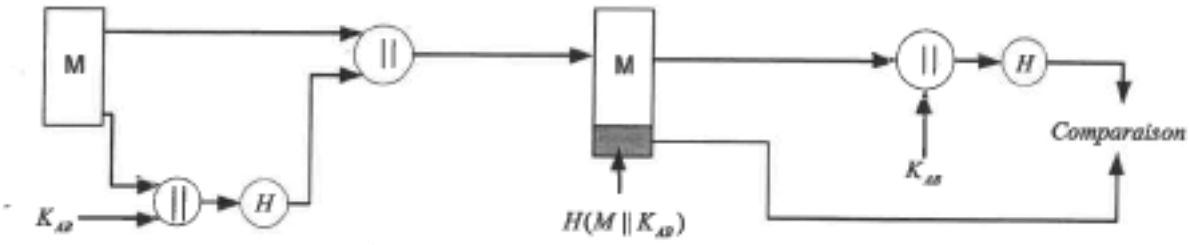
Confidentialité : Oui, il ne peut pas voir le message car il est crypté.
Intégrité : Oui, car s'il change le message, l'empreinte change.
Authentification : Oui, car il y a la clef qui permet de le faire.
Non-répudiation : Ce semestre toujours mettre nan et gagne ¼ des points sur ça.

Question D)

M || $Ek_{AB}[H(M)]$:

Confidentialité : Non car il peut voir le message.
Intégrité : Oui,
Authentification : Oui,
Non-répudiation : Ce semestre toujours mettre nan et gagne ¼ des points sur ça.

Question E)



Confidentialité : Non, car il ne peut pas voir le message.
Intégrité : Oui, car le MitM ne peux pas génère une empreinte valide car il possède la clé qui est inconnu.
Authentification : Oui, car il y a l'utilisation d'une clé comme preuve d'identité.
Non-répudiation : Ce semestre toujours mettre nan et gagne ¼ des points sur ça.

EXERCICE 5 : Authentification.

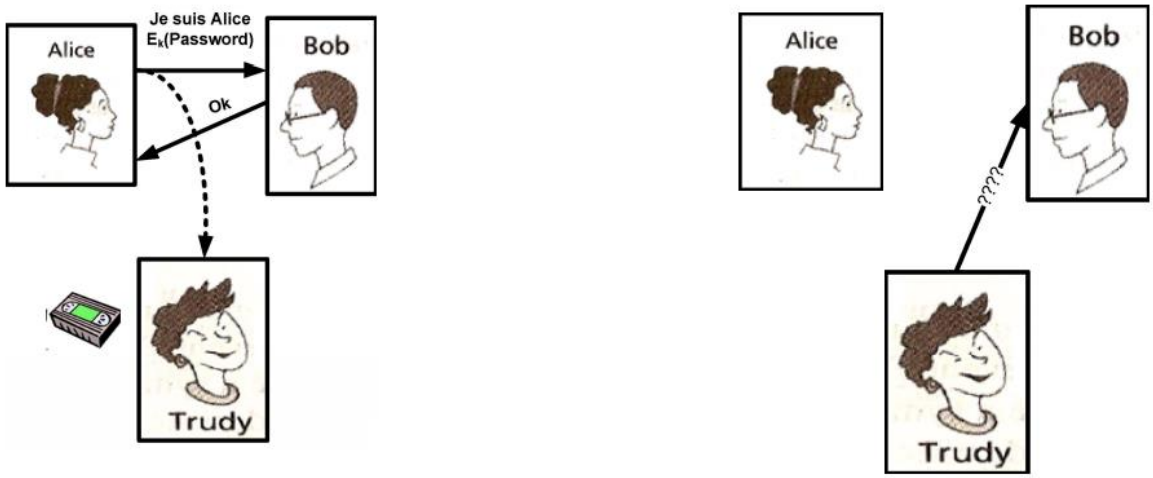


Figure 4 : Protocole d'authentification pda 4.0

Indexe représentative du cas à peu près.

Question a :

Dans ce mécanisme (dans ce cas il n'y à pas Trudy), effectivement puisque Bob et Alice envoie une clé qui permet de les authentifier (identité + preuve) ainsi, on peut dire qu'ils peuvent être sûr de leurs identités respectives selon la définition de l'authentification.

Question b :

Effectivement, dans le cas où une personne nommé C ou Trudy (voir indexe), en interceptant les échanges entre les deux, elle peut voler ainsi la session de Alice ou Bob une fois l'authentification faite et ainsi se faire passer pour Alice ou Bob et voler toutes les informations qui vont passer.

EXERCICE 6 et EXERCICE 7:

Méthode :

Pour cet exercice, on utilise l'algorithme de Vigenère, cependant on ne connait pas la clé, on ne connait que la longueur de la clé, la méthode est la suivante cependant en cas pratiques elle n'est pas infaillible, (le jour de l'exam elle le sera selon le prof) :

Il faut découper le message crypte en fonction de la cle et place ainsi le message par colonne :

Exo 7 :

```
RRMWU = LESHO
SZYHT = MMESN
GVMHK = AISSE
TGYIJ = NTETD
KZYJX = EMEUR
KANAO = ENTLI
HEYHK = BRESE
ZRAPA = TEGAU
DRHSX = XENDR
UVNHR = OITSL
KFXXY = ESDIS
ZVHRZ = TINCT
OBHHY = IONSS
UPCPR = OCIAL
KFHTV = ESNEP
KHPTT = EUVEN
ZRNGK = TETRE
LBHSK = FONDE
KFKJK = ESQUE
YHLAA = SURLU
ZVFXZ = TILIT
KPIBS = ECOMM
AAY   = UNE
```

Puisque la clé est de longueur 5, ainsi j'ai réalisé le découpage des colonnes par 5, puis je dois réaliser une analyse fréquentielle (voir combien de fois apparait chaque lettre dans chaque colonne) et celle qui apparait le plus je réalise un décalage de césar pour déchiffrer la première colonne :
Exemple :

1ère colonne, la lettre qui apparait le plus est la lettre K, je place donc dans un tableau le décalage en mettant K à la lettre E (c'est la méthode avec le chiffrement de césar du prof), et cela me donne : il s'agit d'un décalage de 6 (case rouge) :

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
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

Puis je fais la substitution sur la 1ere colonne, et je transpose le résultat à cote du message (voir résultat en haut), et je continue pour chaque colonne.

`Résultat de la transposition : LMANE EBTXO ETIOE ETFES TEU.`

Exemple pour la colonne 2 :

La lettre qui apparait le plus est la lettre R, ainsi je refais le décalage de César en plaçant R en dessous de la case de E (vert), et cela me donne un chiffrement de 13 (case rouge) :

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
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

Puis je fais la substitution sur la 2eme colonne, et je transpose le résultat à cote du message (voir résultat en haut), et je continue pour chaque colonne.

`Résultat de la transposition : EMITM NREEI SIOCS UEOSU ICN.`

Et je continue comme ça, sur chaque colonne et j'obtiens : Les hommes naissent et demeurent libres et égaux en droits. Les distinctions sociales ne peuvent être fondées que sur l'utilité commune. (Article 1er de la constitution des droits de l'homme il kiff celui la).

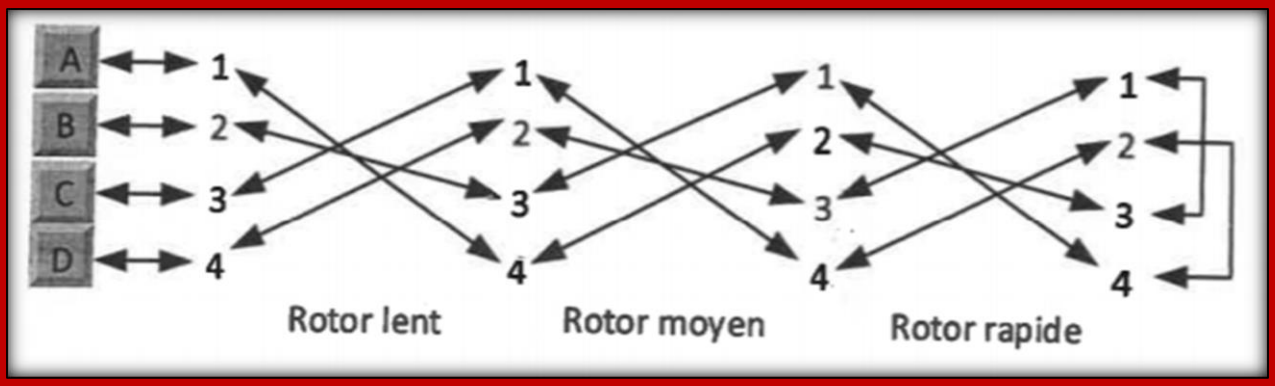
L3 Semestre 6 • Sécurité et réseaux

(IF06X080)

TD/TP n°2

8 # Énigma

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



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

Les rotors sur ces images sont comparés aux horloges mécaniques de l'époque, car elle fonctionne à peu près de la même manière.

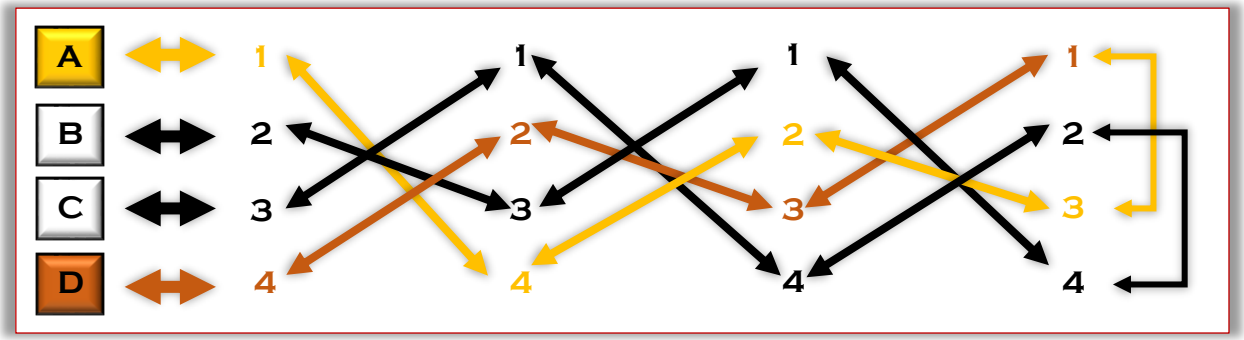
- **Le rotor Rapide** est comparé au rotor des secondes, car il vat réalise un décalage d'un cran à chaque seconde.
- **Le Rotor moyen** est comparé à celui des minutes car il faut attendre que le rotor rapides (secondes) effectue un tour complet (60 sec) pour pouvoir effectuer un décalage de 1.
- **Le dernier et le rotor lent** et il est comparé à celui des heures qui doit attendre que le rotor moyen (minute) réalise un tour complet pour pouvoir faire un décalage de 1.

On veut tenter de chiffrer le message suivant : « AABAAA ».

Pour la première lettre,
on se trouve à l'état initial et on se place à la lettre A,
Puis on suit les flèches tout simplement,

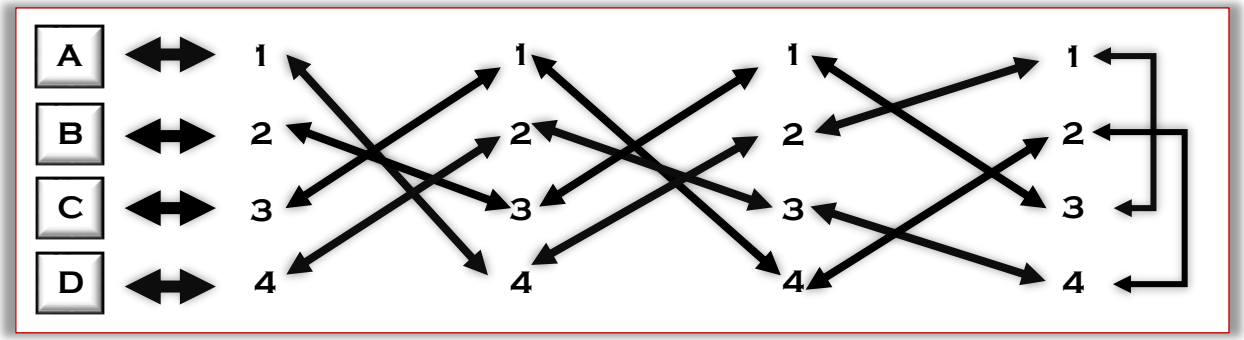
1→4 ,
4→2,
2→3,
3→1,
1→3,
3→2,
2→4

et ça nous donne la lettre D.

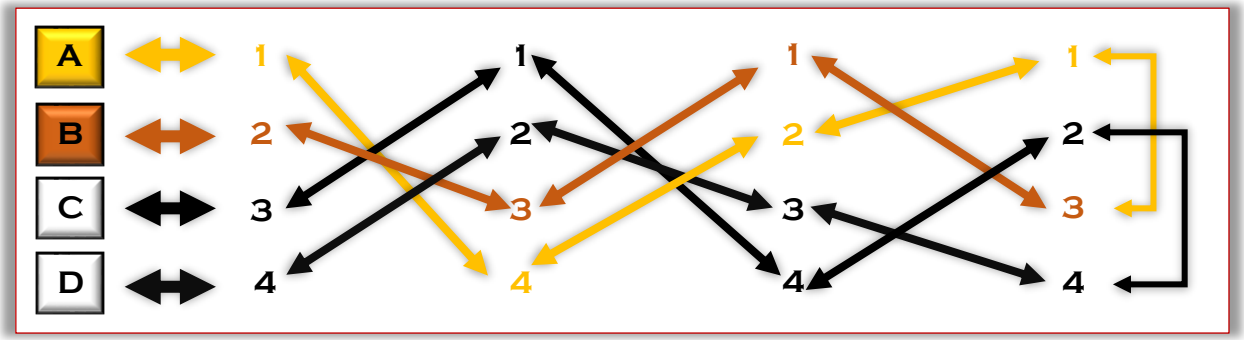


Puis pour la deuxième lettre,
on réalise d'abord un décalage sur le rotor rapide,
pour cela on procède par étapes,
Le 1 à l'état initial était lier au 4, on réalise un décalage de 1 dans les deux et ça deviens 1+1 = 2 et 4+1 modulo 4 = 1,

donc 2→1, puis la même chose avec 2, 2→3(état initial), donc 2+1 = 3 et 3+1 = 4, ainsi on obtient dans le nouveau rotor 3→4, puis en ce qui concerne 3 : 3→1(état initial), on fait le décalage de 1 et on obtient 4→2 et pour finir par élimination on obtiens 1→3, et ça nous donne le nouveau schéma des rotors en dessous :



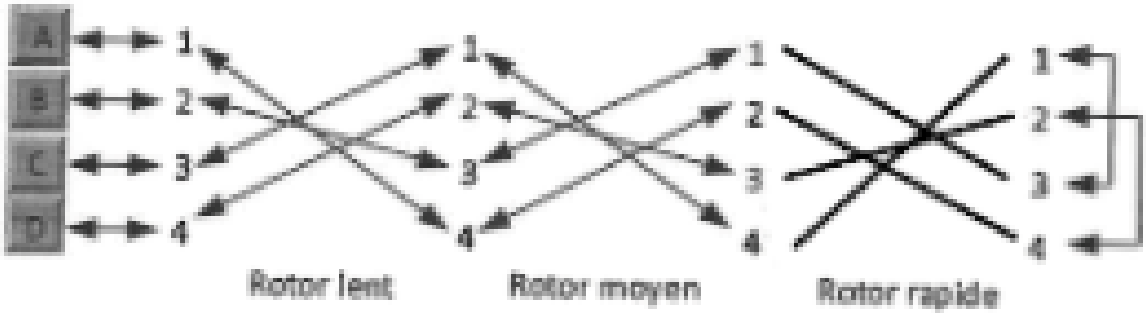
On désire encore une fois la lettre A :
1→4,
4→2,
2→1,
1→3,
3→1,
1→3,
3→2,
et ça nous donne la lettre B, pour l'instant on à DB.



Pour la 3e lettres, on effectue la même procédure, soit un décalage de 1 au niveau des directions du rotor rapides.

- Pour 1 : 1→3 (état initial), donc 1+1 = 2 et 3+1 = 4, ainsi 2→4.
- Pour 2 : 2→1 (état initial), donc 2+1 = 3 et 1+1 = 2, ainsi 3→2.
- Pour 3 : 3→4 (état initial), donc 3+1 = 4 et 4+1 mod 4 =1, ainsi 4→1.
- Pour 4 : Par élimination on obtient 1→3.

Ce qui nous donne la nouvelle conception suivante :

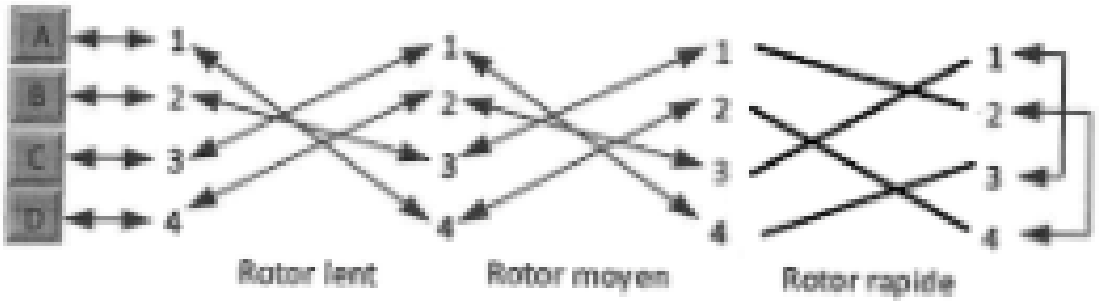


On veut à présent la lettre B, 2→3, 3→1, 1→3, 3→1, 1→4, 4→1, 1→3, et on obtient la lettre C, on a donc pour l'instant pour AAB = DBC.

Pour la 4e lettre, on effectue la même procédure, soit un décalage de 1 au niveau des directions du rotor rapides.

- Pour 1 : 1→3 (état initial), donc 1+1 = 2 et 3+1 = 4, ainsi 2→4.
- Pour 2 : 2→4 (état initial), donc 2+1 = 3 et 4+1 mod 4 =1, ainsi 3→1.
- Pour 3 : 3→2 (état initial), donc 3+1 = 4 et 2+1 = 3, ainsi 4→3.
- Pour 4 : Par élimination on obtient 1→2.

Ce qui nous donne la nouvelle conception suivante :

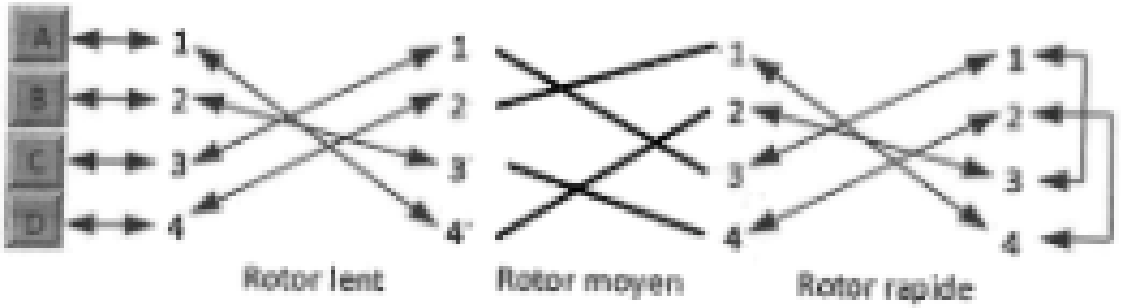


On veut à présent la lettre A, 1→4, 4→2, 2→4, 4→2, 2→1, 1→3, 3→2, et on obtient la lettre C, on a donc pour l'instant pour AABA = DBCB.

Pour la 5e lettre, on effectue la même procédure, soit un décalage de 1 au niveau des directions du rotor rapides, mais puisque qu'on à effectuer 4 décalages donc le rotor rapide reviens à la position initiale, et donc après chaque tour complet on effectue un décalge de 1 dans le rotor moyen :

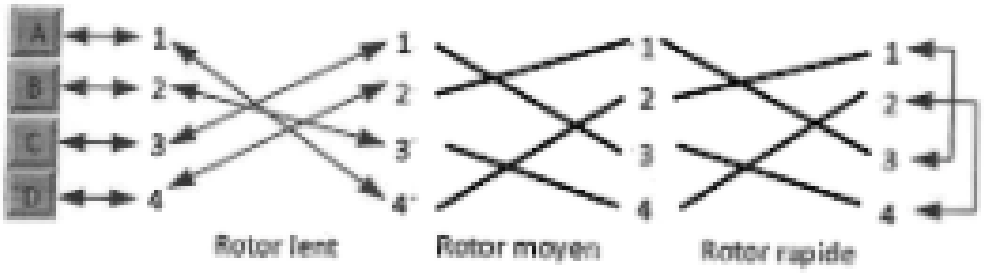
- Pour 1 : 1→4 (état initial), donc 1+1 = 2 et 4+1 mod 4 =1, ainsi 2→1.
- Pour 2 : 2→3 (état initial), donc 2+1 = 3 et 3+1 = 2, ainsi 3→4.
- Pour 3 : 3→1 (état initial), donc 3+1 = 4 et 1+1 =2, ainsi 4→2.
- Pour 4 : Par élimination on obtient 1→3.

Ce qui nous donne la nouvelle conception suivante :



On veut à présent la lettre A, 1→4, 4→2, 2→3, 3→1, 1→3, 3→1, 1→3, et on obtient la lettre C, on a donc pour l'instant pour AABAA = DBCBC.

Pour la dernière lettre, on réalise d'abord un décalage sur le rotor rapide, pour cela on procèdes par étapes, le 1 à l'état initial (voir plus haut) était lier au 4, on réalise un décalage de 1 dans les deux et ça deviens 1+1 = 2 et 4+1 modulo 4 = 1, donc 2→1, puis la même chose avec 2, 2→3(état initial), donc 2+1 = 3 et 3+1 = 4, ainsi on obtiens dans le nouveau rotor 3→4, puis en ce qui concerne 3 : 3→1(état initial), on fait le décalage de 1 et on obtiens 4→2 et pour finir par élimination on obtiens 1→3, et ça nous donne le nouveau schéma des rotors en dessous :



Donc pour la dernière, on se trouve à l'état initial et on se place à la lettre A, Puis on suit les flèches tout simplement, 1→4 ,4→2, 2→1, 1→3, 3→1, 1→2, 2→4 et ça nous donne la lettre D.

Et du coup on obtient que le messages : AABAAA = DBCBCD.

TD 3 :

EXERCICE 1 : Commandes Systemes et réseaux.

1) Quelle commande permet de visualiser l'adresse MAC (Physique) et l'adresse IP (logique) de votre station ? ifconfig -a.
2) A partir de votre terminal, exécuter la commande "ping" avec une station voisine. Quelle commande système permet de visualiser les adresses MAC et IP des hôtes avec lesquelles vous avez échangés des trames ? ARP -a.
3) Identifier les ports suivants :
   - Telnet (23).
   - FTP (21). ftp-DATA (20).
   - SSH (22).
   - HTTP (80).
   - HTTPS (443).
   - DNS (53).
   - SMTP (25).
   - IMAP (143).
   - SNMP (162).

EXERCICE 2 : Serveur Telnet :

Question 1.

Tout d'abord, il faut se placer dans root, puis télécharger en tant que superutilisateur Telnet avec la commande : « apt install telnetd », vérifier que la commande avec fonctionner avec la commande « echo $? » (0 : bien exécuter).
A présent je peux vérifier qu'elle est prête à écouter un contrôle avec la commande « netsta -antp » soit le à pour all, n pour numerique (voir les ports) et t pour tcp.

Question 2 : Effectuer la demande.

Question 3 :

- Qu'elle est le numéro du port du serveur ? 23.
- Quel est le protocole de transport utilisé par Telnet ? TCP.
- Donner la commande qui permet de vérifier que le serveur écoute sur ce port ? netstat -lnt | grep 23 -> grep 23 permet de filtrer celle ou le chiffre 23 est présent.

Question 4 :

Via le logiciel Wireshark, retrouvez votre login et mot de passe. Est-il lisible ? Retrouver aussi le résultat de vos commandes ″ls″, ″pwd″, etc. Sont-ils lisibles par un MITM ?

Oui, ils sont lisibles par la procédure suivant -> filtre : telnet -> sélectionner une ligne de Wireshark -> clique droit -> suivre -> flux TCP.

Je pourrais observer tt ce que j'ai fait dans l'autre machine, même le login et le MDP, ainsi elles peuvent être lisible par un MITM (Man In The Middle).

EXERCICE 3 :

Question 1 :

Tout d'abord, il faut se placer dans root, puis télécharger en tant que superutilisateur usftpd avec la commande : « apt install usftpd », vérifier que la commande avec fonctionner avec la commande « echo $? » (0 : bien exécuter).
A présent je peux vérifier qu'elle est prête à écouter un contrôle avec la commande « netsta -antp » soit le a pour all, n pour numérique (voir les ports) et t pour tcp.

Question 2 : Effectuer la demande.

Question 3 :

- Qu'elle est le numéro du port du serveur ? 21. Et ftp-DATA c'est 20.
- Quel est le protocole de transport utilisé par Telnet ? TCP.
- Donner la commande qui permet de vérifier que le serveur écoute sur ce port ? netstat -lnt | grep 21 -> grep 21 permet de filtrer celle ou le chiffre 21 est présent.

Question 4 :

A l'aide de Wireshark, il suffit d'utiliser le filtre FTP ou FTP-DATA (pour les données) et elles seront directement lisible sur Wireshark sans procédure particulière, cependant on peut suivre la même démarche que Telnet et on aura le résultat avec tout lisible.