Sécurité Informatique
2021

Matière :	*Niveau :*	*Examen :*
Sécurité Informatique	*2ème Année Licence*	*Session Normale S6*
Documents non autorisés	*Durée : 01h*	*Calculatrice scientifique autorisée.*

Exercice 1 : 8 pts (Chiffre par transposition)

*Considérons le chiffre par transposition sur l'alphabet latin de 26 lettres (de **A** à **Z**) comme l'illustre le tableau suivant. La taille de la clé = taille du bloc = 6.*

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a) Alphabet latin avec indices.

1	6	4	3	2	5
M	E	S	S	A	G
E	S	E	C	R	E
T	A	C	H	I	F
F	R	E	R	P	A
R	T	R	A	N	S
P	O	S	I	T	I
O	N				

(b) Matrice de transposition de l'exemple.

*Par exemple, en utilisant la clé **k** = 164325 et le message clair **M** =« MESSAGE SECRET A CHIFFRER PAR TRANSPOSITION », nous obtenant le cryptogramme **C** =« METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON » comme l'illustre la matrice en haut.*

1) *Combien de clés peuvent être composées de ce cryptosystème ?*
2) *Quel est le cryptogramme C correspondant au texte clair M = « MATHEMATIQUES ET INFORMATIQUE » et la clé k = « 356124 » ?*
3) *Quel est le texte clair M correspondant au cryptogramme C = « USCCLSETFEIESTCSEADEXCENA » et la clé k = « 356124 » ?*

Exercice 2 : 7 pts (Objectifs de sécurité)

Soit M un message clair, E un algorithme de chiffrement symétrique, k une clé secrète partagée entre Alice et Bob, H une fonction de hachage et $||$ l'opération de concaténation. Quels sont les objectifs de sécurité assurés dans chacun des scénarios suivants :

1) *Alice envoie à Bob : $M \,||\, H(M)$.*
2) *Alice envoie à Bob : $E_k(M)$.*
3) *Alice envoie à Bob : $E_k(M) \,||\, H(M)$.*

Exercice 2 : 5 pts (Questions de Cours)

1. Quelle est la différence entre un virus, un ver, et un espion ? (1 point)
2. Dressez-vous un tableau comparatif entre la cryptographie symétrique et la cryptographie asymétrique ? (2 points)
3. Citez trois algorithmes de chiffrement symétriques ? (1 point)
4. Citez trois algorithmes de chiffrement asymétriques ? (1 point)

NB : Justifier vos réponses et écrire de manière lisible

Corrigé Type de l'examen: Sécurité Informatique

Réponse à l'exercice 1

1. *La taille de l'espace de clés de ce cryptosystème est le nombre total de clés possibles. Puisqu'il s'agit de permutation de 6 éléments, la taille = 6 ! = 720.*
2. *Le texte clair M = «MATHEMATIQUES ET INFORMATIQUE» et la clé k = «356124» :*

3	5	6	1	2	4
M	A	T	H	E	M
A	T	I	Q	U	E
S	E	T	I	N	F
O	R	M	A	T	I
Q	U	E			

Le cryptogramme C =« HQIA EUNT MASOQ MEFI ATERU TITME ».

3. *Le cryptogramme C = « USCCLSETFEIESTCSEADEXCENA » et la clé k = « 356124 » ?*

Avant de procéder, il faut remarquer que la longueur du message clair est 25 et la taille de la clé est 6. Ainsi 25 = 6x4+1 et nous aurons 6 colonnes de 4 lettres et une colonne de 5 lettres (la première colonne).

3	5	6	1	2	4
F	A	C	U	L	T
E	D	E	S	S	C
I	E	N	C	E	S
E	X	A	C	T	E
S					

Le texte clair M = « FACULTE DES SCIENCES EXACTES »

Réponse à l'exercice 2

1. *Alice envoie à Bob :* $M||H(M)$. *Assurer l'intégrité uniquement.*
2. *Alice envoie à Bob :* $E_k(M)$. *Assurer la confidentialité uniquement.*
3. *Alice envoie à Bob :* $E_k(M)||H(M)$. *Assurer l'intégrité et la confidentialité.*

Réponse à l'exercice 3

Voir le cours.