Corrigé-type

Réponse à l'exercice 1

1. *La **confusion** correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible. La **diffusion** est une propriété où la redondance statistique dans un texte clair est dissipée dans les statistiques du texte chiffré.*

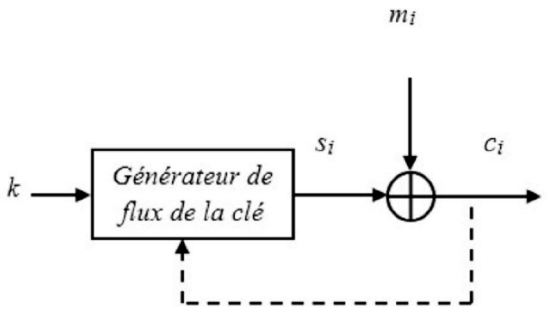
2. *Un système de chiffrement est dit **inconditionnellement sûr** si un attaquant est incapable de le casser même en disposant d'une capacité infinie de calcul. Le **masque jetable** est le seul exemple à ce jour.*

3. *Comparaison entre les systèmes symétriques et les systèmes asymétrique selon au moins 5 critères :*

	Systèmes symétriques	**Systèmes asymétriques**
Apparition	*Anciens (connus des égyptiens vers 2000 av. J.-C)*	*Récents (1976)*
Performances	*Rapides*	*Lents*
Nombre de clés *(n utilisateurs)*	*Grand (complexité polynomiale)* $\frac{n(n-1)}{2}$	*Petit (complexité linéaire)* $2n$
Principe de Sécurité	***Sécurité calculatoire** : (attaque par force brute avec les moyens (performances) actuels prend beaucoup de temps)*	***Sécurité réductionniste (ou sécurité prouvée)** : basée sur un problème mathématique réputé difficile qui donnent lieu à des fonctions à sens unique avec trappe (ou brèche secrète)*
Signature numérique	*Non appropriés*	*Appropriés*
Objectifs	*Confidentialité*	*Confidentialité, authentification, signature numérique et non répudiation*
Echange de clés	*Problématique*	*Très simple*

4. *Une substitution de polygrammes est une substitution qu'on opère sur des blocs (groupes) de caractères (ou lettres) au lieu d'opérer sur un seul caractère (une lettre).*

5. *Un chiffre par flux est un système symétrique et se présente souvent comme l'illustre le schéma suivant. Un générateur de nombres pseudo-aléatoires ayant comme **germe** la clé secrète K, produit une séquence binaire s_i à laquelle on mélange (souvent un XOR bit à bit) la séquence binaire du message clair m_i. Le résultat du mélange est une séquence binaire c_i qui représente le message chiffré. Si le flus de la clé s_i est indépendant de la sortie c_i, le système est qualifié de **synchrone**, sinon (un feedback de c_i) il est **asynchrone**.*



Système de chiffrement par flux.

Réponse à l'exercice 2

1. *La taille de l'espace de clés de ce cryptosystème est le nombre totale de clés possibles. Puisqu'il s'agit de permutation de 6 éléments, la taille = 6! = 720.*

2. *Dans une attaque par force brute avec texte clair connu, en moyenne il faut tester la moitié des clés possibles pour réussir (en supposant que les clés sont équiprobables). Ainsi il faut en moyenne tester* $\frac{720}{2} = 360$ *clés.*

3. *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 ».

4. *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 3

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.*