Corrigé type de l'examen sécurité informatique 2018

Exercice 1 (05 pts): Choisir la ou les bonnes réponses (1, 2 ou 3).

6. Les **logiciels** malveillants :

☐ Spam ☐ déni de service ☐ Maladresse. ■ Ver

7. Les services de sécurité assurés par Message Authentication Code (MAC).

☐ Confidentialité ■ Authentification de l'origine ☐ Non répudiation ■ Contrôle d'intégrité.

8. Les solutions **techniques** de protection :

☐ Formation des utilisateurs ■ Serveur proxy. ■ Pare-feu. ■ Antivirus.

9. Les risques sur les réseaux câblés.

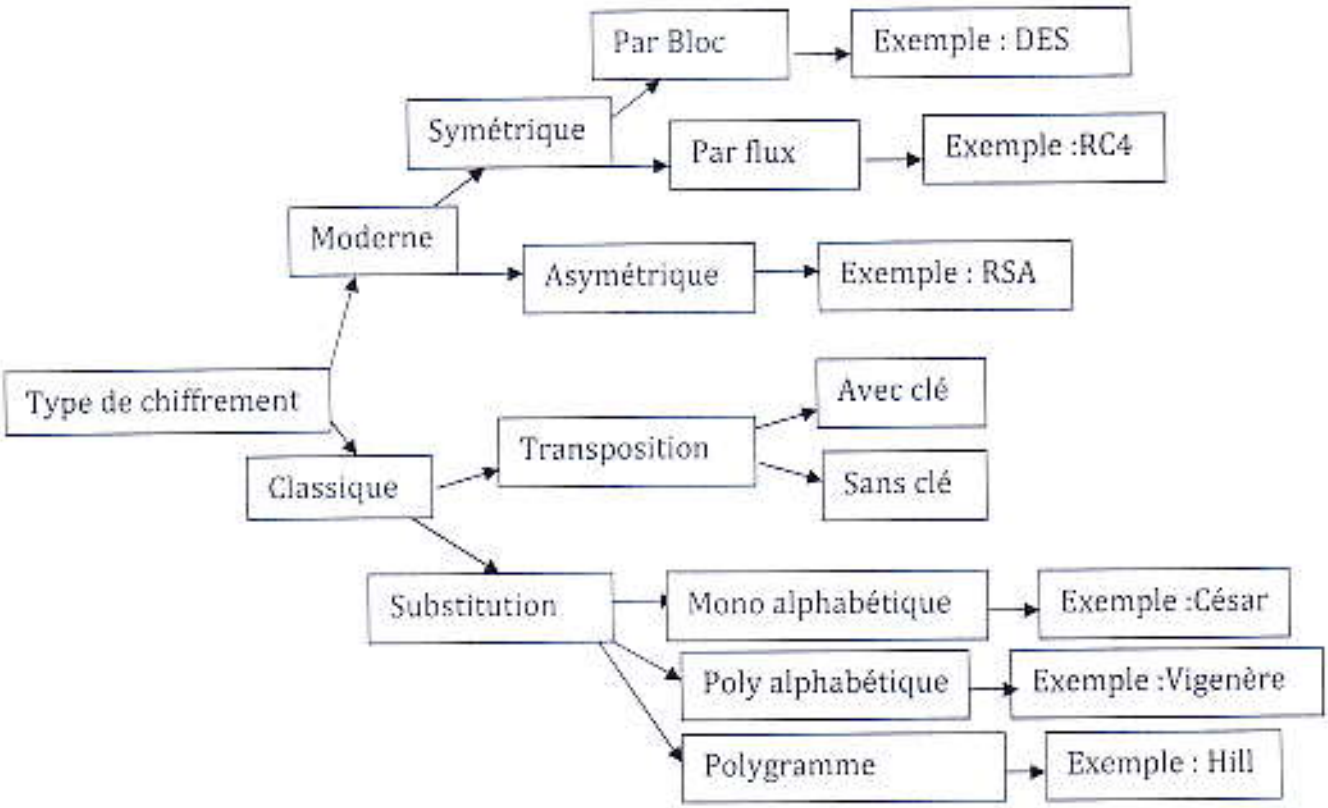
■ Déni de service ☐ Brouillage radio. ■ Usurpation d'identité. ☐ Hameçonnage.

10. Protocole de chiffrement

■ WEP ☐ 802.1X ☐ WPA ☐ VPN.

Exercice 2 (04 pts):

La **classification** des techniques de chiffrement:



Exercice 3 (03 pts):

Deux personnes A et B utilisent la cryptographie asymétrique. Chaque personne possède une paire de clés (clé secrète SK_i/ clé publique PK_i) avec $i \in \{A, B\}$.

1. B utilise la clé $\mathbf{SK_B}$ pour signer un message destiné à A. N'importe qui peut vérifier la signature du message en utilisant la clé $\mathbf{PK_B}$. Le service de sécurité assuré : la non répudiation.
2. B utilise la clé $\mathbf{PK_A}$ pour chiffrer le message ensuite, utilise la clé $\mathbf{SK_B}$ pour signer le message. A utilise $\mathbf{PK_B}$ pour vérifier la signature ensuite, il utilise $\mathbf{SK_A}$ pour déchiffrer et lire le message. Les services de sécurité assurés : Confidentialité et non répudiation.

Exercice 4 (03 + 3.5 + 1.5 = 08 pts):

1- Le protocole d'échange de clé Diffie-Hellman et obtenir la clé secrète **K** si les deux personne Ali et Bachir partagent p = 17 et g = 5, Ali choisit a = 6 et Bachir b = 15.

2- Déchiffrement du message suivant chiffré selon Hill avec $M = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix}$:

« EERZMHCPYJTO»

$\begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix} = M \begin{pmatrix} p_i \\ p_{i+1} \end{pmatrix}$ donc $\begin{pmatrix} p_i \\ p_{i+1} \end{pmatrix} = M^{-1} \begin{pmatrix} c_i \\ c_{i+1} \end{pmatrix}$

$M^{-1} = \frac{1}{|M|} \begin{pmatrix} 2 & -5 \\ -1 & 6 \end{pmatrix}$ où $|M| = (6 * 2) - (1 * 5) = 7$ donc $M^{-1} = \frac{1}{7} \begin{pmatrix} 2 & -5 \\ -1 & 6 \end{pmatrix}$

On a 7 et 26 premiers entre eux donc il existe deux entiers U et V tq 7U+ 26V = 1

Et $U = 7^{-1}$.

26 = 3*7+ 5

7= 1*5+2

5=2*2+ 1

1=5 – 2*2 = (26 – 3*7) – 2*(7 – 1*(26 – 3*7)) = 3*26 – 11*7.

Donc U = -11 mod 26 = 15. Alors $M^{-1} = 15 \begin{pmatrix} 2 & -5 \\ -1 & 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix}$

Déchiffrement

$$\begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \end{pmatrix} mod\ 26 = \begin{pmatrix} 2 \\ 14 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix}\begin{pmatrix} 17 \\ 25 \end{pmatrix} mod\ 26 = \begin{pmatrix} 13 \\ 19 \end{pmatrix}$$

$$\vdots$$

$$\begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix}\begin{pmatrix} 19 \\ 14 \end{pmatrix} mod\ 26 = \begin{pmatrix} 14 \\ 13 \end{pmatrix}$$

Texte clair « Contribution »

3- Déchiffrement le message suivant chiffré avec la technique de Transposition avec clé = plus. Message « OVSUV AZEAG NGXEX X».

l	p	s	u
O	V	S	U
V	A	Z	E
A	G	N	G
X	E	X	X

p	l	u	s
V	O	U	S
A	V	E	Z
G	A	G	N
E	X	X	X

Message clair : « VOUS AVEZ GAGNE».