Université Hassiba Benbouali Chlef
MI/Informatique - Master 1 IL
Examen Sécurité Informatique - 2015

Note : Toute réponse doit être justifiée et argumentée de façon claire.

Exercice___01[4pts]:
SI : Quelle **condition** doit avoir une **solution de sécurité** pour un objet X à protéger ?
CF : Quelle est la taille de la clé d'un **cryptage par flux**?
CB : Quelles sont les différences entre **DES et AES**?
CA : Quel **objectif de sécurité** qui n'est pas réalisé par **RSA**?
AP : Protocole **Diffie-Hellman** résout quel problème en utilisant quel **mécanisme**?

Exercice___02[17pts]:
A- Hill Cipher (4)
Soit **K** une matrice de dimension 2 dans $\mathbf{Z_n}$, On définit une fonction **f** sur $\mathbf{(Z_n)^2}$

f : $(Z_n)^2$ ----------> **$(Z_n)^2$** `K = [a b], C=(x,y)`
M=(m,n) ----------> **f(M)= K.M[n] = C** `[c d]`

2.1- Dans quel cas **f** accepte une **fonction inverse f^{-1}**?
Avec **(f, f^{-1}, K)** on définit un **crypto-system sur $(Z_n)^2$** dont la **clé** est la matrice **K**
2.2- Quelle est les **caractéristiques** de ce crypto-system (sa classe) ?
2.3- En donnant K : **a=3, b=2, c=3 et d=5**, **décrypter C = (24,16)**.

B- Cryptographie moderne (8)
2.4- **4 cases-LFSR** dont la première et la dernière exorées et attachée à l'entrée. Pour une séquence d'initialisation **0001**, donnez sa **table d'état** (jusqu'à sa récurrence).

On dit qu'une fonction f **involutive** ssi **f(f(x))=x**.
On dit que la **clé K de DES** est **faible** si **DES** avec cette clé **K** est **involutive**.
2.5- Décrire la **relation** entre les **sous clés** pour un **DES involutive**?
2.6- Il y a **4 clés faibles** lesquelles?

2.7- RSA soit PK(55,7), encrypter M=10, casser ce crypto système en trouvant sa clé VP. Décrypter C=35.

D-Application (4)
Une solution de Vote électronique (e-Vote qui remplace **vote à bulletin secret classique**) doit offrir quels **services de sécurité**?
On va simuler de façon électronique un **vote sans anonymat** ou on peut savoir qui a voté quoi (lever de main lors d'une réunion). Un ensemble de **clients (électeur**) connectés au **serveur (centre d'élection**) qui vont remplir le bulletin **e-vote**.
2.8- Proposer une **solution de sécurité** (en utilisant un schéma) pour cette situation en justifiant comment va éviter les **fraudes électorales**.

- Bonne Chance –

Université Hassiba Benbouali Chlef
MI/Informatique - Master 1 IL
Solution de l'examen Sécurité Informatique - 2015

Exercice___01[4pts]:
SI : La **solution de sécurité** doit avoir un **cout inferieur** à la **valeur** de l'objet X.
CF : La taille de la clé d'un **cryptage par flux** est **infinie**.
CB : **DES**[**Symétrique**, **16** Rounds, Clé **56bits**] **AES**[**Asymétrique**, **10/12/14** Rounds , Clé **128/192/256b**its]
CA : L'**objectif de sécurité** qui n'est pas réalisé par **RSA** est la **disponibilité**.
AP : Protocole **Diffie-Hellman** résout le problème de l'**échange des clés** en utilisant un cryptage **asymétrique** pour **échanger les clés symétrique**.

Exercice___02[17pts]:
A- Hill Cipher (4)
Soit **K** une matrice de dimension 2 dans $\mathbf{Z_n}$, On définit une fonction **f** sur $\mathbf{(Z_n)^2}$

f : $(Z_n)^2$ ----------> $(Z_n)^2$ `K = [a b], C=(x,y)`
M=(m,n) ----------> f(M)= K.M[n] = C `[c d]`

2.1- **f** accepte une **fonction inverse f^{-1}**, Si la matrice inverse de K existe (K^{-1}) det(K) !=0 .
Avec **(f, f^{-1}, K)** on définit un **crypto-system sur $(Z_n)^2$** dont la **clé** est la matrice **K**
2.2- les **caractéristiques** de ce crypto-system Symétrique, Bloc, $E_K=f$, $D_K=f^{-1}$
2.3- En donnant K : **a=3, b=2, c=3 et d=5 => $K.K^{-1} = I$,I matrice d'identité**
3*a'+2*b'=1 et 3*a'+2*b'=1 => a' = 15, b'=20, c'=17, d'=9 //résolution système 2 équations.
3*a'+5*b'=0 et 3*a'+2*b'=1,
Décrypter C = (24,16). => x = (15*24+20*16)[26] = 4 et y = (17*24+9*16)[26] = 6, **M=(4,6)**

B- Cryptographie moderne (8)
2.4- **4 cases-LFSR** dont la première et la dernière exorées et attachée à l'entrée. Pour une séquence d'initialisation **0001**, donnez sa **table d'état** (jusqu'à sa récurrence).

->-[0|0|0|1]->	1	2	3	4	5	6	7	8	9	10	11
+-|-------|	0001	1000	1100	1110	1111	0111	1011	0101	1010	1101	0110

On dit qu'une fonction f **involutive** ssi **f(f(x))=x**.
On dit que la **clé K de DES** est **faible** si **DES** avec cette clé **K** est **involutive**.
2.5- La **relation** entre les **sous clés** pour un **DES involutive**
Puisque DES involutive donc $DES_K(DES_K(x)) = x$ => $DES_K(x) = DES^{-1}_K(x)$ (cryptage = décryptage)
Puisque le décryptage utilise les sous clés dans l'ordre inverse (K16..K1) alors $K_i=K_{17-i}$ i :1..16
$K_8=K_9$ et K_9 = rotation(K_8)=K_8 donc la rotation doit ne pas avoir d'effet => ss-clés sont **égaux**.
2.6- **4 clés faibles** dont la rotation n'a pas d'effet = >**$1\text{-}0^{28}\text{-}0^{28}$, $2\text{-}0^{28}\text{-}1^{28}$, $3\text{-}1^{28}\text{-}0^{28}$, $4\text{-}1^{28}\text{-}1^{28}$**

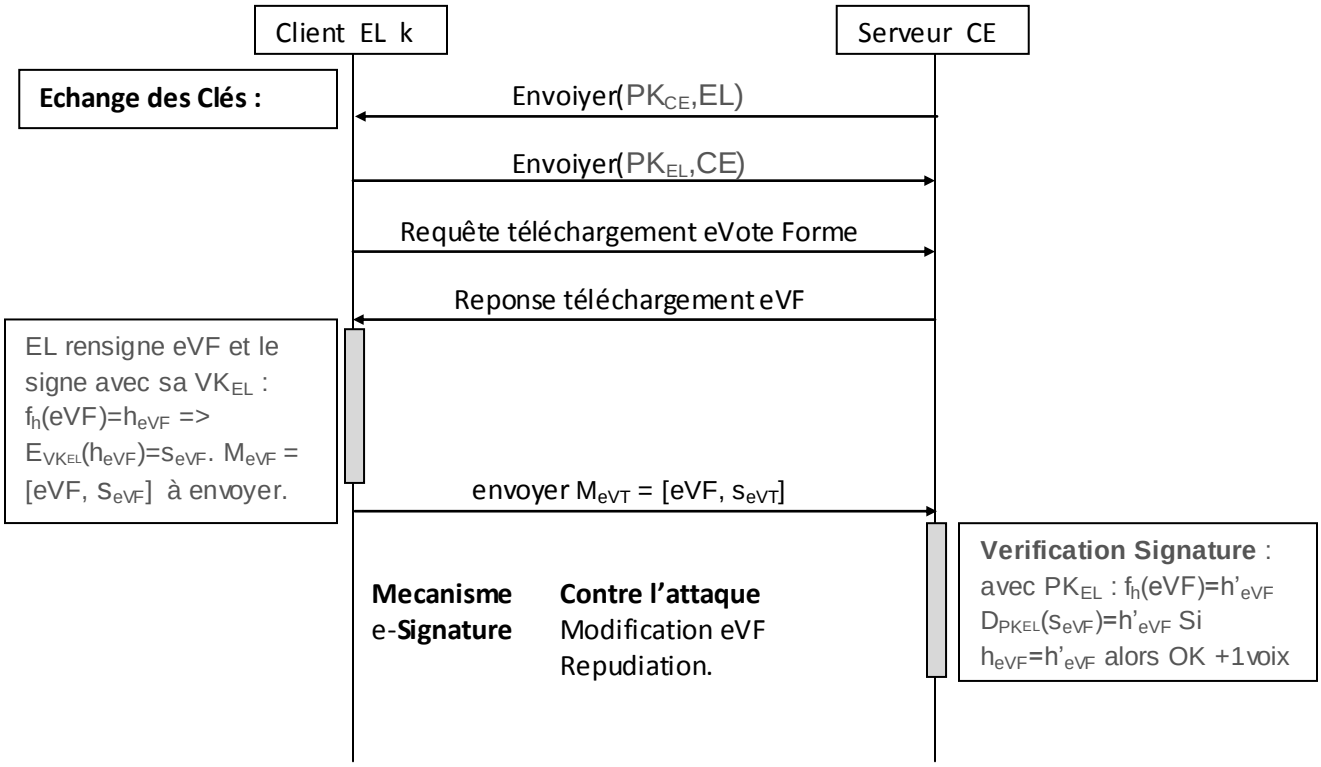
2.7- RSA soit PK(55,7),
- Crypter M=10, $E_{PK}(M)=M^e[n]=10^7[55]=\mathbf{10}$, $[10^2[55]=45=-10$ => $10^4[55]=-10$ => $10^6[55]=-10$
- Casser ce crypto système : comme **55=11*5 unique factorisation** donc => **p=11 et q=5** alors **phi(n)=(p-1)*(q-1)=10*4=40**
d.e=1[phi]=d.7[40]=1 =>d=23 (décimal donnant 1 avec 7 c'est 3 essayer 13, 23 ok) **VK(55,23)**
Décrypter C=35, $D_K(C)=C^d[n]=35^{23}[55]= 35^5*35^5* 35^5* 35^5* 35^3 [55] = 10^4*10*3[55]=$ **30**.
$35^5=10[55]$ et $35^3=30[55]$

D-Application (4)

Une solution de Vote électronique (e-Vote qui remplace **vote à bulletin secret classique**) les **services de sécurité** : Confidentialité et Intégrité

2.8- Une **solution de sécurité (intégrité)**. e-Vote Forme disponible sur le site de CE publiquement.

Génération des clés : AC génère et distribue les clés (PK_{EL}, VK_{EL}) et (PK_{CE}, VK_{CE}).



- Bonne Chance -