Université de khenchela

Faculté des sciences et Technologies L3 ISIL

Examen semestriel : Sécurité informatique (Corrigé type)

Durée de l'examen :1H30 Date : 21/05/2022

Enseignant : Dr. Hichem RAHAB

1 Solution (10 points)

1. Le chiffrement symétrique :

   A - **Garantie la confidentialité du message chiffré**
   B - Utilise une paire de clés publique/privée,
   C - Assure la non répudiation,
   D - **Repose sur la confidentialité de la clé utilisée**
   E - Repose sur la confidentialité de l'algorithme de chiffrement utilisée

2. Le chiffrement Asymétrique :

   A - Garantie l'intégrité du message chiffré
   B - **Utilise une paire de clés publique/privée**
   C - **Peut Assurer la non répudiation**
   D - Repose sur la confidentialité de la clé utilisée
   E - Repose sur la confidentialité de l'algorithme de chiffrement utilisée

3. L'algorithme RSA

   A - Est un système cryptographique symétrique
   B - **Repose sur la difficulté de factoriser un grand nombre en ses facteurs premiers**
   C - Repose sur la difficulté du logarithme discret
   D - **Permet de faire une signature digitale,**
   E - Ne peut pas être utilisé pour assurer la confidentialité

4. Pour garantir la non-répudiation de l'origine, on peut utiliser

   A - Un chiffrement RSA avec la clef publique de l'émetteur
   B - **Un chiffrement RSA avec la clé privée de l'émetteur**
   C - Un MAC
   D - **Une signature digitale**
   E - Un échange de clé Diffie-Hellman

5. DES est :

   A - Est un système cryptographique asymétrique
   B - **Est un système cryptographique à clé secrète**
   C - Un système qui utilise une clé sur 56 bits
   D - Permet de faire une signature digitale
   E - **Permet d'assurer la confidentialité des messages transmis.**

2 Solution (06 points)

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 = «LINFORMATIQUE POUR TOUS» et la clé k = «356124» : Le cryptogramme C =« FIU OQR LMEO RUT IAPU NTOS».

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

3. **Remarque :** Il y a une erreur dans cette partie donc la partie 3 sera annulée.

Le cryptogramme C = « YAASI RLCGE AIAEL THTON CPPRP OIERR PPN TT L AOIRS MI » et la clé k = « 362514 » ?

Avant de procéder, il faut remarquer que la longueur du message clair est 25 et la taille de la clé est 6. Ainsi $42 = 6 \times 7$ et nous aurons 6 colonnes de 7 lettres .

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

Le texte clair M = « LA CRYPTOGRAPHIE PAR TRANSPOSITION MATRICIELLE »

3 Solution (04 points)

Un groupe de N personnes souhaite s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres ne doivent pas pouvoir être lues par les autres.

1. Dans le cas où le groupe choisisse un système de chiffrement symétrique, quel est le nombre minimal de clefs nécessaires ? N*(N-1)/2

2. Quel-est le nombre minimal de clefs nécessaires dans le cas où le groupe choisisse un système de chiffrement asymétrique ? 2*N

3. Quelles clés Ahmed et Souhayla doivent-ils utiliser dans chaque cas :

   A - Ahmed veut envoyé des informations confidentielles à Souhayla. Clé publique de Souhayla

   B - Souhayla souhaite vérifier l'authentification d'un message reçu de Ahmed.Clé publique de Ahmed

   C - Ahmed souhaite envoyer des informations chiffrées et signées à Souhayla. Pour le chiffrement : Ahmed utilise la clé publique de Souhayla. Pour la signature : Ahmed utilise sa clé privée

---

Good Luck