Université de Jijel
Faculté des Sciences et de la Technologie
Département d'Electronique
3ième Année LMD – Télécommunication

Devoir à faire

SECURITE DE L'INFORMATION

Exercice 1

I. Deux partenaires (A) et (B) communiquent entre eux en utilisant l'algorithme ELGAMAL.
Sachant qu'ils utilisent les clefs suivantes : p=77, a=5, s=8 et k=9.

1. **A quel type appartient cet algorithme. ?**
2. **Quelle est la difficulté sur laquelle repose cet algorithme. ?**
3. **Donner son algorithme de fonctionnement en indiquant l'émetteur et le récepteur.**
4. **Indiquer la clef secrète et la clef publique de cette communication.**
5. **Quelle est la clef partagée entre A et B.**
6. **Donner trois types d'attaques pour cet algorithme**
7. **Si le message (M) à transmettre est M=7.**
   Montrer comment les partenaires (A) et (B) utilisent cet algorithme.

II. Si les partenaires (A) et (B) décident de changer l'algorithme d'ELGAMAL par RSA : Et si les clefs utilisées sont : p=7, q=11 et e=7.

1. **Montrer que d = 7^{-1} mod 60 = 43.**
2. **Donner son algorithme en indiquant l'émetteur et le récepteur.**
3. **Indiquer la clef secrète et la clef publique de cette communication.**
4. **Montrer comment (A) et (B) utilisent cet algorithme, avec dans ce cas M = 5.**

Exercice 2

1. **Quelle est la différence entre un virus, un ver, et un spyware ?**
2. **Qu'est-ce que c'est la machine Enigma ?**
3. **Citer les trois éléments de la trinité CIA.**
4. **En cryptographie moderne, la confidentialité repose sur : choisir une réponse parmi les 3 suivantes :**
   a. Le secret de l'algorithme de cryptage,
   ~~b.~~ Le secret de l'algorithme de décryptage,
   c. Le secret d'une clef partagée.
5. **Citez deux algorithmes de chiffrement symétriques ? quelle est l'algorithme le plus utilisé actuellement ?**
6. **Citez deux algorithmes de chiffrement asymétriques ? quelle est l'algorithme le plus utilisé actuellement?**
7. A quoi sert le protocole de Diffie-Hellman?

Exercice 3

1. Quel est le principe de fonctionnement d'un pare-feu ?
2. Citer les avantages et les inconvénients de l'utilisation d'un pare-feu
3. Justifiez votre réponse par le cas de Windows