Université de khenchela

Faculté des sciences et Technologies L3 ISIL

Examen semestriel : Sécurité informatique (Corrigé type)

Durée de l'examen :1 H 30 Date : 13/05/2024

---

1 Solution (4 points)

Système	Attaquant	Dommages	Confidentialité	Intégrité	Disponibilité
A	Intrus	Blockage du site	bas	bas	bas
B	Pirate, concurrent	vol d'argent	moyen	haut	haut
C	Concurrent	Falsification	Haut	Haut	Moyen
D	Concurrent, pirate	blockage et nuisance	Haut	Haut	Haut

2 Solution (8 points)

1. Dans le cas où vous optez pour un système de chiffrement **symétrique**.

   A - Le nombre minimal de clefs nécessaires est : $\frac{N(N-1)}{2} = \frac{50\times49}{2} = 1225$ clés.

   B - Les avantages : Rapidité de transmission, simplicité d'implémentation.

   C - Les limites : Nombre de clés à générés et gérés, et problème d'échange de clés.

2. Dans le cas où l'entreprise choisisse un système de chiffrement **asymétrique**

   A - Le nombre minimal de clefs nécessaires : $N \times 2 = 50 \times 2 = 100$ clés

   B - Les avantages : Nombre de clés limités, Assure plusieurs fonctions (signature numérique, intégrité, ...)

   C - Les limites : Opération très lente (demande beaucoup de calculs), difficulté d'implémentation .

3. Quelles mécanisme de sécurité doit être utilisé dans chaque cas : (Chiffrement symétrique, Chiffrement asymétrique, clé publique de ..., clé secrète de ...)

   A - A veut échanger une grande quantité de données pour une langue période avec B.–> Chiffrement symétrique.

   B - A veut envoyer son clé symétrique à B .–> Clé publique de B.

   C - A veut envoyer des données confidentielles à B –>Clés publique de B ou bien Chiffrement symétrique.

   D - Le directeur veut envoyé des instructions signé à tous le employés. –> Clé privé du directeur.

3 Solution (8 points)

A - Cas d'attaque par force brute.

(a) Il y a $26^5 = 11.881.376$ clés possibles, En moyenne il essaye : $\frac{11.881.376}{2} = 5.940.688$ clés.

(b) Le temps moyen pour trouver la bonne clé est : $\frac{5.940.688}{3.600\times24} = 68.75$ Jours. soit : Deux mois et 8 Jours.

(c) Pour lutter contre la cryptanalyse par force brute, je propose :

i. Augmenter la taille de la clé.

ii. Changer fréquemment la clé.

(d) La période conseillée de changer la clé dans ce cas est de : Deux mois.

B - Le texte claire : "PALASTINEWILLBEFREEFROMTHERIVERTOTHESEAINTHISDECADE".

En éliminant mettant les espaces :"PALASTINE WILL BE FREE FROM THE RIVER TO THE SEA IN THIS DECADE".

Good Luck