Université d'Oum El Bouaghi

Département des Mathématiques et d'Informatique

Niveau : 03ème Licence SI + ISIL — Mardi 14 Mai 2024

Remarque : *Les réponses doivent être brèves, claires et concises* — **Durée**: 1h30'

Matière : Sécurité Informatique

Questions

1) Quel est l'attribut de la sécurité informatique le plus important? Justifiez. — 02 Pts

Il n'y a pas un attribut plus important parmi les attributs de la sécurité informatique, parce que le choix est étroitement lié au contexte et au domaine d'application. Par exemple, si la confidentialité est considérée importante dans certains cas, l'intégrité sera plus importante dans d'autres situations.

2) Dans la technique de cryptage DES, quelle est la taille de la clé? et combien de clés valides existent? — 03 Pts

La taille de la clé est 64 bits dont 8 bits sont des bits de contrôle; donc la taille de la clé est 56 bits.

Le nombre de clés valides est 2^{56} clés

3) Que signifie l'utilisation des infrastructures spontanées ? — 02 pts

Une infrastructure spontanée fait référence à des ressources ou d'éléments qui se forment naturellement ou qui sont mis en place de manière informelle, sans supervision ni autorisation appropriée.

4) Expliquer les principes suivants de la sécurité informatique: la sécurité par obscurité, la défense en profondeur, le principe de maillon faible?

- *La sécurité par obscurité (Security through Obscurity) consiste à cacher les détails de la conception ou de l'implémentation d'un système de sécurité dans l'espoir que l'attaquant ne puisse pas découvrir ou exploiter les vulnérabilités si elles ne sont pas bien connues.* — 01 Pts
- *La défense en profondeur (Defense in Depth) est une stratégie de sécurité qui implémente plusieurs couches de protection pour sécuriser les systèmes et les données..* — 01Pts

- *Le principe du maillon faible (Weakest Link Principle) stipule que la sécurité d'un système est déterminée par son maillon le plus faible. En d'autres termes, le système est aussi sécurisé que son élément le moins sécurisé.*

01 Pts

Exercice 01

Considérons un système utilisant le code ASCII (sur 7 bits) pour représenter les caractères, et supposons que nous souhaitons crypter un message en utilisant la technique de chiffrement affine.

1. Quelle est la condition de la clé dans cette technique de chiffrement ?

La condition de la clé dans la technique de chiffrement affine est que la clé doit être une paire d'entiers (a, b), où a et n sont des nombres entiers premiers entre eux, sachant que n est le nombre de caractères.

01

2. Parmi les clés suivantes (7, 4); (4, 7); (13, 8), quelles sont les clés valides ? justifiez.

(7, 4) et (13, 8) sont des clés valides parce que (7 et 128) et (13 et 128) sont des nombres premiers entre eux. 128 est le nombre de caractères dans le code ASCII ($2^7 = 128$).

02

(4, 7) n'est pas une clé valide parce que 128 et 4 ne sont pas premiers entre eux.

3. Est-ce que la technique affine est inconditionnellement sûre ? Est-elle invulnérable par le calcul ? Justifiez dans chaque cas.

La technique affine n'est pas inconditionnellement sûre, car elle peut être vulnérable aux attaques de force brute si la taille de l'alphabet est petite. Dans le cas du code ASCII sur 7 bits, avec seulement 128 caractères possibles, une attaque par force brute devient réalisable.

01

En ce qui concerne l'invulnérabilité par le calcul, la technique affine peut être vulnérable aux attaques cryptanalytiques si la clé est faible ou si le message est trop court pour contenir suffisamment de variabilité.

01

Exercice 02

On veut utiliser la technique de cryptage asymétrique RSA.

1. Quelles sont les avantages de techniques asymétriques par rapport aux techniques de cryptage symétriques?

Dans les techniques de cryptage asymétriques, il n'est pas nécessaire de partager secrètement une clé de cryptage, car chaque partie possède sa propre paire de clés publique/privée.

01 Pts

2. Calculer la clé privée et la clé publique, en utilisant P=29, Q=31, e=17.

N =P * Q = 29 * 31 = 899.

0.5

$\phi(N) = (P-1) * (Q - 1) = 840$

0.5

e = 17

on calcule d, inverse de 17 mod 840

$\phi(N)$	e	R	Q	T0	T	Temp = (T0 -T*Q)mod $\phi(N)$
840	17	7	49	0	1	(-49) mod840 = 791
17	7	3	2	1	791	(1-791*2) mod 840 = 99
7	3	1	2	791	99	(791-99*2)mod 840 = 593
3	1	0	3	99	593	

01

d = 593 ;

La clé publique (n, e) = (899, 17)

0.5

La clé privée (n, d) = (899, 593)

0.5

3. Est-il possible de déduire la clé privée à partir de la clé publique?

Il est impossible de déduire la clé privée à partir de la clé publique dans le système RSA, à condition que les nombres premiers P et Q soient suffisamment grands et choisis aléatoirement. La sécurité du RSA repose sur la difficulté de factoriser le produit de deux grands nombres premiers (P et Q) pour retrouver la clé privée.

01

Bon courage !

Dr. Toufik MARIR