Examen OS01 : Crypto, sécurité, réseaux

Durée : 2h
Documents : pas de document

Question I : Vigenère (6 points)

1. Expliquez le fonctionnement du chiffré de Vigenère. Précisez quel type de schéma cryptographique il représente (par exemple un schéma de MAC, une fonction de hachage, etc.), comment on chiffre et comment on déchiffre avec cette méthode. (1.5 points)
2. Etant donne la clé VIGENERE et le texte clair JEMAMUSEAVECCECHIFFRE calculez le chiffré Vigenère de ce texte clair avec la clé donnée. (1 point)
3. La méthode de Kasiski a pour but de trouver la taille de la clé utilisée pour générer un chiffré Vigenère. Elle prend en entrée un chiffré Vigenère et donne comme sortie une taille possible pour la clé. Le premier pas c'est de regarder des répétitions de lettres dans le chiffré (séquences de 2 ou plus lettres consécutives qui apparaissent plusieurs fois dans le chiffré). Puis il faut classifier les répétitions, de la plus longue en termes du nombre de caractères qui se répètent, à la plus petite. Puis, pour chaque répétition il faut compter la distance entre les deux fragments qui se répètent. Finalement, la taille de la clé est estimée comme un diviseur commun de la distance entre les fragments répétés le plus longues.
    - Expliquez pourquoi cette méthode marche-t-elle (2 points)
    - Quelles sont les conditions (en termes du chiffré, de la clé, du texte clair) qui vont optimiser la probabilité de trouver la bonne clé en utilisant cette méthode ? (1.5 points)

Question II : OTP + fonctions de hachage (6 points)

1. Le chiffrement à masque unique (One-time pad) est une méthode de chiffrement symétrique. Pour un texte clair donné m (représenté comme une chaine de bits), il faut choisir une clé k, qui est une chaine de bits aléatoirement choisis, de taille égale à m. Pour chiffrer, il faut appliquer l'opération XOR entre le message et la clé. Pour déchiffrer, il faut faire le XOR du chiffré avec la clé.
    - Quelle est la taille du chiffré obtenu ? (0.5 points)
    - Est-ce que cette méthode de chiffrement est sécurisée ? (0.5 points)
    - Quels sont les inconvénients de cette méthode de chiffrement ? (1 point)

2. Listez et expliquez les trois propriétés les plus importantes d'une fonction de hachage cryptographique (1 point).
3. Etant donnée une fonction de hachage cryptographique H_1 qui garantit les trois propriétés citées au point numéro 2, et une fonction de hachage H_2 qui ne garantit aucune de ces propriétés, et

étant donné que les deux fonctions de hachage ont la même taille de sortie, qu'est-ce que vous pouvez dire sur les propriétés de la fonction de hachage H qui a la même taille de sortie que H_1, H_2 et est définie par : $H(x) \coloneqq H_1(x)\ XOR\ H_2(x)$ pour toute valeur de x ? Expliquez vos réponses (3 points)

Question III : Le chiffrement ElGamal (4 points)

Le chiffrement ElGamal date de 1985. Il a été inventé par Taher ElGamal et représente un des algorithmes de chiffrement à clé publique les plus bien-connus aujourd'hui. Cette méthode de chiffrement a trois étapes principales. Dans un premier temps, les participants génèrent des clés dans un groupe cyclique G généré par un élément g d'ordre premier q. Les opérations se feront modulo un autre premier p, qui est également public.

Pour la génération de clés, chaque participant génère une clé privée x choisie aléatoirement entre 1 et $q-1$. La clé publique sera g^x.

Ensuite, pour chiffrer un message *m* (qui doit être un élément du groupe *G*) avec une clé publique g^x, un utilisateur devra choisir une valeur temporaire r et calculera la valeur $c_1 = g^r\ mod\ p$. Puis on calcule $c_2 = m \cdot (g^x)^r \bmod p$. Le chiffré envoyé est égale à c_1, c_2, c'est-à-dire, la concaténation de ces deux valeurs.

Pour déchiffrer avec la clé privée x on calcule $m = \frac{c_2}{(c_1)^x}$.

1. Vérifiez que le déchiffrement donne bien la valeur de m qui a été chiffrée (0.5 points).
2. Qu'est-ce que garantit la sécurité des clés secrètes ? (1 point)
3. Regardez c_2. Quelle valeur doivent-on pouvoir calculer pour pouvoir déchiffrer le message m à partir de cet élément du chiffré ? Qui peut calculer cet élément ? (1 point)
4. Qu'est-ce que nous garantit la sécurité de cette méthode de chiffrement ? (1.5 points)

Question IV : Les protocoles d'échange de clé (4 points)

1. Quel est le rôle d'un protocole d'échange de clé authentifié ? (0.5 points)
2. Soient deux amis Alice et Bob qui ont chacun une paire de clés de chiffrement RSA certifiées par une autorité de certification. Alice et Bob veulent exécuter le protocole d'échange de clé suivant :

Alice (sk_A, pk_A)		Bob (sk_B, pk_B)
Calcule $K \leftarrow \mathrm{HMAC}(pms; pk_A, pk_B)$	$\xleftarrow{Enc(pk_A; pms)}$	Choisit $pms \xleftarrow{\$} \{0,1\}^{128}$ Calcule $K \leftarrow \mathrm{HMAC}(pms; pk_A, pk_B)$

Est-ce que ce protocole est sécurisé contre un attaquant passif ? Expliquez votre réponse (0.75 points)

3. Quels éléments d'authentification inclue ce protocole ? Qui s'authentifie auprès de qui ? (0.75 points)
4. Comment un attaquant actif peut-il usurper l'identité de Bob ? (1 point)
5. Essayez de réparer le protocole par rapport à votre attaque. (1 point)