IN603: Cryptographie - Examen Final

Enseignante: Christina Boura

15 mai 2017

Durée du contrôle : 2h.

Les calculatrices, ordinateurs, téléphones portables, smartphones ne sont pas autorisés. Seule une feuille A4 recto/verso manuscrite est permise.

Justifier toutes les réponses et détailler tous les calculs effectués.
Bonne chance !

Questions

1. En cryptographie symétrique, les deux grandes familles de chiffrement sont le chiffrement à flot et le chiffrement par bloc. Expliquer l'idée de fonctionnement derrière chacune de ces deux familles. Comment fait-on pour traiter des messages de grande taille dans chacun des deux cas ?
2. Expliquer pourquoi l'utilisation d'un seul LFSR pour le chiffrement à flot, ne suffit pas pour garantir la sécurité.
3. Expliquer pourquoi l'utilisation d'un algorithme symétrique pour créer des signatures numériques ne garantit pas la non-répudiation.
4. Dans le cas des signatures numériques, l'intégrité est-elle assurée ? Est-ce pareil pour les signatures manuscrites ? Expliquer votre réponse dans les deux cas.
5. Sur quel problème difficile est basé le protocole d'échange de clés Diffie-Hellman ? Justifier votre réponse.

(5 points)

RSA Alice et Bob souhaitent utiliser le cryptosystème RSA pour communiquer. Alice choisit $p = 7$ et $q = 11$ comme nombres premiers. Son module RSA est alors $n_A = p \cdot q = 77$. Elle choisit $e_A = 7$ comme exposant publique. Sa clé publique est alors $(n_A, e_A) = (77, 7)$.

1. Montrer que $e_A = 7$ est un choix valide.
2. Calculer la clé privée d_A d'Alice en utilisant le théorème d'Euclide étendu.
3. Bob veut envoyer le message $m = 75$ à Alice. Calculer le chiffré correspondant.
4. Alice veut signer le message $m = 17$. Alice envoie $(m, s) = (17, 73)$ à Bob, où $s = 73$ est la signature supposée correspondre au message. Expliquer comment Bob vérifie la signature. Est-ce Alice le vrai auteur du message ?
5. Expliquer pourquoi on dit que la sécurité du système RSA est basée sur le problème de la factorisation.
6. Alice et Bob souhaitent utiliser RSA afin de se mettre d'accord sur un secret partagé K_{AB} qu'ils utiliseront comme clé d'un chiffrement symétrique pour pouvoir échanger des messages rapidement. Expliquer le déroulement de ce protocole.
7. On suppose qu'Oscar réussit à faire une attaque de l'homme du milieu. Si on note (n_B, e_B) la clé publique de Bob, et d_B sa clé privée, et (n_O, e_O) la clé publique d'Oscar et d_O sa clé privée, expliquer en détail comment marche cette attaque et montrer comment sont calculées les clés secrètes établies par Alice, Bob et Oscar à la fin.
8. Expliquer en un paragraphe comment l'utilisation des certificats numériques permet de se protéger contre l'attaque de l'homme du milieu.

(9 points)

Une extension du DES

1. Qu'elle est la taille de clé (en bits) du DES ? Cette taille est-elle suffisante ? Expliquer.
2. Nous considérons ici une variante de l'algorithme DES, qu'on appellera DESA :

$$\mathrm{DESA}_{k_1,k_2}(m) = \mathrm{DES}_{k_1}(m) \oplus k_2.$$

Le chiffrement d'un bloc de message m avec cet algorithme consiste à appliquer l'algorithme DES sur m avec une clé k_1 de 56 bits et calculer ensuite l'OU exclusif ($\oplus$) du résultat avec une clé k_2 de 64 bits.

(a) Dans une première approche, quelle est la complexité d'une recherche exhaustive de la clé de DESA ?

(b) Montrer qu'il existe une attaque utilisant deux couples clairs-chiffrés connus contre DESA qui demande 2^{57} evaluations de la fonction de DES (c.-à-.d DESA ne ralentit la recherche exhaustive que d'un facteur de 2). Donner un algorithme précis de cette attaque permettant de retrouver les clés k_1 et k_2.

(4 points)

Théorème des restes chinois Un restaurant spécialisé dans les grandes réceptions possède deux types de tables : des tables de 7 personnes et des tables de 15. Ce soir, une grande soirée d'entreprise aura lieu dans ce restaurant. Si on n'utilise que des tables de 7, après avoir rempli le plus de tables possibles, il restera 4 personnes débout. Si on n'utilise que des tables de 15, après avoir rempli le plus de tables possibles, il restera cette fois-ci 3 personnes débout.

Sachant que le nombre de personnes participants à la soirée est entre 210 et 315, déduire le nombre exact de personnes présents dans la soirée.

(2.5 points)

Attention ! Pour tous les exercices, tous les calculs faits doivent figurer sur la copie finale rendue.