Master – 1$^{\text{ère}}$ année – Informatique / MINT

Cryptographie – Examen

15 janvier 2019

Durée : 2h – Tous documents interdits – Aucun accès à un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Questions de cours

1. **DES**

   Expliquer pourquoi on utilise le triple DES. En particulier, quelles sont les raisons pour lesquelles on ne se contente pas du double DES. Expliquer en détails.

2. **Le mode de chiffrement CBC**

   Dans cette question, on considère un algorithme de chiffrement par blocs noté E, avec une clé notée K. On suppose que $E_K : \{0,1\}^n \mapsto \{0,1\}^n$, avec $K \in \{0,1\}^k$. En d'autres termes, $E_K(t)$ désigne le chiffré du message t de longueur n, selon la clé K de k bits.

   (a) Faire le schéma du mode de chiffrement CBC.

   (b) Pour un message clair de la forme $x = x_1||x_2||\ldots||x_\ell$, où pour chaque i, $x_i \in \{0,1\}^n$, donner les formules qui expriment le message chiffré y en fonction du message clair.

   (c) Expliquer comment on déchiffre le message chiffré y.

   (d) Expliquer le rôle de la "valeur initiale" IV.

3. **Fonctions de hachage**

   (a) Que dit le paradoxe des anniversaires ? (donner une réponse la plus précise possible, avec si possible une formule)

   (b) Quelle condition nécessaire donne-t-il sur la valeur de n pour qu'une fonction $f : \{0,1\}^* \longrightarrow \{0,1\}^n$ soit à collisions fortes difficiles ?

Exercice 1 (*Une attaque sur le mode CBC*)
Une fonction de chiffrement sur des blocs de n bits $E : (K, x) \mapsto y = E(K, x)$ est utilisée en mode CBC pour chiffrer un message $m = (m_1, \ldots, m_t)$. On obtient un cryptogramme $c = (IV, c_1, \ldots, c_t)$, où IV est le vecteur d'initialisation.

1. Montrer que si deux blocs du cryptogramme, c_i et c_j sont identiques, avec $1 \leq i < j \leq t$, alors on dispose d'une information sur les blocs de clairs m_i et m_j (montrer que $m_i \oplus m_j$ est connu).

2. On suppose que les blocs de cryptogramme sont répartis aléatoirement. Quelle est la probabilité pour qu'il existe deux blocs de n bits égaux dans un cryptogramme de t blocs ? Quelle condition doit satisfaire la taille n des blocs pour que cette probabilité soit inférieure à 1/1000 sur des cryptogrammes d'un million de blocs ?

Exercice 2 (*Une variante de DES*)

Afin d'avoir un algorithme plus rapide, des ingénieurs décident de faire les modifications suivantes sur le DES :

- La permutation des 32 bits après les boîtes-S est supprimée.
- La fonction d'expansion E est modifiée de la façon suivante. On commence par diviser les 32 bits de l'entrée en 8 blocs de 4 bits. Puis on étend chaque bloc à 6 bits en recopiant le 3ème et le 4ème bit, et en les plaçant en 5ème et 6ème positions de la sortie. (En d'autres termes, x_1, x_2, x_3, x_4 devient $x_1, x_2, x_3, x_4, x_3, x_4$.).

Montrer que l'on peut complètement casser cette version modifiée de DES (qui comprend 16 tours comme le DES). Analyser la complexité de votre attaque.

Exercice 3 (*Calcul AES*)

1. Que signifie "AES" ? Qui sont les inventeurs de l'algorithme AES ?
2. Rappeler comment est défini le produit de deux octets dans l'algorithme AES. [Rappel : le polynôme $X^8 + X^4 + X^3 + X + 1$ intervient dans la définition.]
3. Calculer $\{C7\} \times \{5A\}$.
4. Quelle propriété possède le polynôme $X^8 + X^4 + X^3 + X + 1$? Quelle est la conséquence sur l'opération de multiplication des octets ?

Exercice 4 (*Fonction de hachage*)

1. Rappeler la définition d'une fonction :
   - à collisions fortes difficiles (= "collision-resistant")
   - à collisions faibles difficiles (= "second-preimage resistant")
   - à sens unique (= "one-way")
2. Soit $f : \{0,1\}^{2m} \longrightarrow \{0,1\}^m$ une fonction de hachage. Soit maintenant une deuxième fonction de hachage définie par

$$h : \begin{array}{ccc} \{0,1\}^{4m} & \longrightarrow & \{0,1\}^m \\ x_1 || x_2 & \mapsto & f(f(x_1)||f(x_2)) \end{array}$$

   où $||$ désigne l'opération de concaténation. Montrer que si f est à collisions fortes difficiles, alors h est aussi à collisions fortes difficiles.

Exercice 5 (*Signature RSA*)

1. Calculer le module n et l'entier $\varphi(n) = (p-1)(q-1)$ associés aux nombres premiers $p = 17$ et $q = 23$.
2. Quels sont les exposants secrets de signature associés aux exposants publics $e = 11$ et $e = 13$?
3. Quelle est la signature de $m = 100$?
4. Vérifier que la vérification fonctionne.

Exercice 6 (*RSA et clairs liés*)

Montrer que si un attaquant dispose des chiffrés RSA c et c' d'un clair aléatoire m et d'un clair m' lié à m par la relation $m' = m + 1$, pour une clé publique $(N, e = 3)$, alors il peut efficacement retrouver m.

Indication : on pourra chercher des nombres entiers α, β, γ, δ tels que $m.(c' + \alpha.c + \beta) = c' + \gamma.c + \delta \bmod N$.