Master – 1ère année

Cryptographie – Contrôle continu

28 novembre 2017

Consignes :

- **Durée : 1h30.**
- **Documents interdits. Aucun accès à une calculatrice, un téléphone portable, un smartphone, ou tout autre dispositif électronique, connectable ou non.**

Questions de cours

1. **L'algorithme one-time-pad**
   (a) Comment est défini l'algorithme one-time-pad ?
   (b) Quel niveau de sécurité permet-il d'obtenir ? Expliquer.
   (c) En contrepartie, quel est son principal défaut dans une utilisation pratique ?
2. **L'algorithme DES**
   (a) Sur quelle construction se base le DES ?
   (b) 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 détail.
3. **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.
4. **L'algorithme AES**
   (a) Quelles sont les tailles de l'entrée, de la sortie et de la clé dans l'algorithme AES ? Combien y a-t-il de tours ?
   (b) Dans l'algorithme AES, rappeler comment est défini le produit de deux octets. [Rappel : le polynôme $X^8 + X^4 + X^3 + X + 1$ intervient dans la définition.]
5. **Fonctions de hachage**
   (a) Donner la définition d'une fonction à collisions fortes difficiles, d'une fonction à collisions faibles difficiles, d'une fonction à sens unique.
   (b) Que dit le paradoxe des anniversaires ? Donnez le plus de détails que vous pouvez.
   (c) 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 (Chiffrement de Hill)
Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier compris entre 0 et 25. L'algorithme est un chiffrement par blocs de m lettres, qui transforme un bloc $(x_1, x_2, \ldots, x_m)$ en un bloc $(y_1, y_2, \ldots, y_m)$ défini par la relation algébrique :

$$(y_1, y_2, \ldots, y_m) = (x_1, x_2, \ldots, x_m).A$$

où A est une matrice carrée d'ordre m à coefficients dans $\mathbb{Z}/26\mathbb{Z}$, tous les calculs étant donc faits modulo 26. Par exemple avec $m = 2$ et $A = \begin{pmatrix} 5 & 1 \\ 12 & 3 \end{pmatrix}$, le message $(10, 21)$ est chiffré en $(10, 21).A = (10 \times 5 + 21 \times 12, 10 + 21 \times 3) = (16, 21)$. Le déchiffrement d'un bloc se fait en multipliant le bloc chiffré par la matrice inverse de A. Une matrice carrée à coefficients dans $\mathbb{Z}/26\mathbb{Z}$ est inversible si et seulement si son déterminant est inversible modulo 26.

1. Dans le cas $m = 2$, montrer que l'inverse de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
2. Calculer la matrice inverse de celle donnée en exemple.
3. Décrire une méthode permettant d'attaquer le chiffrement de Hill "à clair connu".
4. Application : on dispose des couples $((2, 9), (11, 11))$, et $((7, 3), (11, 23))$, retrouver A.

Exercice 2 (Calcul AES)
Dans le contexte de l'AES, calculer le produit des octets $A6$ et $5D$. On expliquera clairement les différentes étapes du calcul.

Exercice 3 (Fonction de hachage)
Soit $f : \{0,1\}^m \longrightarrow \{0,1\}^m$ une fonction quelconque. On définit $h : \{0,1\}^{2m} \longrightarrow \{0,1\}^m$ de la manière suivante. Pour toute valeur $x \in \{0,1\}^{2m}$:

- on écrit $x = x_1 || x_2$ avec $x_1, x_2 \in \{0,1\}^m$.
- on pose alors $h(x) = f(x_1) \oplus f(x_2)$.

Montrer que h n'est pas à collisions fortes difficiles.

Master – 1ère année – Informatique / MINT

Cryptographie – Examen

17 janvier 2018

Consignes :

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

Exercice 1 (3 points) [*Questions diverses*]

1. Une recherche exhaustive sur les 56 bits d'une clé DES nécessite environ 56 heures. Combien de temps faudrait-il approximativement sur une clé de 64 bits ?

   ☐ 56 heures ☐ 64 heures ☐ 64 jours ☒ plus d'un an

2. Alice a utilisé le chiffrement "one-time pad" pour envoyer un message $m \in \{0,1\}^{100}$ à Bob. Ils partageaient tous deux une clé aléatoire $k \in \{0,1\}^{100}$. Charlie intercepte le chiffré $c = m \oplus k$. Quel est le temps nécessaire pour retrouver m ?

   ☐ instantané ☐ 100 essais ☐ 2^{100} essais ☐ impossible

3. Une implémentation de RSA, utilisant des exposants public et privé aléatoires de la taille du module, annonce le temps de calcul suivant : 1 milliseconde pour chiffrer un message de 512 bits avec une clé de 512 bits. Sachant que cette implémentation utilise l'algorithme d'exponentiation vu en cours, quel temps nécessiterait le chiffrement RSA d'un message de 2048 bits avec une clé de 2048 bits (en millisecondes) ?

   ☐ 1 ☐ 8 ☐ 16 ☐ 32 ☐ 64 ☐ 128

4. Afin de pouvoir distinguer ses communications personnelles de ses communications professionnelles, Alice utilise deux clés publiques RSA, ses correspondants utilisant l'une ou l'autre selon le type de communication. Afin d'accélérer la génération de clés, Alice ne choisit que trois grands nombres premiers p, q et r de 512 bits, qu'elle garde secrets. Ses deux modules RSA publics sont alors $N_1 = pq$ et $N_2 = qr$. Alice choisit aléatoirement deux couples d'exposants privés et publics (d_1, e_1) et (d_2, e_2) vérifiant donc $e_1 d_1 \equiv 1 \bmod (p-1)(q-1)$ et $e_2 d_2 \equiv 1 \bmod (q-1)(r-1)$. Quelle est la sécurité obtenue ?

   ☐ impossible à déterminer ☐ identique au RSA traditionnel ☐ aucune sécurité

5. Un problème du mode CBC est qu'aucun parallélisme n'est possible. Il faut connaître le chiffré du bloc précédent. Une proposition est de séparer l'ensemble des blocs en par exemple deux groupes : ceux de numéro pair et ceux de numéro impair. On fait donc deux CBC en parallèle, l'un avec la clé k_1, et l'initialisation IV_1, l'autre avec k_2 et IV_2. Comment garder la sécurité de CBC ?

   □ Je peux utiliser la même clé et le même IV

   □ Je peux utiliser la même clé mais pas le même IV

   □ Les clés doient être différentes et les IV aussi

   □ Je ne peux pas avoir la sécurité d'un unique CBC

6. Pour la signature de longs messages, on utilise habituellement une fonction de hachage destinée à transformer le message avant signature. Sachant qu'une borne supérieure pour une recherche exhaustive se situe vers 2^{80}, quelle longueur de haché doit-on préconiser pour éviter les contrefaçons ?

   □ 40 bits □ 80 bits □ 128 bits □ 160 bits

Exercice 2 (3 points) [*Variante du DES*]
Des théoriciens proposent une variante de DES (dite avec *blanchiment*) qui utilise une clé de 120 bits de la forme $K = (K_1, K_2) \in \{0,1\}^{56} \times \{0,1\}^{64}$ et qui chiffre un bloc m de 64 bits sous la forme

$$c = DES_{K_1}(m) \oplus K_2.$$

Montrer qu'il existe une attaque à deux clairs connus contre cette variante de DES qui demande 2^{57} évaluations de la fonction DES (*i.e.* que cette variante ne ralentit la recherche exhaustive que d'un facteur 2).

Exercice 3 (3 points) [*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 $\{D1\} \times \{67\}$.
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 (3 points) [*Construction d'une fonction de hachage*]

1. Rappeler la définition d'une fonction à collisions fortes difficiles, d'une fonction à collisions faibles difficiles, d'une fonction à sens unique.

2. Soient $\mathcal{E}$ un ensemble fini, et f_0 et f_1 deux permutations sur $\mathcal{E}$ (*i.e.* deux fonctions bijectives sur $\mathcal{E}$) à sens unique. On appelle *rencontre* entre f_0 et f_1 tout couple $(a, b) \in \mathcal{E} \times \mathcal{E}$ tel que $f_0(a) = f_1(b)$. On dit que les fonctions f_0 et f_1 *ne se rencontrent pas* s'il est algorithmiquement difficile de trouver une rencontre entre f_0 et f_1.

   À partir d'une paire de telles fonctions à sens unique qui ne se rencontrent pas, et d'un élément $e \in \mathcal{E}$ fixé, on construit une fonction h sur l'ensemble de toutes les chaînes binaires finies $\{0,1\}^*$ de la façon suivante :

$$h : \begin{array}{ccc} \{0,1\}^* & \longrightarrow & \mathcal{E} \\ x = x_1 x_2 \ldots x_k & \mapsto & f_{x_1}(f_{x_2}(\ldots f_{x_k}(e)\ldots)) \end{array}.$$

   Montrer que la fonction h ainsi construite est à collisions fortes difficiles.

Exercice 5 (2 points) [*Calcul RSA*]
Calculer $101^{4800000023} \bmod 35$.

Exercice 6 (4 points) [*RSA avec modulo commun*]
On suppose que deux entités Alice et Bob utilisent un schéma de chiffrement RSA avec le même modulo n et des exposants publics différents e_1 et e_2.

1. Montrer qu'Alice peut déchiffrer les messages adressés à Bob.

2. Montrer qu'un attaquant Charlie peut déchiffrer un message envoyé à la fois à Alice et Bob, à condition d'avoir $\text{pgcd}(e_1, e_2) = 1$.

3. Application numérique : supposons que $n = 35$, $e_1 = 7$ et $e_2 = 17$. On suppose que – pour un même message clair donné x – les messages chiffrés envoyés respectivement à Alice et à Bob sont $y_1 = 32$ et $y_2 = 23$. Trouver le message clair x.

Exercice 7 (3 points) [*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 lié $m + 1$, 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 $m.(c' + \alpha.c + \beta) = c' + \gamma.c + \delta \bmod N$.

Master – 1ère année – Informatique et MINT

Cryptographie – Rattrapage

13 juin 2018

Consignes :

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

Exercice 1 (8 points) [*Questions diverses*]

1. Une recherche exhaustive sur les 56 bits d'une clé DES nécessite environ 56 heures. Combien de temps faudrait-il approximativement sur une clé de 64 bits ?

   ☐ 56 heures ☐ 64 heures ☐ 64 jours ☐ plus d'un an

2. Alice a utilisé le chiffrement "one-time pad" pour envoyer un message $m \in \{0,1\}^{100}$ à Bob. Ils partageaient tous deux une clé aléatoire $k \in \{0,1\}^{100}$. Charlie intercepte le chiffré $c = m \oplus k$. Quel est le temps nécessaire pour retrouver m ?

   ☐ instantané ☐ 100 essais ☐ 2^{100} essais ☐ impossible

3. Une implémentation de RSA, utilisant des exposants public et privé aléatoires de la taille du module, annonce le temps de calcul suivant : 1 milliseconde pour chiffrer un message de 512 bits avec une clé de 512 bits. Sachant que cette implémentation utilise l'algorithme d'exponentiation vu en cours, quel temps nécessiterait le chiffrement RSA d'un message de 2048 bits avec une clé de 2048 bits (en millisecondes) ?

   ☐ 1 ☐ 8 ☐ 16 ☐ 32 ☐ 64 ☐ 128

4. Afin de pouvoir distinguer ses communications personnelles de ses communications professionnelles, Alice utilise deux clés publiques RSA, ses correspondants utilisant l'une ou l'autre selon le type de communication. Afin d'accélérer la génération de clés, Alice ne choisit que trois grands nombres premiers p, q et r de 512 bits, qu'elle garde secrets. Ses deux modules RSA publics sont alors $N_1 = pq$ et $N_2 = qr$. Alice choisit aléatoirement deux couples d'exposants privés et publics (d_1, e_1) et (d_2, e_2) vérifiant donc $e_1 d_1 \equiv 1 \bmod (p-1)(q-1)$ et $e_2 d_2 \equiv 1 \bmod (q-1)(r-1)$. Quelle est la sécurité obtenue ?

   ☐ impossible à déterminer ☐ identique au RSA traditionnel ☐ aucune sécurité

5. Une technique classique d'identification est le "mot de passe". Si on a confiance dans le serveur, cette technique

   ☐ est sûre une fois ☐ résiste aux attaques passives ☐ est zero-knowledge[1]

6. Un problème du mode CBC est qu'aucun parallélisme n'est possible. Il faut connaître le chiffré du bloc précédent. Une proposition est de séparer l'ensemble des blocs en par exemple deux groupes : ceux de numéro pair et ceux de numéro impair. On fait donc deux CBC en parallèle, l'un avec la clé k_1, et l'initialisation IV_1, l'autre avec k_2 et IV_2. Comment garder la sécurité de CBC ?

   ☐ Je peux utiliser la même clé et le même IV

   ☐ Je peux utiliser la même clé mais pas le même IV

   ☐ Les clés doient être différentes et les IV aussi

   ☐ Je ne peux pas avoir la sécurité d'un unique CBC

7. Pour la signature de longs messages, on utilise habituellement une fonction de hachage destinée à transformer le message avant signature. Sachant qu'une borne supérieure pour une recherche exhaustive se situe vers 2^{80}, quelle longueur de haché doit-on préconiser pour éviter les contrefaçons ?

   ☐ 40 bits ☐ 80 bits ☐ 128 bits ☐ 160 bits

8. Alice connaît la factorisation de $n = pq$, et elle seule. Pour prouver son identité, elle accepte, de qui le souhaite, un nombre $y = x^2 \bmod n$. Puis elle retourne une racine carrée de y, ce qu'elle seule peut calculer. Ce système d'authentification résiste

   ☐ à rien ☐ aux attaques passives ☐ est zero-knowledge

Exercice 2 (*Construction d'une fonction de hachage*) (4 points)

1. Rappeler la définition d'une fonction à collisions fortes difficiles, d'une fonction à collisions faibles difficiles, d'une fonction à sens unique.

2. Soient $\mathcal{E}$ un ensemble fini, et f_0 et f_1 deux permutations sur $\mathcal{E}$ (*i.e.* deux fonctions bijectives sur $\mathcal{E}$) à sens unique. On appelle *rencontre* entre f_0 et f_1 tout couple $(a, b) \in \mathcal{E} \times \mathcal{E}$ tel que $f_0(a) = f_1(b)$. On dit que les fonctions f_0 et f_1 *ne se rencontrent pas* s'il est algorithmiquement difficile de trouver une rencontre entre f_0 et f_1.

   À partir d'une paire de telles fonctions à sens unique qui ne se rencontrent pas, et d'un élément $e \in \mathcal{E}$ fixé, on construit une fonction h sur l'ensemble de toutes les chaînes binaires finies $\{0,1\}^*$ de la façon suivante :

$$h : \begin{array}{lcl} \{0,1\}^* & \longrightarrow & \mathcal{E} \\ x = x_1 x_2 \dots x_k & \mapsto & f_{x_1}(f_{x_2}(\dots f_{x_k}(e)\dots)) \end{array}.$$

   Montrer que la fonction h ainsi construite est à collisions fortes difficiles.

[1] On rappelle qu'un algorithme d'authentification est dit "zero-knowledge" si le fait de l'utiliser (pour s'authentifier) ne révèle rien sur ses propres secrets.

Exercice 3 (*Algorithme AES*) (4 points)

1. Que signifie "AES" ? Qui sont les inventeurs de l'algorithme AES ? En quelle année l'AES est-il devenu un standard international ?
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 $\{B7\} \times \{92\}$.
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 ? Expliquer précisément.

Exercice 4 (*Chiffrement/déchiffrement RSA*) (4 points)
Dans toute la suite, on pourra utiliser les résultats numériques suivants :

- $319 = 11 \times 29$; $10^{11} = 263 \bmod 319$; $263^2 = 216 \times 319 + 265$;
- $133^3 = 12 \bmod 319$; $133^{25} = 133 \bmod 319$;
- $11^2 = 121 \bmod 280$; $11^4 = 81 \bmod 280$; $11^8 = 121 \bmod 280$; $11^{16} = 81 \bmod 280$;
- $95 = 64 + 31$; $81 \times 11 = 51 \bmod 280$; $81 \times 121 = 1 \bmod 280$.

On considère la clé publique RSA $(11, 319)$, c'est-à-dire que $n = 319$ et $e = 11$.

1. Quel est le chiffrement avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Déchiffrer le message $C = 133$.
4. En pratique, lorsqu'on utilise l'algorithme RSA, quelle taille doit avoir le modulo n pour garantir un bon niveau de sécurité ? Expliquer avec le plus de détails possibles.