Examen ISEC 2012-2013

Auteurs
J.-C. Bajard, L. Perret

Version du 13 février 2014

Calculatrice et documents **interdits**. Le barème est donné à titre indicatif.

Exercice 1 – Cours (4 points)

– Comment fonctionne l'authentification par MAC ?
– Comment fonctionne le CBC-MAC ?
– Donner les deux grandes phases du protocole TLS ?
– Donner le principe de la certification X.509 ?
– Que pensez vous de la sécuité d'un certificat X.509 qui utilise MD5 ?

Exercice 2 – Maple (4 points)

Nous décrivons ici un algorithme proposé par Shanks pour calculer le logarithme discret dans $\mathbb{Z}_p$ (avec p premier). C'est un compromis temps-mémoire basé sur l'observation suivante. Soient $m = \lceil \sqrt{p} \rceil$, g un élément générateur et $\beta = g^x \bmod p$. La division Euclidienne de x par m donne $x = mj+i, 0 \leq i, j < m$. Nous avons alors $\beta(g^{-i}) \equiv g^{mj} \bmod p$. La méthode BSGS consiste à calculer une table des $\beta g^{-i} \bmod p, 0 \leq i < m$ (pas de bébés), ainsi que des $g^{mj} \bmod p$, $0 \leq j < m$ (pas de géants), et à trouver la valeur commune à ces deux tables :

1. Calculer $g^{mj} \bmod p$, $0 \leq j < m$.
2. Trier les paires $(j, g^{mj} \bmod p)$ selon la deuxième coordonnée ; soit L_1 la liste obtenue.
3. Calculer $\beta g^{-i} \bmod p$, $0 \leq i < m$.
4. Trier les paires $(i, \beta g^{-i} \bmod p)$ selon leur deuxième coordonnée, soit L_2 la liste obtenue.
5. Trouver $(j, y) \in L_1$, et $(i, y) \in L_2$.
6. Retourner $x =?$ (**à compléter**)

– Compléter la dernière ligne de l'algorithme (i.e. ligne 6).
– Ecrire une procédure `GiantStep:=proc(g,p)` qui prend en entrées un générateur `g`, ainsi que le modulo `p` et retourne la liste L_1.
– Ecrire une procédure `BabyStep:=proc(beta,g,p)` qui prend en entrées `beta` (β), un générateur `g`, et le modulo `p` et retourne la liste L_2.
– En déduire la procédure `Shanks:=proc(beta,g,p)` qui implante l'algorithme ci-dessus.

Exercice 3 – Miller-Rabin (6 points)

Soit n un entier premier impair. Notons $n = m \cdot 2^h + 1$, avec m impair et $h \geq 0$. Soit a un entier premier avec n. On construit la suite :

$$b_0 \equiv a^m \bmod n, b_1 \equiv b_0^2 \bmod n, \ldots, b_h \equiv b_{h-1}^2 \bmod n.$$

– Montrer que $b_h \equiv b_0^{2^h} \bmod n$.
– En déduire que $b_h \equiv 1 \bmod n$.

Dans la suite, on suppose que $b_0 \neq 1$. Soit $i, 0 < i \leq h$, le plus petit indice i tel que $b_i \equiv 1 \bmod n$.

– Montrer que $b_{i-1}^2 - 1 \equiv 0 \mod n$ et $b_{i-1} \not\equiv 1 \bmod n$.

- Expliquer pourquoi le polynôme $X^2 - 1$ n'a que deux racines modulo n.
- En déduire que $b_{i-1} \equiv -1 \bmod n$.

On montre que si $n \geq 3$ est un entier composé impair de la forme $n = m \cdot 2^h + 1$, avec m impair et $h \geq 0$, alors le nombre d'entiers $a \in \mathbb{Z}_n^*$ pour lesquels la suite $b_0, \ldots, b_h$ vérifie :

1. $b_h \equiv 1 \bmod n$,
2. $b_{i-1} \equiv -1 \bmod n$ avec $i, 0 < i \leq h$, le plus petit indice i tel que $b_i \equiv 1 \bmod n$,

est inférieur à $(n-1)/2$.

- Proposer une méthode pour tester si un nombre est composé ?
- Proposer une méthode pour tester si un nombre est premier ?

Exercice 4 – Merkle-Damgård (6 points)

Soient $f : \{0,1\}^{n+r} \mapsto \{0,1\}^n$ une fonction de compression sans-collision (i.e. $\forall x, y \in \{0,1\}^{n+r}, f(x) = f(y)$ implique que $x = y$), IV $\in \{0,1\}^n$ un vecteur d'initialisation. La chaîne x (de longueur $\leq 2^r$) est divisée en t blocs de r bits $x_1, \ldots, x_t$. Soit x_{t+1} un autre bloc de r bits qui contient la représentation binaire de la longueur de la chaîne x. On calcule l'empreinte de x comme :

$$H_0 = \mathrm{IV},\ H_i = f(H_{i-1} \mid\mid x_i),\ \forall i, 1 \leq i \leq t,\ H_{t+1} = f(H_t \mid\mid x_{t+1}).$$

Dans la suite, on note par $\mathrm{MD}(x)$ l'empreinte d'une chaîne x (c'est à dire H_{t+1}).

- Soient $x, y \in \{0,1\}^*$ tels que $\mathrm{MD}(x) = \mathrm{MD}(y)$. Montrer que x et y sont de la même taille.
- Plus généralement, montrer que $\mathrm{MD}(x) = \mathrm{MD}(y)$ implique :

  $$x_i = y_i, \forall i, 1 \leq i \leq t+1,$$

  avec t le nombre de blocs de x.
- En déduire que la fonction MD est sans-collision.