Cryptographie - Master Ingénierie Informatique - Examen 2015-2016

Consignes. Durée 2h00. Tout document ou dispositif électronique est interdit. Le barème est donné à titre indicatif.

Exercice 1 (Feistel faible, (3 points) **) Rappel** *Dans un schéma de Feistel, on divise le texte clair en deux moitiés L_0R_0 et on itère le calcul suivant pendant r tours :*

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= (L_i \oplus f_{k_{i+1}}(R_i)) \end{aligned}$$

Ici on utilise un schéma de Feistel simplifié où la clef de tour k_{i+1} est toujours la même, disons k, et la fonction de codage f_k est le xor avec k. On a donc :

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus (R_i \oplus k) \end{aligned}$$

Question *Quelles sont les faiblesses de ce schéma en fonction du nombre de tours ?*

Exercice 2 (Mac faible, (6 points) **)** *Soit $\mathcal{F} : 2^n \to [2^n \to 2^n]$ un générateur de fonctions pseudo-aléatoire.* **Rappel** *On dit qu'un MAC est* **sûr** *si un attaquant PPT ayant pris connaissance des MAC des messages $m_1, \ldots, m_p$ (p polynomial en n) a une probabilité* **négligeable** *de produire un MAC* **valide** *pour un message m différent de $m_1, \ldots, m_p$.*

Soit $m = m_1 \cdots m_\ell$ un message avec $m_i \in 2^n$, $i = 1, \ldots, \ell$ et ℓ polynomial en n. On considère 3 schémas pour construire un Mac :

1. $$Mac_k^1(m) = \mathcal{F}_k(m_1) \oplus \cdots \oplus \mathcal{F}_k(m_\ell)$$

   où $\oplus$ est le ou-exclusif sur n bits.

2. $$Mac_k^2(m) = [r \leftarrow 2^n : (r, \mathcal{F}_k(r) \oplus \mathcal{F}_k(m_1) \oplus \cdots \oplus \mathcal{F}_k(m_\ell))]$$

   où la notation $r \leftarrow 2^n$ veut dire que r est un vecteur de n bits tiré avec probabilité uniforme. Notez que dans ce cas le MAC est composé de $2n$ bits, à savoir le vecteur r et le résultat du xor.

3. $$Mac_k^3(m) = [r \leftarrow 2^n : (r, \mathcal{F}_k(r) \oplus \mathcal{F}_k((1)_2 + m_1) \oplus \cdots \oplus \mathcal{F}_k((\ell)_n + m_\ell))]$$

   où $(i)_2$ est la représentation en base 2 du nombre naturel i, $+$ est l'addition en base 2 modulo 2^n et on suppose $\ell < 2^{n/2}$. Dans ce cas aussi le MAC est composé de $2n$ bits.

Question *Montrez que aucun de ces MAC est sûr.*

Exercice 3 (RSA premiers proches, (7 points)) *Dans cet exercice on peut faire les hypothèses suivantes :*

- *La distance moyenne entre deux points tirés avec probabilité uniforme dans l'interval* $[1, m]$ *est* $m/3$.
- *Si* p *est un nombre premier, le prochain nombre premier plus grand que* p *est en moyenne à une distance* $\log(p)$.

Soient $p > q \geq 3$ *nombres premiers avec* $n = p \cdot q$.

Questions

1. *On pose* $t = (p+q)/2$ *et* $s = (p-q)/2$. *Montrez que :* $n = t^2 - s^2$.
2. *Supposons que* $s < 2^{20}$ *et que* $q \approx 2^{512}$. *Proposez un algorithme* **pratique** *pour trouver* p *et* q *à partir de* n.
3. *Supposons que pour générer* p *et* q *on a d'abord généré* $q \approx 2^{512}$ *et ensuite pris comme* p *le plus petit premier plus grand que* q. *Pensez-vous que l'algorithme proposé dans* 2. *peut s'appliquer à la situation en question ? Expliquez.*
4. *Supposons que pour générer* p *et* q *on a fixé le premier et dernier bit à* 1 *et ensuite on a généré les* 510 *bits restants avec probabilité uniforme et on a testé la primalité. Pensez-vous que l'algorithme proposé dans* 2 *peut s'appliquer à cette situation ? Expliquez.*

Exercice 4 (signature El Gamal (4 points)) *On suppose* p *nombre premier,* g *générateur pour* $(Z_p)^*$ *et* $A = g^a \bmod p$ *pour un* $a \in \{1, \ldots, p-1\}$ *gardé sécret par Eve. On suppose aussi une* **fonction de hachage**

$$h : \{0,1\}^* \to \{1, \ldots, p-2\}$$

Pour **signer** *un document* $x \in \{0,1\}^*$, *Eve choisit :*

- $k \in \{1, \ldots, p-2\}$ *premier avec* $p-1$,
- *détermine son inverse multiplicative* k^{-1} *modulo* $p-1$,
- *et calcule* (r, s) *où :*

$$r = g^k \bmod p, \qquad s = (k^{-1} \cdot (h(x) - a \cdot r)) \bmod (p-1) \ .$$

Adam connaît la clef publique d'Eve (p, g, A). *S'il reçoit un message* x *et une signature* (r, s) *il accepte le message seulement s'il vérifie les propriétés suivantes :*

$$(1) \quad 1 \leq r \leq (p-1), \qquad (2) \quad (A^r r^s \equiv g^{h(x)}) \bmod p \ .$$

Questions

1. *Montrez que une signature d'Eve passe la vérification d'Adam.*
2. *On suppose* $p = 11$, $g = 2$, $a = 5$. *Déterminez la clef publique d'Eve.*
3. *Calculez la signature d'Eve pour un document* x *tel que* $h(x) = 7$ *et en supposant qu'elle choisit* $k = 3$.
4. *Explicitez les vérifications que Adam doit effectuer.*

Solutions

Solution à l'exercice 1 Par les propriétés du xor on a :

$$L_{i+1} = R_i \quad R_{i+1} = L_i \oplus R_i \oplus k$$
$$L_{i+2} = R_{i+1} \quad R_{i+2} = L_i$$
$$L_{i+3} = L_i \quad R_{i+3} = R_i$$

Donc si le nombre de tours est un multiple de 3 le chiffrement est la fonction identité et si le nombre de tours est congru à 1 ou à 2 modulo 3 alors le chiffrement dévoile moitié du texte clair.

Solution à l'exercice 2

1. Le Mac de $m_1 \cdot m_2$ est identique au Mac de $m_2 \cdot m_1$.
2. Idem.
3. Prenons m_i tel que $m_i + (i)_2 = 0$ (donc $(m_i \equiv -i)\ mod\ 2^n$ pour $i = 1, \ldots, \ell$. Alors :

$$\begin{array}{ll} Mac_k^3(m_1) & = (r, \mathcal{F}_k(r) \oplus \mathcal{F}_k(0)) \\ Mac_k^3(m_1 m_2 m_3) & = (r, \mathcal{F}_k(r) \oplus \mathcal{F}_k(0) \oplus \mathcal{F}_k(0) \oplus \mathcal{F}_k(0)) \\ & = (r, \mathcal{F}_k(r) \oplus \mathcal{F}_k(0)) \end{array}$$

   Donc il est suffisant de connaître le *Mac* de m_1 pour construire le *Mac* de $m_1 m_2 m_3$, $m_1 \cdots m_5$, $m_1 \cdots m_7$,...

Solution à l'exercice 3

1.

$$\frac{p^2 + 2pq + q^2}{4} - \frac{p^2 - 2pq + p^2}{4} = pq = n$$

2. L'algorithme : à partir de $s = 1$, on cherche un s tel que :

$$\begin{array}{ll} n + s^2 & \text{est un carré, disons } t^2 = n + s^2 \\ t + s & \text{est premier, disons } p = t + s \\ t - s & \text{est premier aussi, disons } q = t - s \end{array}$$

   On note qu'il y a des algorithmes efficaces pour savoir si un nombre est un carré et s'il est premier.
3. Si on génère $q \approx 2^{510}$ on s'attend à que $p - q \approx \log 2^{510} \approx 500$. Donc $s = (p-q)/2 \approx 250$ sera trouvé par l'algorithme après un petit nombre d'itérations.
4. D'après l'hypothèse on s'attend à que $p - q \approx 2^{510}/3$. Donc $s \approx 2^{508}$ qui est un nombre enorme qu'on ne pourra jamais atteindre.

Solution à l'exercice 4

1. On suppose $r = g^k \, mod \, p$ et $(s \equiv k^{-1} \cdot (h(x) - a \cdot r)) \, mod \, (p-1)$. On note $(A^r r^s \equiv g^{a \cdot r} g^{k \cdot s}) \, mod \, p$. Donc le test est équivalent à :

$$(g^{k \cdot s} \equiv g^{(h(x) - a \cdot r)}) \, mod \, p$$

Comme g est un générateur, ceci est équivalent à :

$$(k \cdot s \equiv h(x) - a \cdot r) \, mod \, (p-1)$$

ce qui est vrai par définition de s.

2. $p = 11$, $g = 2$, $A = g^a = 2^5 \equiv 10 \, mod \, 11$.
3. On note que $k = 3$ est premier avec 10 et $k^{-1} = 7$. Il suit que $r = 2^3 = 8$ et $s = 7(7 - 8 \cdot 5) \equiv 9 \, mod \, 10$. Donc la signature calculée par Eve est $(8, 9)$.
4. Adam vérifie $1 \leq 8 \leq 10$ et

$$(10^8 \cdot 8^9 \equiv 2^7) \, mod \, 11$$

Ce qui est équivalent à :

$$((10^2)^4 \cdot (2^{10})^2 \equiv 1) \, mod \, 11$$

qui suit de $(10^2 \equiv 1 \equiv 2^{10}) \, mod \, 11$.