Master CSI 1 2008-2009

Cryptologie, MHT 811 : Examen du 27 avril 2009

Master Sciences et Technologies, mention Mathématiques ou Informatique, spécialité Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

Durée : 3h. Sans document. Les exercices sont indépendants.

– Exercice 1.

a) Quel est l'ordre multiplicatif de 2 modulo 71 ?

b) Alice et Bob décident d'utiliser le protocole de Diffie-Hellman dans le sous-groupe de $(\mathbb{Z}/71\mathbb{Z})^*$ engendré par $\alpha = 2$. Alice choisit l'exposant secret $\alpha = 6$ et Bob l'exposant secret 9. Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ?

– Exercice 2. On considère un système RSA de modulo $n = 451$ et d'exposant public $e = 3$.

a) Vérifier que 128 est une signature légitime du message 2.

b) Trouver, sans chercher l'exposant secret d, les signatures des messages $4, 8, 16$.

– Exercice 3. Soient p et q deux nombres premiers impairs distincts et soit l'entier $n = pq$. On rappelle que la quantité $\phi(n)$ désigne l'indicateur d'Euler de n, soit le nombre d'entiers positifs inférieurs à n et premiers avec n.

a) Soit un entier x premier avec n. Montrer que $x^{\phi(n)/2} = 1 \mod p$ et que $x^{\phi(n)/2} = 1 \mod q$ et que $x^{\phi(n)/2} = 1 \mod n$.

b) Montrer que si $ed = 1 \bmod \phi(n)/2$, alors pour tout entier x on $x^{ed} = x \bmod n$.

– Exercice 4. Sur deux cartes à puces distinctes P et P' est implantée une même fonction de chiffrement RSA, modulo un entier $n = pq$ et utilisant un même exposant de chiffrement e. Autrement dit chacune des deux cartes prend comme entrée un message M et est censée rendre un cryptogramme égal à $M^e \mod n$. La carte P rend toujours la bonne valeur, cependant un défaut de programmation fait que P' rend un cryptogramme C tel que $C = M^e \mod p$ et $C = M^e + 1 \mod q$. Comment utilisez-vous les cartes P et P' pour trouver p et q ?

– Exercice 5. On considère le procédé de signature suivant. Le signataire S a rendu publique la donnée d'un nombre premier p, d'un élément primitif α modulo

p, et d'une quantité $P = \alpha^s \mod p$ où s est un entier secret connu de S seul. De plus, une fonction aisément calculable f de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ est elle aussi rendu publique.

Pour signer un entier M le signataire S réalise les opérations suivantes :
– il choisit un entier aléatoire r premier avec $p-1$, puis évalue $u = \alpha^r \mod p$,
– il calcule $v = r^{-1}(M - f(u)s) \mod p-1$.
La signature du message M est la donnée du couple (u, v).

a) Pour quelle fonction f retrouve-t-on la signature El Gamal classique ?

b) Comment peut-on vérifier l'authenticité de la signature (u, v) de M ?

c) Supposons que le signataire S ait choisi, par facilité, la fonction f constante et égale à zéro. Montrer comment vous pouvez contrefaire une signature d'un quelconque message M.

d) On met en œuvre le procédé avec $p = 53$, $\alpha = 2$, $P = 15$, et pour f la fonction $x \mapsto x^2 \mod 52$. Vérifier que α est bien primitif modulo p.

e) Vérifier que $(u = 22, v = 20)$ est bien une signature légitime du message $M = 20$.

f) Les valeurs de M et de (u, v) sont celles de la question précédente. Vous remarquez que $\alpha^4 = u^8 \mod 53$. En déduire une signature légitime de $M + 4$.

g) Plus généralement, pour des valeurs de p, α, u, v quelconques, on essaye de réaliser l'attaque de la question précédente en cherchant un quelconque couple (x, y) (différent de $(0, 0)$) tel que $\alpha^x = u^y \mod p$. Combien faut-il tester approximativement de couples (x, y)

(i) si on connaît l'ordre q de u

(ii) si on ne connaît pas l'ordre q de u.

– Exercice 6. On considère le chiffrement RSA $M \mapsto C = M^3 \mod n$ avec $n = 1189 = 29 \times 41$.

a) Soit $M = 360$ et C le chiffré associé. Montrer que

$$M + C = 0 \mod n.$$

b) Trouver tous les autres messages M tels que $M + C = 0 \mod n$.

c) On change le modulo, cette fois-ci $n = 989 = 23 \times 43$. Trouver tous les messages M tels que $M + C = 0 \mod n$.

d) Expliquer le phénomène.

e) On considère maintenant la fonction de chiffrement RSA $M \mapsto C'$ associée au même n mais à l'exposant public $e = 5$. Pour combien de valeurs de M a-t-on $C = C'$?

f) Les trouver.

g) Mêmes questions que les deux précédentes en replaçant $e = 5$ par $e = 7$.

– Exercice 7. Dans une variante du système de Rabin, la clé publique est un couple (n, b) et la clé privée est la factorisation $n = pq$, où p et q sont deux nombres premiers. Pour un message $M \in \mathbb{Z}/n\mathbb{Z}$, le cryptogramme est

$$C = M(M + b) \mod n.$$

a) Décrire un algorithme et/ou une formule pour déchiffrer le cryptogramme C.

b) On suppose que $p = 19$, $q = 59$ et $b = 135$.
- Calculer toutes les racines carrées de 1 modulo n.
- Calculer le cryptogramme du message $M = 999$.
- Quels sont tous les clairs possibles pour le cryptogramme trouvé précédemment ?