UHP, Faculté des sciences — Sujet d'examen

Diplôme : Master Informatique 1
Épreuve : Introduction à la Cryptologie
Examen 1re session
Date : Mardi 13 décembre 2005
Horaire : 10h à 12h

Durée du sujet : 2h
Rédacteurs : PZ, LF
Documents autorisés :
Notes de cours
Calculatrice autorisée

Les notes de cours sont autorisées. Prendre soin de motiver les réponses.

Exercice 1. Vous êtes le responsable technique d'une société spécialisée en cryptographie. Un client vient vous voir. Ce client, qu'on nommera Alice car il désire rester anonyme, veut envoyer un message à son ami Bob, en garantissant à la fois la confidentialité (seul Bob doit pouvoir lire le message), l'intégrité (Bob doit pouvoir vérifier que le message n'a pas été modifié, intentionnellement ou non), et l'origine (Bob doit pouvoir vérifier que le message vient bien d'Alice). Que conseillez-vous à votre client Alice ? Détaillez le protocole que vous proposez.

Exercice 2. Indiquer pour chacune des fonctions suivantes (i) si elles sont à sens unique ; (ii) si elles sont résistantes aux collisions.
- $h_1(x) = x^3 \bmod p$ pour p premier de 1024 bits ;
- $h_2(x) = x^3 \bmod n$ pour $n = pq$, avec p et q deux nombres premiers de 512 bits ;
- $h_3(x) = 3^x \bmod p$ pour p premier de 1024 bits.

Exercice 3. On considère le chiffrement à flot ci-dessous, où les m_i sont les caractères du message clair, et les c_i les caractères du message chiffré :

$$\begin{aligned} \sigma_{i+1} &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}) \\ z_i &= g(\sigma_i, k) \\ c_i &= h(z_i, m_i). \end{aligned}$$

Le déchiffrement s'effectue de la même manière, avec $m_i = h^{-1}(z_i, c_i)$ à la place de $c_i = h(z_i, m_i)$.

Ce chiffrement est-il auto-synchronisant ? Si oui, le montrer. Si non, le montrer. Que se passe-t-il si on remplace $\sigma_{i+1} = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1})$ par $\sigma_{i+1} = (m_{i-t}, m_{i-t+1}, \ldots, m_{i-1})$?

Exercice 4. Soit la suite $s_j = s_{j-1} + s_{j-2} + s_{j-3} + s_{j-4} \bmod 2$. Que peut-on dire des valeurs obtenues à partir des valeurs initiales $s_0 = s_1 = s_2 = s_3 = 1$? Combien de suites différentes (modulo translation) peut-on obtenir ?

Exercice 5. On rappelle le polynôme irréductible $m(x) = x^8 + x^4 + x^3 + x + 1$ sur $GF(2)$ utilisé pour AES. Quel est l'inverse de x^7 modulo $m(x)$? Calculer $x^{42} \bmod m(x)$. [Aide : plusieurs méthodes sont possibles. Bien détailler le raisonnement et les calculs éventuels.]

Exercice 6. On propose la variante suivante d'échange de clé à la Diffie-Hellman. Alice et Bob choisissent un anneau $(A, +, \times)$, et un grand entier N (public). (Par exemple, $A = \mathbb{Z}/p\mathbb{Z}$ pour p premier, ou $A = \mathbb{Z}/n\mathbb{Z}$ pour $n = pq$.) Alice choisit a aléatoire dans A et calcule $\alpha = Na$ qu'elle envoie à Bob. Bob quant à lui choisit b aléatoire dans A et calcule $\beta = Nb$ qu'il envoie à Alice. Alice garde l'éléments a secret, et Bob fait de même pour b.

- Comment Alice et Bob peuvent-il fabriquer un secret commun ?
- Le système obtenu est-il sûr ? Si oui, pourquoi ? Si non, pourquoi ?
- Mêmes questions pour $\alpha = a^N$ et $\beta = b^N$.

Exercice 7. Dix-sept personnes veulent pouvoir s'échanger des messages deux à deux. Si elles choisissent un système à clé secrète, combien de clés faut-il en tout ? Même question pour un système à clé publique. Quels sont les avantages de chaque système ? Lequel conseillez-vous ?

Exercice 8. Un module RSA $n = pq$ avec p et q de la forme $2^k + 3$ et de 512 bits chacun est-il sûr ? Argumenter.

Exercice 9. Alice envoie le message m — avec chiffrement par RSA — à Bob, Charlie, Danny, Edwige et Fanny qui ont des modules RSA différents, mais le même exposant public $e = 5$. Est-ce dangereux ? Argumenter.

Exercice 10. Danny veut partager un secret n entre Alice, Bob et Charlie, sans que deux d'entre eux puissent le reconstruire. Il fabrique un groupe G, un générateur g de grand ordre dans G, et une décomposition $n = a + b + c$, puis donne g^a à Alice, g^b à Bob, et g^c à Charlie. Ils peuvent ainsi reconstruire g^n en multipliant leurs valeurs : $g^n = g^a g^b g^c$.

- La donnée de g^n ne permet pas facilement de retrouver la valeur de n. Comment contourner ce problème ?
- En supposant que le secret est maintenant g^n, Alice et Bob peuvent-ils le reconstruire sans l'aide de Charlie ?
- En supposant derechef que le secret est n, qu'Alice connaît a, que Bob connaît b, et qu'ils connaissent tous les deux g^c, peuvent-ils retrouver n ?

Exercice 11. On note p_i le i-ième nombre premier : $p_1 = 2$, $p_2 = 3$, etc. Alice souhaite partager un message secret entre n participants de la manière suivante :

- Alice calcule $N = \prod_{i=1}^{n} p_i$ et encode le message secret m comme un entier tel que $0 \leq m \leq N - 1$.
- Alice distribue au j-ième participant le morceau de secret $n_j = m \bmod p_j$.

Montrez que le protocole décrit est bien un protocole de partage de secret, à savoir que les n participants ensemble peuvent retrouver le secret initial m, mais que même $n-1$ ne le peuvent pas. Le partage de secret vous semble-t-il équitable entre les participants ? Argumentez.