UHP, Faculté des sciences — Sujet d'examen

Diplôme : DEA Informatique
Épreuve : Arithmétique et Cryptologie
Examen 1re session
Date : Jeudi 6 janvier 2005
Horaire : 10h à 12h

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

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

Exercice 1. Pour chacun des choix suivants de mise en œuvre d'une primitive asymétrique, discuter en quelques lignes avantages et inconvénients (efficacité de construction, efficacité d'utilisation et sécurité).

a. Clé RSA de la forme $(2^{p_1}-1)\cdot(2^{p_2}-1)$ avec $p_1+p_2\approx 1024$.

b. Même question avec $p_1+p_2\approx 10000$.

c. Clé RSA de la forme $(2^{2^n}+1)\cdot(2^{2^m}+1)$, avec les deux facteurs premiers et $n,m\approx 10$.

d. Clé El Gamal avec p de la forme $2^{2^n}+1$.

e. Clé RSA avec le même N pour un groupe d'utilisateurs, mais des couples (d,e) différents.

f. Clé El Gamal avec le même (g,p) pour un groupe d'utilisateurs (ou le même groupe G) mais un a différent.

g. Clé RSA avec $e=3$.

h. Clé RSA avec $d=3$.

i. Clé El Gamal avec $a=3$.

j. Clé RSA avec $e=65537$

k. Clé RSA avec $d=65537$

l. Clé El Gamal avec $a=65537$.

m. Clé RSA avec $|p-q|\leq 1000000$.

n. Clé RSA avec $q=2^n+t$, avec $t\leq 2^{n/2}$.

Exercice 2. Pourquoi ne peut-on pas utiliser le système RSA suivant : clé publique e,p, clé secrète d tel que $ed=1 \bmod \varphi(p)$, chiffrement et déchiffrement comme dans RSA ? Même question en remplaçant p par p^2.

Exercice 3. Vous devez calculer $x^{45} \bmod n$. Donner un algorithme utilisant le moins de multiplications modulaires possible (en considérant qu'un carré coûte autant qu'une multiplication).

Exercice 4. Vous devez fabriquer un module RSA de la forme $N = p \cdot q$, avec N ayant 1024 bits. Comment vous y prenez-vous ? Détaillez la complexité des algorithmes utilisés.

Exercice 5. Montrer que 1033 est premier à l'aide du test $N - 1$ (on pourra admettre 2, 3, 5 et 7 premiers).

Exercice 6. Protocoles d'authentification. Alice, qui connaît un secret s, souhaite s'authentifier auprès de Bob. Pour chacun des protocoles suivants, évaluer la sécurité en quelques lignes. On indique dans chaque cas si l'adversaire éventuel est actif (il peut intervenir dans la communication) ou passif (il se contente d'écouter, et ne devient actif qu'ensuite). Dans les cas où la transmission d'un certificat est nécessaire pour rendre le protocole sûr, l'indiquer.

a. Alice envoie s à Bob (qui est présumé connaître s). Charlie passif.

b. Alice envoie $DES_s^{25}(00000000)$ à Bob. Charlie passif.

c. Alice envoie $MD5(s)$ à Bob. Charlie passif.

d. Alice et Bob font un échange de clés à la Diffie-Hellman, se mettent d'accord sur une clé k et Alice envoie $E_k(s)$ à Bob (Charlie passif).

e. Même question avec Charlie actif.

f. Bob envoie m à Alice, qui renvoie $MD5(s||m)$. Charlie passif.

g. Même question avec Charlie actif.

h. Bob présente à Alice le texte "Je m'appelle Alice" à signer. Charlie passif.

Exercice 7. a. Soit p premier impair, et $1 \leq a < p$. On note $\mathrm{ord}(a, p)$ le plus petit entier $k > 0$ tel que $a^k \equiv 1 \bmod p$. Montrer que k divise $p - 1$.

b. On dit qu'un entier a, $1 \leq a < p$, est un résidu quadratique modulo p s'il existe b, $1 \leq b < p$, tel que $a = b^2 \bmod p$. Sinon, on dit que a est un non-résidu quadratique modulo p. Montrer qu'il existe autant de résidus quadratiques que de non-résidus.

c. Soit $N = p \cdot q$ un module RSA, p et q premiers, un exposant public e et un exposant privé $d = e^{-1} \bmod (p-1)(q-1)$. Montrer que pour tout entier a, $1 \leq a < N$, on a $a^{ed-1} \equiv 1 \bmod N$.

d. Soit un entier a, $1 \leq a < N$. Montrer que $\mathrm{ord}(a, p)$ divise $ed - 1$.

e. On pose $ed - 1 = 2^s \cdot t$ avec t impair. Montrer que si $a^{2^{s'}t} \equiv 1 \bmod p$, avec $0 \leq s' < s$, alors $\mathrm{ord}(a, p)$ divise $2^{s'}t$.

f. En déduire un algorithme qui, à partir de N, e et d, permet de trouver p et q. Montrer que cet algorithme trouve p et q lorsque $\nu_2(\mathrm{ord}(a, p)) \neq \nu_2(\mathrm{ord}(a, q))$, où $\nu_2(m)$ est la 2-valuation de l'entier m, c'est-à-dire la plus grande puissance de 2 divisant m. Quelle est la complexité de cet algorithme, en fonction du nombre de bits de N ?