TELECOM

Contrôle des connaissances 2004/2005

CRYPTOGRAPHIE

17 novembre 2004

On sera attentif à la précision de la rédaction. Les résultats devront toujours être justifiés que ce soit par une démonstration, un algorithme ou une vérification numérique. Les protocoles seront décrits précisément.

Documents et calculettes non autorisés

Exercice 1

Quelle est la taille des blocs pour le système AES ? Combien le système AES comporte-t-il d'étage lors du codage d'un bloc ? Quelles sont les longueurs de clés possible dans le système AES ?

Exercice 2

Alice construit un cryptosystème RSA à partir des nombres $p_a = 59$, $q_a = 41$ et l'exposant de la clé publique $e_a = 7$. Quel est l'exposant d_a de sa clé secrète ? que publie-t-elle que garde-t-elle secret ?

Bob construit un cryptosystème RSA à partir des nombres $p_b = 47$ et $q_b = 67$ il doit choisir l'exposant de la clé publique parmi les nombres

$$3,\ 4,\ 5,\ 55,\ 161,\ 3041$$

Quel sera son choix ? On note e_b son choix.

Exercice 3

Montrer que 37 et 47 sont premiers. Calculer

$$17^{-1} \mod 48, \quad (10 - 17 \times 4) \times (7^{-1}) \mod 36$$

Exercice 4

Alice et Bob veulent correspondre en utilisant le cryptosystème El-Gamal. Ils choisissent leurs paramètre :

	Alice	Bob
p	37	47
α	4	3
g	2	5

Donnez les clefs publiques de Bob et d'Alice.
Grâce à ce cryptosystème ils s'envoient des nombres en base 10. Ils codent l'un et l'autre par blocs de 2.
Bob reçoit le message $(y_1, y_2) = (17, 15)$, Quel message, M, lui a envoyé Alice ?
Ce message est signé $(\gamma_a, \delta_a) = (17, 1)$. Le message a-t-il été envoyé par Alice ?
On suppose que le chiffre 17 dans la signature est correct. Quel aurait du être alors la signature d'Alice ?.

Annexe 1 : Le système El-Gamal

Alice veut transmettre un message M à Bob
1.–Bob choisit un grand nombre premier p_b (grand devant M) et deux nombres g_b et α_b inférieurs à p
2.–Bob calcule $\beta_b = g^{\alpha_b}$, β_b, g_b, p_b, est sa clef publique, α_b est sa clef secrète.
3.–Alice choisit k_a et calcule

$$y_1 \equiv g_b^{k_a} \pmod{p_b} \text{ et } y_2 = \beta_b^{k_a} M$$

La paire $e_K(M, k_a) = (y_1, y_2)$ est le message codé qu'Alice envoie à Bob.

Pour décoder Bob calcule $M \equiv y_2 (y_1^{\alpha_b})^{-1} \pmod{p_b}$. Comme $y_1^{\alpha_b} = g^{k_a \alpha_b} \pmod{p}$ on a :

$$d_K(y_1, y_2) = y_2 (y_1^{\alpha_b})^{-1} \equiv \beta_b^k M (g_b^{k\alpha_b})^{-1} \equiv g_b^{\alpha_b k_a} M g^{-\alpha_b k_a} \equiv M \mod p$$

Signature El Gamal

On reprend les notations précédentes. Soit M un message qu'Alice veut transmettre en le signant à Bob.
Soit $K_a = (p_a, g_a, \beta_a)$ la clef publique d'Alice et α_a sa clef secrète. Alice choisit $k'_a \in (\mathbb{Z}/p_a\mathbb{Z})^*$ (secret) que l'on suppose de plus premier à $p_a - 1$. On définit

$$\text{sign}_{K_a}(M, k'_a) = (\gamma_a, \delta_a)$$

avec

$$\begin{aligned} \gamma_a &\equiv g_a^{k'_a} \mod p_a \\ \delta_a &\equiv (M - \alpha_a \gamma_a) {k'_a}^{-1} \mod (p_a - 1) \end{aligned}$$

Pour M, $\gamma_a \in (\mathbb{Z}/p_a\mathbb{Z}_p)^*$ et $\delta_a \in (\mathbb{Z}/(p_a - 1)\mathbb{Z})$ on définit

$$\boldsymbol{\text{ver}_{K_a}(M, \gamma_a, \delta_a) = (vrai) \Leftrightarrow \beta_a^{\gamma_a} \gamma_a^{\delta_a} \equiv g_a^M \mod p_a}$$

On constate que cette procédure réalise bien une signature du message M

Annexe 2 : Données numériques

Puisances de 16 modulo 37 :

$1, 16, 34, 26, 9, 33, 10, 12, 7, 1, 16, 34, 26, 9, 33, 10, 12, 7, 1, 16, 34, 26, 9,$
$33, 10, 12, 7, 1, 16, 34, 26, 9, 33, 10, 12, 7, 1$

Puisances de 2 modulo 37 :

$1, 2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13, 26, 15, 30, 23, 9, 18, 36, 35, 33, 29, 21,$
$5, 10, 20, 3, 6, 12, 24, 11, 22, 7, 14, 28, 19, 1]$

Puisances de 17 modulo 47 :

$1, 17, 7, 25, 2, 34, 14, 3, 4, 21, 28, 6, 8, 42, 9, 12, 16, 37, 18, 24, 32, 27,$
$36, 1, 17, 7, 25, 2, 34, 14, 3, 4, 21, 28, 6, 8, 42, 9, 12, 16, 37, 18, 24, 32, 27, 36, 1$

Puisances de 7 modulo 85 :

$1, 7, 49, 3, 21, 62, 9, 63, 16, 27, 19, 48, 81, 57, 59, 73, 1, 7, 49, 3, 21,$
$62, 9, 63, 16, 27, 19, 48, 81, 57, 59, 73, 1, 7, 49, 3, 21, 62, 9, 63, 16, 27,$
$19, 48, 81, 57, 59, 73, 1, 7, 49, 3, 21, 62, 9, 63, 16, 27, 19, 48, 81, 57, 59, 73$

Puisances de 7 modulo 91 :

$1, 7, 49, 70, 35, 63, 77, 84, 42, 21, 56, 28, 14, 7, 49, 70, 35, 63, 77, 84, 42,$
$21, 56, 28, 14, 7, 49, 70, 35, 63, 77, 84, 42, 21, 56, 28, 14, 7, 49, 70, 35, 63,$
$77, 84, 42, 21, 56, 28, 14, 7, 49, 70, 35, 63, 77, 84, 42, 21, 56, 28, 14, 7, 49, 70,$
$35, 63, 77, 84, 42, 21, 56, 28, 14$

puissances de 4 modulo 85

$1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16,$
$64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4, 16, 64, 1, 4,$
$16, 64, 1, 4, 16, 64, 1, 4, 16, 64]$

puissances de 4 modulo 91

$1, 4, 16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1, 4,$
$16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1, 4, 16, 64,$
$74, 23, 1, 4, 16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1, 4, 16, 64, 74, 23, 1$