Université de Nice-Sophia Antipolis
M2 IFI, parcours CSSR
Cryptographie & Sécurité 2010–2011

Examen de novembre 2010

Nom : _____

Prénom : _____

Durée : 2h

Note :

L'examen comporte plusieurs parties indépendantes. Répondez sur la copie avec clarté et concision.

1 Questions courtes [5 points]

1. Expliquez pourquoi un chiffre déterministe ne peut assurer la sécurité sémantique.

On considère l'expérience IND-CPA pour laquelle l'adversaire a accès au chiffre. Quand il choisit m_0 et m_1, il calcule aussi $Enc_{pk}(m_0)$ et $Enc_{pk}(m_1)$ et, quand il reçoit c, il ne lui reste plus qu'à comparer avec $Enc_{pk}(m_0)$ et $Enc_{pk}(m_1)$ pour décider quel est le clair correspondant à c.

2. Expliquez la différence entre un certificat racine « légitime » et un certificat auto-délivré.

La différence porte sur la confiance. Un cert. légitime est largement distribué et permet à la vérif de remonter la chaîne de certif. vers racine tandis qu'un certif. auto-délivré doit être ajouté (et vérifié) manuellement par l'utilisateur

3. Expliquez la raison pour laquelle on transmet toujours une clé publique au moyen d'un certificat.

Pour contrer une attaque de l'homme du milieu.

4. Décrivez la technique pour assurer l'authentification au moyen d'un MAC (*message authentication code*).

Les 2 parties s'entendent sur une clé K (partagée secrète) et, pour chaque message transmis, ils ajoutent à M la valeur $h(M\|K)$ ou $h(K\|M)$ ou $h_K(M)$ aux paquets.

5. Pourquoi la signature numérique ne permet-elle pas d'assurer le service de confidentialité ?

Sinon on perd la propriété que n'importe qui peut faire la vérif. L'algo de vérif demande qu'on ait le message en clair pour fonctionner. Il est donc impossible d'assurer la confidentialité.

2 Le paradoxe du voleur de cartes bancaires [3 points]

1. Un voleur de cartes bancaires s'interroge sur le nombre de cartes bleues qu'il doit voler pour avoir plus d'une chance sur deux d'avoir deux cartes avec le même code secret. En détaillant vos calculs, donnez-lui ce nombre : ($\ln(2) \approx 0.7$ et $\sqrt{1+x} \approx 1 + \frac{x}{2}$)

Nombre de codes secrets possibles : 10^4 (4 digits) correspond à n. On cherche donc la valeur k tq pour $p > 1/2$ $k \geq \sqrt{2n \ln 2} = 1{,}17 \cdot \sqrt{10^4} \simeq 117$

Il lui faut donc voler environ 117 cartes pour avoir plus d'1 chance sur 2 pour que 2 cartes aient le même code

2. Quel est ce nombre s'il souhaite avoir plus de deux chances sur trois ($\ln(3) \approx 1.1$)

On remonte à l'égalité $\ln \ln \frac{1}{q} \alpha k^2$

Dans ce cas $q = 1/3$ (événement complémentaire)

et $\ln\left(\frac{1}{3}\right) = \ln 3 \ldots = 1,1$

et $k > \sqrt{2 \ln \ln 3} = \sqrt{2,2 \cdot 10^4} \simeq 149$

Il lui faut donc voler environ 149 cartes pour avoir plus d'1 chance sur 3 pour que 2 cartes aient le même code.

3 Clés publiques [6 points]

On étudie un système à clé publique à la El Gamal avec une structure de groupe additive.
Pour p premier et α un élément primitif de $\mathbb{Z}_p$, on calcule $\beta \equiv \alpha a \mod p$. On signe alors M par (γ, δ) comme

$$\begin{cases} \gamma \equiv k\alpha \mod p & \text{pour } k \text{ une valeur aléatoire} \\ \delta \equiv (M - a\gamma)k^{-1} \mod p \end{cases}$$

1. Quels sont les paramètres publics et privés de ce système ?

Analogue à ElGamal :

Publics : α, β, p

Privé : a

2. Quelle condition M doit vérifier ?

M doit être un entier modulo p ie

$M < p$

3. Quel est le problème qui est supposé difficile ?

Etant donnés α, β, p retrouver a ie résoudre chercher a tq $\beta = \alpha^a \bmod p$

4. Décrivez une attaque simple sur les paramètres de ce mécanisme de signature.

Il suffit de trouver l'inverse de $\alpha \bmod p$ par Euclide étendu par exemple et de calculer

$$\alpha^{-1}\beta = (\alpha^{-1}\alpha)a \bmod p$$

d'où on tire $a = \alpha^{-1}\beta \bmod p$

5. Montrez que la signature est valide si et seulement si $\gamma\beta + \gamma\delta \equiv \alpha M \mod p$

$$\gamma(\beta+\delta) = \alpha k\left(\alpha a + (M - a\gamma)k^{-1}\right) = \alpha M \bmod p$$
$$= (\alpha^{-1}\alpha)k(\alpha a + (M - a\gamma)k^{-1}) = (\alpha^{-1}\alpha)M \bmod p$$
$$= \alpha k a + M - a\gamma = M \bmod p \quad (\text{or } \gamma = k\alpha)$$
$$= \alpha k a + M - a k \alpha = M \bmod p$$

6. Supposons que le générateur de nombres pseudo-aléatoires de l'expéditeur tombe en panne et renvoie toujours la valeur a. Dites comment un adversaire peut s'en rendre compte s'en servir pour attaquer le système.

Il calcule donc $\gamma = \alpha^a \bmod p$

$$\delta = (M - a\gamma)a^{-1} \bmod p$$

On remarque que le message transmis (M, γ, δ) a pour $\gamma = \alpha^a = \beta$ paramètre public et $\delta = a^{-1}M - \beta \bmod p$.

Il suffit donc de calculer a (cf. quest 4), pour retrouver $M = a(\beta+\delta) = a(\gamma+\delta) \bmod p$.

4 Chiffre de Merkle-Hellman [6 points]

On considère $A = (3, 6, 12, 24)$, une suite super-croissante.

1. Construisez B la suite perturbée obtenue avec un module $m = 53$ et un mutiplicateur $t = 23$.

$A = (3, 6, 12, 24)$ } $\times 23 \mod 53$
$B = (16, 32, 11, 22)$

les opérations se font facilement à la main !

2. Vérifiez (en justifiant) que 30 est l'inverse multiplicatif de 23 en arithmétique modulo 53.

$23 \times 3 = 69 \Rightarrow 23 \times 30 = 690$ | 53
-53 13
160
-159
1 ← reste de la div.

Euclidienne de 23×30 par 53.

3. Rappelez quels sont les paramètres publics et privés du chiffre ainsi obtenu.

Publics B
Privés t, t^{-1} (et A) et m

On considère le codage des lettres en binaire suivant :

A	00000	I	01000	Q	10000
B	00001	J	01001	R	10001
C	00010	K	01010	S	10010
D	00011	L	01011	T	10011
E	00100	M	01100	U	10100
F	00101	N	01101	V	10101
G	00110	O	01110	W	10110
H	00111	P	01111	X	10111
				Y	11000
				Z	11001

4. Codez le clair `OUI` (attention ! coder n'est pas chiffrer !).

O = 01110
U = 10100
I = 01000

0111 0101 0001 000 (1)

cf p. suivante

5. Chiffrez le codage du clair OUI au moyen du chiffre de Merkle-Hellman en détaillant vos calculs. Le cas échéant, s'il faut compléter le codage binaire du clair, on ajoutera des 1 à la fin pour compléter.

$\langle (16,32,11,22), (0,1,1,1) \rangle = 65$
$\langle (16,32,11,22), (0,1,0,1) \rangle = 54$
$\langle (16,32,11,22), (0,0,0,1) \rangle = 22$
$\langle (16,32,11,22), (0,0,0,1) \rangle = 22$
↑ ajouté

} transmis 65, 54, 22, 22

6. Déchiffrez 33 33 38 48 33 en rappelant les étapes suivies pour retrouver le clair.

33 33 38 48 33
36 36 27 9 36 ← ×30 mod 53

Puis on résout chaque problème de somme de sous-ens avec A et chacune des valeurs ci-dessus

$A = (3, 6, 12, 24)$

36 → 0011
33 → 1101
27 → 1001
9 → 1100
36 → 0011

On regroupe par blocs de 5

00111 → G
10110 → O
01110 → O
00011 → D

le message clair était "GOOD" !