Département informatique **Le 03/06/2013**
Faculté Electronique et Informatique **Master SSI 1ère année**
USTHB

Examen de Cryptographie et Sécurité
Durée : 1h30 – Documents non autorisés

Exercice 1 (7pts)
Le but de l'exercice est de trouver des chiffrements dont la fonction de déchiffrement est la même que la fonction de chiffrement.
1. Si la fonction de chiffrement est involutive quelle est la clé de déchiffrement ?
2. On se place dans le cas d'un chiffrement par décalage sur l'alphabet Zn. Trouver toutes les clés involutives (i.e. telles que la fonction de chiffrement est involutive). Traiter les cas n = 26 et n = 29.
3. Si le chiffrement est affine sur Zn, caractériser les clés involutives. Préciser le nombre de clés involutives dans le cas où n est un nombre premier.

Exercice 2 : (13pts)
On s'intéresse à l'algorithme cryptographique d'ElGamal.
1. Peut-on avoir pour un même message clair plusieurs messages chiffrés ? justifier votre.
2. Afin d'utiliser l'algorithme ElGamal , Alice et Bob s'entendent sur les valeurs de p; g. Soit g=3 montrer que g est générateur de Z_7 .
3. Soit a = 4 la clé secrète d'Alice, donner la clé publique d'Alice.
4. Supposons que Bob veut envoyer le message m=2 à Alice avec un aléa k=5; quel est le message chiffré correspondant à envoyer à Alice ?
5. Montrer comment Alice retrouve le message m à partir du message chiffré reçu.
6. Une mauvaise utilisation de la signature d'ElGamal consiste à utiliser la même valeur de k pour signer plusieurs messages. Montrer que si Bob signe deux différents messages m_1,m_2 avec la même valeur k et obtient les signatures (r,s_1), (r,s_2); Oscar pourra générer une signature pour tout message dans des conditions particulières.
7. Supposons que le générateur de nombres pseudo-aléatoires d'Alice tombe en panne. Elle décide d'utiliser sa clé privée a à la place. Comment Oscar qui intercepte (m,r,s) peut-il se rendre compte de cette panne ?
8. Considérons a variante de la signature d'ElGamal où p, g, a, A, k, r sont les mêmes pour la signature d'ElGamal mais $s= (1 - ma)k^{-1}r^{-1} \bmod (p-1)$. quelle est la vérification de cette signature ?
9. Montrer qu'Oscar peut casser cette signature.

Département informatique **Le 03/06/2013**
Faculté Electronique et Informatique **Master SSI 1ère année**
USTHB

Corrigé

Exercice 1: (7pt)

1- (1pt) La clé de chiffrement est égale à la clé de déchiffrement.

2- (2pt) Les chiffrements par décalage s'écrivent $x \rightarrow x + K$ [n]. Les clefs involutives sont celles pour lesquelles $f^{-1}(f(x))=x$; $f^{-1}(x+K)=x+2K = x \rightarrow 2K=0$[n].
(0.5pt) Pour n=26 ce sont les clefs pour lesquelles 2K = 26q soit K = 13q. On a alors K = 13;K =0.
(0.5pt) Pour n=29, on a K=0

3- (2pt) Chiffrement affine : on cherche les fonctions de codage telles que $f_{a,b}(f_{a,b}(x))\equiv x$ pour tout x dans E (c'est-à-dire $(f_{a,b})^{-1}= f_{a,b}$) : on doit donc avoir pour tout x dans E $a(ax+b)+b\equiv x$ [n]soit $a^2x+ab+b\equiv x$ [n]. Donc il faut que $a^2\equiv 1$ [n]et $b(a+1)\equiv 0$ [n]
(1pt) Si n est premier, la solution pour les deux équations précédentes est a=n-1 et $b\in Z_n$, les clés sont les couples (n-1,b) il y a n clés

Exercice 2: (13pt)

1. (1pt) Notons que ce calcul dépend du choix de k et donc que pour un message clair donné, il y a plusieurs messages chiffrés correspondants
2. (1.5pt) $3^1 = 3$; $3^2 = 9 = 2$; $3^3 = 2 * 3 = 6$; $3^4 = 6 * 3 = 4$; $3^5 = 4 * 3 = 5$; $3^6 = 5 * 3 = 1$, tous les calculs sont modulo 7, ainsi $g = 3$ génère tous les éléments de Z_7, il est générateur de Z_7.
3. (0.5pt) Soit $a = 4$ la clé secrete d'Alice, Alors $A = g^a \pmod p = 3^4 \pmod 7 = 4$. La clé publique est ($p = 7$; $g = 3$;$A = 4$)
4. (1pt) Le message chiffré est un couple (c_1; c_2) il est obtenu comme suit :
   $c_1 = g^k \pmod p = 3^5 \pmod 7 = 5$
   $c_2 = mA^k \pmod p = 2 * 4^5 \pmod 7 = 2 *2 = 4$
5. (2pt) Soit le couple reçu par Alice (c_1; c_2) , elle déchiffre le message comme suit :
   $m = c_1^{-a} c_2 \pmod p$
   $= 5^{-4}4 \pmod 7$
   $= (5^{-1})^4 4 \pmod 7$
   $= 3^4 4 \pmod 7$
   $= 4 * 4 \pmod 7$
   $= 2$
6. (2pt) $S_1= k^{-1}(m_1-ar) \bmod p-1$
   $S_2= k^{-1}(m_1-ar) \bmod p-1$
   $k=(s1-s2)(m1-m2)^{-1} \bmod p-1$ si pgcd((m1-m2), p-1)=1, on trouvera k et conséquent on trouvera a la clé secrète, on pourra signer tout message
7. (2pt) La clé publique est (p ; g; $A = g^a$) si k=a, $r=g^a=A \bmod p$ et oscar remarque que r=A
8. (2pt) la vérification est $g*r^{-rs}= A^m$
9. (1pt) A partir de r,s choisis, on peut définir un message m.