Sécurité - Master Ingénierie Informatique - Examen 2012-2013

Durée 2h. L'utilisation de notes de cours est autorisée, l'utilisation de livres et de dispositifs électroniques est interdite.

Exercice 1 (cryptoanalyse affine) *La fonction de chiffrement E utilisée est un chiffrement de Hill en dimension 2. La correpondence lettres–chiffres modulo 26 est standard : $A \leftrightarrow 0$, $B \leftrightarrow 1$, ..., $Z \leftrightarrow 25$. On sait que le chiffrement de $AABCEDFG$ est $AAJIQRDC$ Trouvez le chiffrement de $HILL$. Expliquez votre méthode.*

Exercice 2 (programmation fonction hash en Java) *Si $t_0, ..., t_n$ est une suite de bits alors on denote par $val(t_0, ..., t_n)$ l'entier $\Sigma_{i=0,...,n}(t_i \cdot 2^i)$. Si m est un entier positif alors $\lfloor log_2 m \rfloor$ dénote l'entier $max\{k \mid 2^k \leq m\}$. Etant donné deux entiers positifs g et m, pour calculer le hash d'une suite de bits $t_0, ..., t_n$ on calcule $h = (g^{val(t_0,...,t_n)}) \bmod m$ et on retourne les $\lfloor log_2 m \rfloor$ bits les moins significatifs de la représention binaire de h. Écrire une fonction* Java *qui implemente cette methode avec un en tête de la forme :*

```
static boolean[] hash (boolean[] t, int g, int m)
```

La méthode doit avoir une complexité proportionnelle à $(n+1)$ (la longueur de la suite de bits en entrée). Aucune fonction de bibliothèque est autorisée.

Exercice 3 (test pour les résidus quadratiques) *Soit $p > 2$ nombre premier. On dit que a dans le groupe multiplicatif $(\mathbf{Z}_p)^*$ est un résidu quadratique s'il existe $x \in (\mathbf{Z}_p)^*$ tel que $(x^2 \equiv a) \bmod p$. Rappel : $(\mathbf{Z}_p)^*$ est un groupe cyclique avec $\phi(p-1)$ générateurs.*

1. *Calculez les résidus quadratiques pour $p = 7$.*
2. *Montrez que si a est un résidu quadratique alors $(a^{(p-1)/2} \equiv 1) \bmod p$.*
3. *Montrez qu'un générateur de $(\mathbf{Z}_p)^*$ ne peut pas être un résidu quadratique et calculez les générateurs pour $p = 7$.*
4. *Montrez que si $a \in (\mathbf{Z}_p)^*$ et $(a^{(p-1)/2} \equiv 1) \bmod p$ alors a est un résidu quadratique.*

Exercice 4 (attaque sur un protocole) *On se place dans le cadre du modèle de Dolev-Yao. L'objectif du protocole est d'etablir des clefs de session nouvelles entre participants avec l'aide d'un tiers de confiance* S. *Dans le cas décrit ci-dessous il y a trois participants* A, B *et* C *et les nouvelles clefs sont* Kab *et* Kbc. *Au debut du protocole chaque participant partage une clef avec* S *(*Kas, Kbs *et* Kcs*).*

```
A, B, C, S :    participants
Kab, Kbc :      nouvelles clefs symétriques
Na, Nb, Nc :    nonces
Kas, Kbs, Kcs : clefs symétriques
h : une fonction qui prend un message et une clef et produit un message

1. A calcule Xa = h((A,B,Na),Kas), (A,B,Na)
   A ->B : Xa

2. B calcule Xb = h((B,C,Nb,Xa),Kbs), (B,C,Nb,Xa)
   B -> C : Xb

3. C calcule Xc = h((C,S,Nc,Xb),Kcs), (C,S,Nc,Xb)
   C ->S : Xc

4. S calcule Yc = A, B, Kab xor h(Na,Kas), {A,B,Na}Kab,
                  B, A, Kab xor h(Nb,Kbs), {B,A,Nb}Kab,
                  B, C, Kbc xor h(Nb,Kbs), {B,C,Nb}Kbc,
                  C, B, Kbc xor h(Nc,Kcs), {C,B,Nc}Kbc
   S -> C : Yc


5. C calcule Yb = A, B, Kab xor h(Na,Kas), {A,B,Na}Kab,
                  B, A, Kab xor h(Nb,Kbs), {B,A,Nb}Kab,
                  B, C, Kbc xor h(Nb,Kbs), {B,C,Nb}Kbc
   C -> B : Yb

6. B calcule Ya = A, B, Kab xor h(Na,Kas), {A,B,Na}Kab
   B ->A : Ya
```

1. *A chaque session du protocole, les participants doivent calculer les données nouvelles suivantes :* Na, Nb, Nc, Kab, Kbc. *Pour chaque donnée, spécifiéz le participant qui la génère et le pas de calcul (1-6) où célà se passe.*
2. *Expliquez en détail comment au pas 4 le participant* S *analyse le message* Xc *réçu par* C*, sous quelles conditions il l'accepte et dans ce cas comment il calcule le message* Yc *à partir du message* Xc.
3. *En utilisant les propriétés du xor montrez que* C *peut apprendre la clef* Kab.

Solutions

Cryptoanalyse affine

1 point En utilisant $AABCED$, la matrice différence des textes clairs est :

$$P = \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$$

et celle des textes chiffrés correspondants est :

$$C = \begin{bmatrix} 9 & 16 \\ 8 & 17 \end{bmatrix}$$

1,5 points La matrice P a une inverse :

$$P^{-1} = \begin{bmatrix} 15 & 6 \\ 16 & 5 \end{bmatrix}$$

1,5 points On dérive la matrice (=clef) de chiffrement :

$$CP^{-1} = \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$$

1 point Il suit que le chiffrement de $HILL$ est $NMDD$.

NB Le fait que la matrice difference P est égale à la matrice de chiffrement est bien sûr un hasard.

Programmation Java

```
static boolean[] hash(boolean[] t, int g, int m){
// calcul du hash : 3 points
        int n = t.length;
        int hash=1;
        int power = g;
        for (int i=0; i<n;i++){
            if (t[i]){hash = (hash * power)%m;}
            power = (power * power)%m;}
// calcul du log : 1 point
        int log=0;
        int d=m/2;
        while (d !=0 ){d=d/2; log=log+1;}
// conversion hash en binaire : 1 point
        boolean[] result = new boolean[log];
        for (int i=0;i<log;i++){
            boolean r;
            if ((hash%2)==0){r=false;} else {r=true;}
            result[i]=r;
            hash=hash/2;}
return result; }
```

Test pour les résidus quadratiques

1 point On calcule modulo 7 :

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 \ .$$

Donc les résidus quadratiques sont : $\{1, 2, 4\}$.

1 point Si $(x^2 \equiv a)\ mod\ p$ alors par Fermat on a :

$$(1 \equiv x^{(p-1)} \equiv (x^2)^{(p-1)/2} \equiv a^{(p-1)/2})\ mod\ p \ .$$

1 point Si $(a \equiv x^2)\ mod\ p$ est un résidu quadratique alors

$$(x^{(p-1)} \equiv a^{(p-1)/2} \equiv 1)\ mod\ p \ .$$

Donc a n'a pas ordre $(p-1)$ et n'est pas un générateur. Par ailleurs, on sait qu'il doit y avoir :

$$\phi(7-1) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$$

générateurs. Comme les générateurs ne peuvent pas être des résidus quadratiques les seules possibilités qui restent sont 3 5 et 6. On élimine 6 car $(6^2 \equiv 1)\ mod\ 7$.

2 points Soit g un générateur et $i \in \{1, \ldots, (p-1)\}$ tel que $(g^i \equiv a)\ mod\ p$. Ceci implique que :

$$(g^{(i \cdot (p-1))/2} \equiv 1)\ mod\ p$$

Comme l'ordre de g est $(p-1)$ on doit avoir que $(p-1)$ divise $i \cdot (p-1)/2$ ce qui implique que i est pair. Mais alors $i = 2k$ et $(a \equiv (g^k)^2)\ mod\ p$ est un résidu quadratique.

Attaque sur un protocole

1 point
```
Na: A au pas 1.
Nb: B au pas 2.
Nc: C au pas 3.
Kab, Kbc: S au pas 4.
```

2 points
```
De Xc, S apprend Nc, Xb.
Il cherche a déchiffrer h((C,S,Nc,Xb),Kcs) avec Kcs et
vérifie que le message contient (C,S,Nc,Xb).
De Xb, S apprend Nb, Xa.
Il cherche a déchiffrer h((B,C,Nb,Xa),Kbs) et
vérifie que le message contient (B,C,Nb,Xa).
Enfin, de Xa, S apprend Na. Il cherche a déchiffrer h((A,B,Na),Kas) et
vérifie que le message contient (A,B,Na).
A la fin de cette phase, S a appris Na, Nb et Nc.
Il génère les clefs Kab et Kbc et peut donc calculer Yc.
```

2 points Si le participant `C` est malhonnête il peut apprendre la clef de session `Kab` partagée par les participants `A` et `B`. Pour ce faire, `C` utilise les composantes :

`Kab xor h(Nb,Kbs)  et  Kbc xor h(Nb,Kbs)`

du message envoyé par `S` au pas `4`. Comme `C` connaît la clef de session `Kbc`, il peut calculer

`Kbc xor Kab xor h(Nb,Kbs) xor Kbc xor h(Nb,Kbs) = Kab`