Cryptographie - Master Ingénierie Informatique - Examen 2014-2015

Durée 2h30.

Exercice 1 (Hill) *On sait que le chiffrement de Hill du mot THISISALIGHT est KVWCWCDZOWQF et qu'on a utilisé la correspondance standard entre lettres et nombres modulo 26 : $A \leftrightarrow 0$, $B \leftrightarrow 1$,..., $Z \leftrightarrow 25$. Déterminez :*

1. *la dimension de la matrice de chiffrement,*
2. *la matrice de chiffrement,*
3. *son déterminant,*
4. *la matrice inverse et*
5. *déchiffrez le mot DZNNEY.*

Exercice 2 (modes opératoires) *On considère des blocs de n bits et on suppose que E_k et D_k sont des fonctions de chiffrement et déchiffrement sur n bits. On introduit deux modes dits OFB et CFB pour transmettre m blocs $p_1, \ldots, p_m$ de n bits.*

mode OFB *On fixe un vecteur de n bits IV. On calcule m blocs $c_1, \ldots, c_m$ comme suit :*

$$z_0 = IV, \quad z_i = E_k(z_{i-1}), \quad c_i = E_k(p_i \oplus z_i), \quad 1 \leq i \leq m \ .$$

mode CFB *On fixe un vecteur IV de n bits. On calcule m blocs $c_1, \ldots, c_m$ comme suit :*

$$c_0 = IV, \quad c_i = E_k(c_{i-1}) \oplus p_i, \quad 1 \leq i \leq m \ .$$

Dans le cours nous avons étudié les modes ECB et CBC. Dans ECB on a : $c_i = E_k(p_i)$, pour $i = 1, \ldots, m$. Dans CBC on a : $c_0 = IV$ et $c_i = E_k(c_{i-1} \oplus p_i)$ pour $i = 1, \ldots, m$. On peut mettre en série *les modes opératoires où chaque mode utilise une clef différente. Par exemple le mode $(ECB \mid CBC)$ est le suivant en supposant que k est la clef pour ECB et k' celle pour CBC :*

$$c_0 = IV, \quad c_i = E_{k'}(c_{i-1} \oplus E_k(p_i)), \quad 1 \leq i \leq m \ .$$

1. *Le récepteur connaît la clef k. Pour les modes OFB et CFB décrits ci-dessus expliquez comment en recevant la suite $IV, c_1, \ldots, c_m$ il peut déterminer la suite $p_1, \ldots, p_m$.*
2. *Supposez que le bloc c_i ne soit pas transmis correctement. Que se passe-t-il du point de vue du récepteur dans les modes OFB et CFB ?*
3. *Explicitez la définition du mode $(CBC \mid CFB)$ et expliquez comment le récepteur des blocs chiffrés peut calculer les textes clairs correspondants.*

Exercice 3 (RSA faible) *Supposons que Bob utilise le chiffrement RSA avec un module n assez grand pour qu'il soit impossible de le factoriser. Supposons qu'Alice envoie à Bob un message dans lequel chaque caractère alphabétique est représenté par un nombre de 0 à 25 (A par 0, B par 1,...) chiffré séparément. Décrire comment un attaquant passif peut facilement décrypter un message chiffré avec cette méthode.*

Exercice 4 (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 5 (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.*