Université de Nice-Sophia Antipolis
M2 IFI, parcours CSSR

Cryptographie & Sécurité 2011–2012

Examen de février 2012

Nom :

Prénom :

Durée : 2h

Note :

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

1 Codage de Huffman

Une source qui émet 6 symboles a donné lieu à l'arbre de Huffman décrit dans la figure 1. Le symbole est un nœud de l'arbre et les lettres du codage sont sur les arêtes.

4 → 0
3 → 11
E → 1000
F → 1001
1 → 1010
2 → 1011

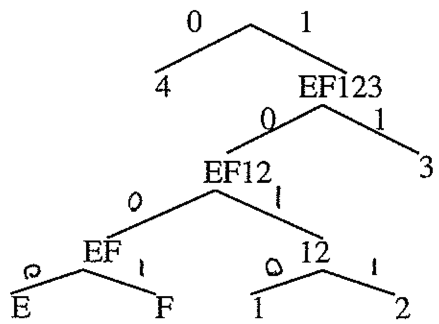

FIGURE 1 – Arbre de Huffman.

1. Décodez le signal suivant (lu de la gauche vers la droite) :

0 1 1 0 1 0 1 1 0 1 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 0

4 3 4 2 4 F 4 E 4 3 4 1

C B O N C A

On rappelle ci-dessous les valeurs hexadécimales du code ASCII des lettres majuscules :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
41	42	43	44	45	4~~4~~6	47	48	49	4a	4b	4c	4d	4e	4f
P	Q	R	S	T	U	V	W	X	Y	Z	␣			
50	51	52	53	54	55	56	57	58	59	5a	20			

6 caractères

ASCii 7 bits → 42 bits
8 bits → 48 bits

2. Quel était le texte avant compression ?

CBONCA

Si on recode la version compressée (avec un bourrage de tête par des 0), bit de poids faible à droite, on obtient la chaîne hexadécimale : `1ad286a`.

3. Calculez le rapport de compression lorsque la donnée brute et la donnée compressée sont exprimées :

1. en binaire :

(ASCii 8 bits) 6 caractères compressés en 26 bits $|C|/|B| = 26/48 = 0{,}54$

2. en hexadécimal :

$|B| = 12$ hex $|C| = 7$ hex $|C|/|B| = 7/12 = 0{,}58$

Quelle est la donnée compressée la plus intéressante en terme de rapport de compression ?

Il est plus intéressant de considérer la suite binaire.

4. Expliquez pourquoi une opération de compression ne peut pas donner de bon résultat lorsqu'elle est appliquée après le chiffrement.

Un modèle de chiffre parfait est réputé donner une distribution de chiffrés proche de l'aléatoire. Or une suite aléatoire n'est pas compressible. Donc, chiffrer puis compresser ne peut pas donner de bon résultat car l'algo de compression ne peut pas fonctionner convenablement.

2 Hachage compressif

Nous nous intéressons à la construction de Merkle-Hellman d'une fonction de hachage à partir de la fonction de compression définie de la manière suivante :
Soient $b(x)$ et $k(x)$, deux polynômes sur $\mathbb{F}_2[x]$ tels que : $d^\circ(b) \leq 3$ et $d^\circ(k) \leq 1$. On rappelle que ϑ, la représentation polynomiale du mot b de 4 bits : $b_3b_2b_1b_0$ (bit de poids faible à droite) est $b_3x^3 + b_2x^2 + b_1x + b_0$. Notre fonction de compression g prend un mot de 6 bits en entrée et fournit un mot de 2 bits en sortie par l'opération :

$$g(k,b) = \vartheta^{-1}(\vartheta(k) + (\vartheta(b) \mod x^2 + x + 1))$$

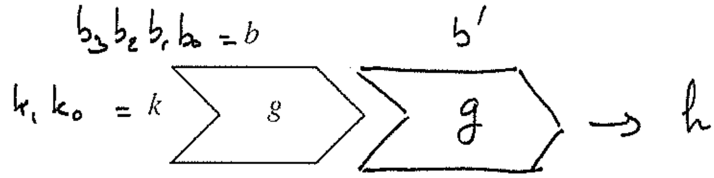

FIGURE 2 – Illustration du fonctionnement de chainage de la fonction de compression

1. Calculez l'empreinte du mot hexadécimal 1a de codage binaire $\overbrace{0\ 0\ 0\ 1}^{1}\ \overbrace{1\ 0\ 1\ 0}^{a}$.

IV = 0 = k On réduit 1 mod $x^2+x+1 = 1$ qui sera la valeur chaînée en entrée de la fonction de compression du bloc b' : $1010 = x^3+x$
On doit réduire $x^3+x+1 \mod x^2+x+1 = x$ car $x^2 = x+1$ et $x^3 = 1$. Le résultat est $\boxed{x = 10}$

On rappelle que $\ln(2) \simeq 0.7$ et que $\sqrt{1+x} \simeq 1 + \frac{x}{2}$.

2. Utilisez le paradoxe des anniversaires pour trouver combien d'entrées il faudrait considérer pour trouver une collision :

- avec une probabilité supérieure à 1/2 :

Les sorties sont sur 2 bits. On cherche $k \geq \sqrt{2 \cdot 4 \ln(2)} \approx 2{,}3$
Il faut donc considérer 3 entrées pour trouver une collision avec proba > 1/2

- avec une probabilité supérieure à 3/4 :

On passe au complémentaire $q = 1/4$. On reprend la formule du cours $2n \ln(1/q) \approx k^2$ avec $q = 1/4$ donc
$k = \sqrt{2n \ln(4)}$ avec $n = 4$
$k \approx 3{,}33$ et il faut considérer 4 entrées pour trouver une collision avec proba > 3/4

3. Dans notre cas, il est plus facile de trouver une collision. Expliquez comment en construire une et illustrez votre construction.

On utilise la propriété de la classe d'équivalence mod x^2+x+1
Ainsi, pour une valeur initiale nulle, les messages 1 et x^3 donnent une même empreinte

00 0001 $\rightarrow$ $0+1$ $\rightarrow$ 1

00 1000 $\rightarrow$ $0+x^3\ (x^2+x+1)$ $\rightarrow$ 1.

4. Déduisez de ce qui précède que la fonction de hachage construite à partir de notre fonction de compression n'est pas résistante aux collisions.

Si la fonction de compression n'est pas résistante aux collisions, la fonction de hachage non plus. Nous avons vu comment construire une collision dans la question 3

3 Chiffre parfait

Soit $n > 0$ un entier. Un *carré latin* de rang n est un tableau T de taille $n \times n$ qui contient les entiers $\{1, \ldots, n\}$ tel que chacun de ces n entiers apparaît une fois sur chaque ligne et sur chaque colonne (pour $n = 9$, c'est par exemple la solution d'un problème de sodoku).

1. Donnez un exemple de carré latin de rang 4.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Etant donné un carré latin T de rang n, on lui associe un chiffre pour lequel l'espace des clairs, des chiffrés et des clés est l'ensemble $\{1, \ldots, n\}$. Le clair m est chiffré avec la clé k en lisant le contenu $T[m, k]$ (ligne m, colonne k).

2. En utilisant l'exemple de la question **1.**, donnez un exemple de chiffrement.

On prend $m = 2$ $\quad k = 3$ $\quad T[2,3] = 4$

$\{2\}_3 = 4$

3. Montrez que ce chiffre est parfait en expliquant sous quelles conditions.

On utilise le théorème de Shannon. En effet, $|C| = |K|$ et $Pr(m) > 0$ $\forall m \in P$. Les n clés peuvent être choisies avec la même proba. Il reste à vérifier que $\forall m \in P$ et $\forall c \in C$, il existe une unique clé $k \in K$.

On fixe $m \in P$ et $c \in C$. On considère la colonne m. Par définition d'un carré latin, le nombre c de la colonne m n'apparaît que sur une seule ligne, la ligne k. Alors k est la seule clé qui relie m et c. D'après le théorème de Shannon, le système garantit un secret parfait