Nom: Prénom:

L3 informatique. Sécurité. Partie J.-F. COUCHOT.

Seule une fiche manuscrite recto-verso de format A4 est autorisée. Tout moyen de communication est interdit. Toutes les réponses doivent être justifiées. Sans justification, une réponse est considérée comme fausse.

Présentation du chiffre de Merkle-Hellman

On présente ci-dessous le chiffre de Merkle-Hellman permettant de chiffrer/déchiffrer un mot $m \in \{0,1\}^k$ de k bits. L'algorithme est présenté en 4 étapes.

1. Étape de générations aléatoires d'entiers naturels.
   (a) Génération aléatoire d'une séquence $a = [a_1, \ldots, a_k]$ de k entiers naturels super croissante, c'est-à-dire telle que pour chaque i, $2 \leq i \leq k$,
   $$a_i > a_1 + \cdots + a_{i-1}. \tag{1}$$
   Dit autrement, le $i^{\text{ème}}$ élément a_i est plus grand que la somme $a_1 + \cdots + a_{i-1}$ des éléments qui le précèdent.
   (b) Choix aléatoire d'un entier naturel n tel que celui-ci est supérieur à $a_1 + \cdots + a_k$.
   (c) Choix aléatoire d'un entier naturel l inférieur à n et tel que l et n sont premiers entre eux.
2. Étape de génération des clés de chiffrement K et de déchiffrement K^{-1}.
   (a) La clé $K = [b_1, \ldots, b_k]$ de chiffrement est la séquence des k entiers naturels tels que pour chaque i, $1 \leq i \leq k$ on a :
   $$b_i \equiv l \times a_i \mod (n). \tag{2}$$
   (b) Calcul de l'entier naturel g inverse de l modulo n : en d'autres termes $g \times l \equiv 1 \mod (n)$.
   (c) La clé de déchiffrement est le triplet $K^{-1} = (n, g, [a_1, \ldots, a_k])$.
3. Chiffrement du message $m = [m_1, \ldots, m_k] \in \{0,1\}^k$ selon la clé $K = [b_1, \ldots, b_k]$. Le message chiffré c est est le nombre défini par
   $$c = m_1 \times b_1 + \cdots + m_k \times b_k \tag{3}$$
4. Déchiffrement du message c selon la clé $K^{-1} = (n, g, [a_1, \ldots, a_k])$.
   (a) Calcul de l'entier $p \equiv g \times c \mod (n)$.
   (b) Résolution de l'équation suivante d'inconnues booléennes $x = [x_1, \ldots, x_k]$:
   $$x_1 \times a_1 + x_2 \times a_2 + \cdots + x_k \times a_k = p \tag{4}$$
   Ce système a une et une seule solution, c'est $m = [m_1, \ldots, m_k]$.

Nom: Prénom:

Exercice 1 – Application directe de ce chiffre.

Question 1.1. On considère $k = 4$ et $a = [1, 3, 5, 11]$. Montrer que la séquence a est super croissante.

Question 1.2. L'entier naturel $n = 23$ est choisi. Montrer que l'entier naturel $l = 7$ est un candidat correct pour ce chiffre.

Question 1.3. En utilisant l'algorithme d'Euclide étendu (et pas une autre méthode), montrer que $g = 10$ est bien l'inverse de 7 modulo 23.

Question 1.4. Construire la clé K de chiffrement.

Question 1.5. Montrer que l'on peut chiffrer le mot $m = 1011$ avec cette clé K. Construire alors ce chiffré c.

Question 1.6. Vous recevez l'entier $c' = 36$. Le déchiffrer en appliquant l'étape 4. du chiffre.

Nom: Prénom:

Exercice 2 – Un peu de théorie

Question 2.1. Aurait-on pu prendre la suite des k premières puissances de 2 par rapport à la propriété de super croissance ? Le justifier.

Question 2.2. Aurait-on pu prendre la suite des k première puissances de 2 d'un point de vue sécurité ? Le justifier.

Question 2.3. Est-ce un chiffrement symétrique ? Asymétrique ?

Exercice 3 – Développements

Question 3.1. Donner le code de la fonction `genere_sequence_super_croissante(k)` qui génère une séquence aléatoire super croissante de taille `k`.