Master CSI 1 2024-2025

Cryptologie — 4TCY802U

DST — mardi 13 mai 2025

Documents non autorisés
Le barème est indicatif

1 LFSR ($\approx$ 4 points)

On considère une suite $(s_i)_{i\geqslant 0}$ dont les 12 premiers termes sont $0,0,1,0,0,1,0,0,0,1,1,0$. On suppose que la complexité linéaire de cette suite est $\leqslant 6$.

(a) Trouver le polynôme de rétroaction de cette suite.

(b) Est-il irréductible ?

(c) Quelle est la complexité linéaire de cette suite ?

(d) Quelle est sa période ?

2 Variante de Rabin ($\approx$ 4 points)

On considère le chiffrement de Rabin avec pour clef publique un entier RSA N. La clef privée est la donnée de deux nombres premiers distincts p et q tels que $N = pq$ et $p \equiv q \equiv 3 \pmod 4$. Pour un message $m \in \mathbf{Z}$, avec $1 < m < N$ et m premier avec N, le chiffré est

$$c = \left(m^2 \mod N, \left(\frac{m}{N}\right), k\right),$$

avec $k = 0$ si $m < N/2$ et $k = 1$ sinon.

(a) Décrire un algorithme de déchiffrement et montrer qu'il retourne bien m sans ambiguïté.

(b) On suppose que $p = 23$, $q = 31$.
- — Calculer toutes les racines carrées de 1 modulo $N = pq$.
- — Déchiffrer $c = (140, -1, 1)$.

3 Variante de RSA ($\approx$ 3 points)

On considère la variante suivante du système RSA. La clé secrète du destinataire consiste en les deux nombres premiers distincts p et q, et sa clé publique est l'entier $N = pq$. Le chiffrement du message m modulo N premier avec N est

$$c \equiv m^N \pmod N.$$

On note $a = q^{-1} \mod (p-1)$ et $b = p^{-1} \mod (q-1)$ (on suppose que q est bien inversible modulo $(p-1)$ et p inversible modulo $(q-1)$).

(a) Étant donné un chiffré c de m, montrer que le message m est l'unique entier modulo N tel que $m \equiv c^a \pmod{p}$ et $m \equiv c^b \pmod{q}$.

(b) Application numérique : soient $p = 23$, $q = 29$, $N = 667$ et soit le message chiffré $c \equiv 186 \pmod{667}$. Calculer les exposants a et b, puis s'en servir pour déchiffrer c.

$\boxed{4}$ Pohlig-Hellman ($\approx$ 3 points)

Soit le nombre premier $p = 73$. On admet que $g = 5$ est une racine primitive modulo p. Soit $h = 21$. On désire calculer le logarithme discret x de h en base g par la méthode de Pohlig-Hellman.

(a) On a $h^{36} = (hg^{-1})^{18} = (hg^{-3})^9 = 72$. En déduire la valeur de x modulo 8.

(b) On a $g^{24} = 8$, $h^{24} = 1$ et $h^8 = 8$. En déduire la valeur de x modulo 9.

(c) En déduire la valeur de x.

$\boxed{5}$ ECDSA ($\approx$ 4 points)

On rappelle le schéma de signature ECDSA

- **Paramètres globaux :**
  P un point d'ordre q d'une courbe elliptique
  $H : \{0,1\}^* \to \mathbf{Z}/q\mathbf{Z}$ une fonction de hachage cryptographique
- **Génération de clef :** $pk := Q := xP$ avec x aléatoire $0 < x < q$, $sk := x$
- **Signature de m avec la clef x :**
  r aléatoire, $0 < r < q$, $R := (x_R, y_R) := rP$, si $x_R \mod q = 0$, recommencer avec un autre r.
  $s = r^{-1}(x(x_R \mod q) + H(m)) \in \mathbf{Z}/q\mathbf{Z}$. Si $s = 0$, recommencer avec un autre r.
  La signature est $\sigma := (\sigma_1, \sigma_2) := (x_R \mod q, s)$.
- **Vérification d'une signature (σ_1, σ_2) de m avec la clef $pk = Q$**
  $u_1 :\equiv H(m)\sigma_2^{-1} \pmod{q}$; $u_2 :\equiv \sigma_1\sigma_2^{-1} \pmod{q}$; $(x_1, y_1) := u_1P + u_2Q$
  La signature est correcte si $\sigma_1 \equiv x_1 \pmod{q}$

(a) À quoi sert un algorithme de signature ? Pourquoi utiliser un tel algorithme utilisant des courbes elliptiques plutôt qu'un algorithme similaire utilisant des corps finis ?

(b) Montrer que si $\sigma = (\sigma_1, \sigma_2)$ est la sortie de la procédure de signature d'un message m avec la clef privée x alors la procédure de vérification appliquée à σ, m et la clef publique $Q = xP$ déclare que σ est valide (indication : montrer que le point (x_1, y_1) calculé dans la vérification est égal au point R calculé dans la procédure de signature).

(c) Dans cette question, on considère une mauvaise implantation de la procédure de signature dans laquelle le nombre r n'est pas choisi aléatoirement mais est choisi toujours égal à la même valeur (inconnue). On suppose disposer de deux messages m, m', avec $m \neq m'$, et de leurs signatures σ et σ' créées par cette implantation en utilisant la même clef secrète de signature x. Montrer que l'on peut retrouver x en temps polynomial.

(d) Supposons dans cette question avoir trouvé un message m tel que $H(m) = 0$. Montrer qu'il est possible de calculer efficacement (en temps polynomial) une signature ECDSA valide de m sans connaître la clef secrète x.

(e) Dans cette question, on suppose que la fonction de hachage utilisée, H, est remplacé par l'identité : $H = Id : \{1, \dots, n-1\} \to \{1, \dots, n-1\}$. Montrer qu'il est possible de calculer efficacement une signature d'un message non maîtrisé $m \in \{1, \dots, n-1\}$ sans connaître la clef secrète. Indication : au lieu de $R = rP$ calculé lors de la procédure de signature, considérer un point $R = aP + bQ$ pour certains a, b et bien choisir ensuite les valeurs de s et m.

$\boxed{6}$ Signatures BLS ($\approx$ 4 points)

Soient q un grand nombre premier et $(G, +)$ et $(G_t, \times)$ deux groupes cycliques d'ordre q. On note P un générateur de G et $e : G \times G \to G_t$ un couplage cryptographique symétrique (de type 1).

Soit H une fonction de hachage cryptographique qui à une chaîne de bit quelconque m associe $H(m) \in G$. On rappelle le fonctionnement du système de signature BLS. La clef secrète de signature est un entier $1 < x < q$ aléatoire. La clef publique de vérification est le point $Q = xP \in G$. La signature d'une chaîne de bit m avec la clef secrète x est $\sigma = xH(m) \in G$.

(a) Rappeler quels sont les propriétés d'un tel couplage cryptographique.

(b) Quel problème précis doit résoudre un attaquant pour calculer une signature BLS de m sans connaître la clef secrète x ? En déduire l'algorithme de vérification de ce système de signature.

Soit $n > 1$ un entier. Dans la suite de l'exercice, on suppose que n personnes utilisent ce schéma de signature BLS. Pour $i = 1, \dots, n$, on note x_i avec $1 < x_i < q$, la clef secrète de l'utilisateur i et $Q_i = x_i P \in G$ sa clef publique. Soit $m_1, \dots, m_n$ des messages. Pour $i = 1, \dots, n$, on note $\sigma_i \in G$ la signature par l'utilisateur i du message m_i avec le système de signature BLS.

(c) Montrer comment combiner les signatures $\sigma_1, \dots, \sigma_n$ en un seul élément σ de G de telle manière qu'il soit possible étant donné σ, les messages $m_1, \dots, m_n$ et les clefs publiques $Q_1, \dots, Q_n$ de vérifier que σ est bien une combinaison de signatures par les utilisateurs 1 à n des messages $m_1, \dots, m_n$. Donner cette procédure de vérification.

(d) Soit m un message non signé par l'utilisateur 1. Montrer qu'un attaquant peut faire croire qu'il a signé avec l'utilisateur 1 ce message m : autrement dit, montrer qu'un attaquant sans connaître ni x_1 ni la signature par l'utilisateur 1 de m, peut construire une clef publique Q_a et $\sigma \in G$ de telle manière que l'entrée σ, m, m, Q_1, Q_a soit acceptée par la procédure de vérification donnée à la question précédente. Proposer une défense contre cette attaque.