Master CSI 1 2023-2024

Cryptologie — 4TCY802U

DST — vendredi 3 mai 2024

Documents non autorisés

1 LFSR

On considère une suite $(s_i)_{i\geqslant 0}$ dont les 12 premiers termes sont $1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0$. 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

Dans une variante du système de Rabin, la clef publique est un couple (N, b) et la clef privée est la factorisation $N = pq$, où p et q sont deux nombres premiers distincts. Pour un message $M \in \mathbf{Z}/N\mathbf{Z}$, le chiffré est

$$C = M(M + b) \mod N.$$

(a) Décrire un algorithme de déchiffrement, retournant un des messages clairs possibles.

(b) On suppose que $p = 23$, $q = 47$ et $b = 60$.
- Calculer toutes les racines carrées de 1 modulo N.
- Calculer le chiffré associé au message en clair $M = 111$.
- Quels sont tous les clairs possibles pour le chiffré trouvé précédemment ?

3 Chiffrement RSA

Alice et Bob utilisent le système RSA avec le même modulo N mais avec des exposants publics e_A et e_B distincts. On supposera que e_A et e_B sont premiers entre eux. On suppose qu'un même message M est envoyé à Alice et Bob sous forme chiffrée, et qu'un observateur Oscar intercepte les deux chiffrés $C_A = M^{e_A} \mod N$ et $C_B = M^{e_B} \mod N$.

(a) Montrer comment Oscar peut retrouver facilement M à partir de C_A et C_B.

(b) Le faire explicitement, sans factoriser N, pour les valeurs $N = 11021$, $e_A = 7$, $e_B = 13$, $C_A = 5342$ et $C_B = 348$.

4 Signatures RSA-FDH

On utilise les notations habituelles N, e, d de RSA. On désigne par h une fonction de hachage cryptographique de $\{0,1\}^*$ dans $(\mathbf{Z}/N\mathbf{Z})^\times$. On rappelle le protocole de signature RSA-FDH : pour signer une chaîne de bits m, avec sa clef privée d, Alice calcule $\sigma :\equiv h(m)^d \pmod N$.

(a) Quelle est la clef publique de vérification ? Quelle est la procédure de vérification de signature ?

(b) Alice utilise $(N, e, d) = (143, 7, 103)$. Vérifier que ce choix convient.

(c) Alice a signé un message m, dont le haché est $h(m) = 79$, obtenant la signature $\sigma = 118$ avec RSA-FDH. Vérifier que cette signature est correcte, avec les paramètres de la question précédente.

Dans la suite on considère des valeurs N, e, d quelconques. On suppose dans les trois questions suivantes qu'Alice n'utilise pas de fonction de hachage : l'espace des messages est $(\mathbf{Z}/N\mathbf{Z})^\times$ et $\sigma = m^d \mod N$.

(d) Oscar récupère les signatures valides σ_1 et σ_2 de deux messages $m_1, m_2 \in (\mathbf{Z}/N\mathbf{Z})^\times$, signés par Alice. Montrer comment Oscar peut construire la signature valide d'un autre message.

(e) Oscar souhaite obtenir la signature valide d'Alice d'un certain $m \in (\mathbf{Z}/N\mathbf{Z})^\times$, signifiant « Alice doit 1000 € à Oscar ». Montrer, en utilisant la question précédente, comment Oscar peut arriver à ses fins en demandant à Alice de signer deux messages apparemment anodins.

(f) Montrer comment Oscar peut construire un message (possiblement sans sens, contrefaçon existentielle) et sa signature valide, sans interaction avec Alice.

On suppose maintenant, dans toute la suite, que l'on utilise une fonction de hachage cryptographique h de $\{0,1\}^*$ dans $(\mathbf{Z}/N\mathbf{Z})^\times$ en suivant le protocole RSA-FDH.

(g) Quelles propriétés de h évitent les deux attaques précédentes ?

(h) On suppose que h n'est pas résistante à la seconde pré-image. Oscar récupère la signature valide σ d'un message m. Montrer comment Oscar peut construire une signature valide pour un message différent de m.

5 Logarithme discret

Soit p un nombre premier et soit g un élément primitif modulo p. Soit $h = g^x \mod p$ où $x \in \{0, 1, \ldots, p-1\}$. On suppose h connu et l'on s'intéresse à déterminer x. Soit $x_{\ell-1} \ldots x_1 x_0$ l'écriture en base 2 de x, c'est à dire $x = \sum_{i=0}^{\ell-1} x_i 2^i$.

(a) Montrer qu'il est possible de trouver en un temps de calcul raisonnable la parité de x, c'est-à-dire le bit x_0.

(b) On suppose dans la suite que $p \equiv 3 \pmod 4$. Montrer que si $x_0 = 0$ et que si vous disposez d'un algorithme qui vous calcule efficacement la valeur de x_1, alors vous pouvez calculer efficacement la valeur de $g^{x/2}$.

(c) En déduire que si vous disposez d'un algorithme efficace qui, étant donné tout $f = g^a \bmod p$ vous donne le deuxième bit a_1 de a dans son écriture binaire ($a = \sum_{i=0}^{\ell-1} a_i 2^i$), alors vous pouvez construire un algorithme efficace qui calcule x à partir de h. Décrire l'algorithme.

6 Un système de chiffrement utilisant les couplages

Soient p_1 et p_2 deux grands nombres premiers distincts et $N = p_1 p_2$. Soit $(G, +)$ et $(G_t, \times)$ deux groupes cycliques d'ordre N. On note P un générateur de G et $Q \in G$ un élément d'ordre p_1.

On note $e : G \times G \to G_t$ un couplage cryptographique symétrique, c'est à dire une application bilinéaire non dégénérée calculable efficacement.

On considère le schéma de chiffrement asymétrique suivant. La clef publique est constituée de P, Q et N, ainsi que la description des groupes G et G_t. Soit B un entier et $m \in \{0, \ldots, B\}$. Pour chiffrer m, on choisit un entier r aléatoire avec $1 < r < N$, et on calcule le chiffré C par $C = mP + rQ$ dans G.

(a) Donnez une clef privée et un algorithme de déchiffrement permettant de retrouver m à partir de C. Comment choisir la borne B pour que le déchiffrement reste efficace ?

(b) On note C un chiffré de m et C' un chiffré de m'. Montrez que sans connaître la clef privée, on peut obtenir un chiffré de $m + m'$.

(c) Même question pour obtenir un chiffré de $m \times m'$: il n'aura pas exactement la même forme que C et C', mais il faut pouvoir toujours le déchiffrer efficacement. Comment ?

(d) Quels problèmes peut on résoudre pour retrouver la clef privée à partir de la clef publique ?