TD1 : Cryptographie

Exercice 1

Rappeler les quatre niveaux d'attaque d'un système cryptographique. Expliquer comment casser un code de César dans chacun de ces niveaux.

Exercice 2

Compléter les affirmations suivantes :

1. Pour chiffrer un message, Arielle utilise la clé de .
2. Pour déchiffrer un message, Arielle utilise la clé de .
3. Pour signer un message, Arielle utilise la clé de sur un hash du message.
4. Pour authentifier un message, Arielle déchiffre le hash avec la clé de et compare au .

Exercice 3

Soit p un nombre premier et $a \in \mathbb{Z}/pZ^*$.

1. Combien vaut $a \times 2a \times \cdots \times (p-1)a$?
2. On note r_i le reste dans la division de $i \times a$ par p. Montrer que si $r_i = r_j$ alors $i = j$.
3. En déduire que $a^{p-1} = 1$ modulo p.

Exercice 4

Arielle et Bertrand utilisent le protocole de Diffie-Hellman avec $n = 719$ et $g = 3$. Arielle choisit $a = 16$.

1. Quelle valeur Arielle envoie-t-elle à Bertrand ?
2. Bertrand répond 543. Quelle est la valeur finale partagée par Arielle et Betrand ?

Exercice 5

Arielle et Bertrand communiquent en utilisant le cryptosystème d'El Gamal avec $p = 719$, $g = 3$.

1. La clé privée d'Arielle est $x = 4$. Quelle est sa clé publique ?
2. Chiffrer le message $m = 25$ quand l'entier aléatoire est $r = 3$.
3. Déchiffrer le résultat pour vérifier.

Exercice 6

Arielle et Bertrand communiquent en utilisant le cryptosystème RSA.

1. Si $pq = 77$, donner cinq valeurs possibles pour d.
2. Si $pq = 403$ et $d = 7$, déterminer e.
3. Chiffrer $m = 25$.
4. Déchiffrer le résultat pour vérifier.

Exercice 7

Un cryptosystème est dit malléable si un attaquant peut modifier le chiffré d'un message m afin d'obtenir le chiffré du message $f(m)$ (sans avoir à déchiffrer le message).

On fixe un entier t et la fonction $f : m \to t \times m$. Dans cet exercice, on ne considère que des messages dans $\mathbb{N}$.

1. Montrer que le cryptosystème El-Gamal est malléable en expliquant comment un attaquant peut appliquer f à un message, en ne connaissant que (la clé publique et) le message chiffré.
2. Même question pour RSA.
3. (À méditer) Pourquoi la malléabilité pose problème ? Comment s'en prémunir ?