Module TR-c8

TD N° 1 – Notions de Base en Cryptographie

Exercice 1 – Cryptage par transposition

Rappel : Le principe du système de cryptage *Vigenère* est relativement simple. Dans un tableau, dit *carré de Vigenère*, on remplace la lettre du message à chiffrer par la lettre obtenue à l'intersection de la colonne repérée par cette lettre, et de la ligne définie par la lettre de la clé associée à la lettre du message.

Pour chiffrer **Pour déchiffrer**

- Chiffrez le texte "CESTBIENTOTFINI" avec le code à transposition par la clé "SOURT".
- Retrouver le clair du crypte "LEDCITMHGMMZWRGII" codé avec le système de cryptage *Vigenère* et à l'aide de la clé "SECRET".

Exercice 2 – Systèmes à clés symétriques ou secrètes

Un système de messagerie sécurisé met en relation un groupe de N utilisateurs. Le groupe souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système symétrique de chiffrement. Ainsi, chaque utilisateur doit connaître la clé secrète de chacun des autres membres du groupe.

1. Quel est le nombre minimal de clés symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique (à clé publique).

3. Quel le nombre minimal de paires de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent au même groupe). Quelle(s) clé(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est à dire qui utilise la cryptographie symétrique et asymétrique).

6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Exercice 3 – Signature et cryptage

Bob a publié un puzzle et propose une bouteille de vin à la première personne qui arrive à le résoudre. Cette personne s'appelle Alice et veut envoyer la solution M à Bob signé mais aussi crypté. Pour cela Alice utilise la *cryptographie et la signature à clé publique*. On notera par C_B la clé publique de Bob et par D_A la clé privée d'Alice.

1. Dans quel ordre Alice doit signer et chiffrer pour être sûr de recevoir la bouteille de vin ? Est-ce qu'il vaut mieux que Alice envoie $\mathbf{C_B}(M),\mathbf{D_A}(\mathbf{C_B}(M))$ ou $\mathbf{C_B}(M,\mathbf{D_A}(M))$?

Exercice 4 – Perte d'une clé privée

Alice, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-elle encore envoyer des courriers électroniques chiffrés ? En recevoir ?
2. Peut-elle encore signer les courriers électroniques qu'elle envoie ? Vérifier les signatures des courriers électroniques qu'elle reçoit ?
3. Que doit-elle faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?