Sécurisation des communications

Capacités attendues : Décrire les principes de chiffrement symétrique (clef partagée) et asymétrique (avec clef privée/clef publique).

1. Le chiffre de César

Le chiffre de César est une méthode simple de chiffrement par décalage. Dans ce chiffre, chaque lettre du texte est remplacée par une autre lettre située un certain nombre de positions plus loin dans l'alphabet. Par exemple, avec un décalage de 3, "A" deviendrait "D", "B" deviendrait "E", etc.

Chiffrer le texte suivant en utilisant un décalage de 3 :
"BONJOUR"

2. Le chiffre de substitution

Le chiffre de substitution est une méthode où chaque lettre du message est remplacée par une autre, mais cette fois de manière plus aléatoire, selon une clé secrète. Contrairement au chiffre de César, il n'y a pas de décalage fixe.

Chiffrer le texte "**CRYPTAGE**" en utilisant la table de substitution suivante (chaque lettre de l'alphabet est remplacée par une autre) :

A → Q	H → I	O → G	V → C
B → W	I → O	P → H	W → V
C → E	J → P	Q → J	X → B
D → R	K → A	R → K	Y → N
E → T	L → S	S → L	Z → M
F → Y	M → D	T → Z	
G → U	N → F	U → X	

3. Le chiffre de Vigenère

Le chiffre de Vigenère est un chiffre par substitution, mais avec une clé qui varie. Au lieu de décaler chaque lettre du texte de manière fixe (comme dans le chiffre de César), le décalage dépend des lettres de la clé. Ce chiffre est plus sécurisé, car il utilise une clé qui se répète pour chaque lettre du message.

La clé est un mot ou une phrase, et chaque lettre de ce mot détermine le décalage pour la lettre correspondante du texte. Par exemple, si la clé est "CLE", on utilise le décalage de "C" (qui est 3), puis celui de "L" (qui est 11), puis "E" (qui est 4), et cela se répète.

Chiffrer le texte suivant avec la clé "**CLE**" en utilisant le chiffre de Vigenère : "**SECURITE**"

4. Le hachage (hashing)

Le hachage est une méthode utilisée pour vérifier l'intégrité des données, c'est-à-dire pour vérifier si des données ont été modifiées de manière non autorisée. Un algorithme de hachage transforme un message en une valeur de longueur fixe appelée "empreinte" ou "hash". Cette empreinte est unique pour chaque message, ce qui permet de vérifier si le message a été altéré.
L'algorithme de hachage que nous allons utiliser ici est le plus simple pour l'exercice, appelé **MD5**. Il génère une chaîne de 32 caractères hexadécimaux.

5. La cryptographie asymétrique (RSA)

La cryptographie asymétrique utilise une paire de clés : une clé publique et une clé privée. La clé publique est utilisée pour chiffrer les données, et la clé privée est utilisée pour les déchiffrer. Un des systèmes les plus connus pour cela est l'algorithme RSA.
Imaginons que l'on veuille envoyer un message secret à quelqu'un en utilisant RSA. La personne à qui est envoyé le message possède une clé publique, et l'envoyeur utilise cette clé pour chiffrer son message. Seule la personne possédant la clé privée correspondante pourra déchiffrer le message.

Exemple simple de chiffrement RSA avec de petits nombres pour illustrer la méthode.
Imaginons les paramètres suivants pour une clé RSA :
- Clé publique (e = 7, n = 33)
- Clé privée (d = 3, n = 33)

Le message que l'on veut envoyer est le nombre "**4**". En RSA, on chiffre un message **m** en utilisant la formule suivante :

$$c = m^e \bmod (n)$$

où :

- m est le **message clair** (sous forme d'entier),
- c est le **message chiffré** (le *chiffre*),
- e est l'**exposant de chiffrement** (clé publique),
- n est le **modulo**, produit de deux grands nombres premiers p et q,
- mod signifie « modulo » : on prend le reste de la division

Chiffrer le message "**4**" avec la clé publique (e = 7, n = 33).

Vérifier en appliquant la formule de déchiffrement : **$m = c^d \bmod (n)$**
Et la clé privée précédente.

6. Sécurisation (exercice tiré du sujet NSI 2024 - Métropole J2)

La base de données de Bob est hébergée sur un serveur auquel il accède depuis un client sur son ordinateur personnel. Pour sécuriser la connexion, un algorithme de chiffrement symétrique est utilisé.

1. Expliquer brièvement ce qu'est un algorithme de chiffrement symétrique.

La clé de chiffrement, notée C dans la suite, est choisie aléatoirement par le serveur à chaque connexion depuis un client. Afin que le chiffrement et le déchiffrement puisse se faire sans problème, le serveur doit envoyer au client la clé C de façon sécurisée.

2. Rappeler brièvement ce qu'est un algorithme de chiffrement asymétrique.

On suppose à présent que Bob possède une clé publique et une clé privée. La clé publique de Bob est supposée connue par le serveur.

3. Proposer alors une solution pour que le serveur puisse envoyer la clé C à l'ordinateur de Bob de façon sécurisée, c'est-à-dire pour que seul Bob puisse déchiffrer la clé envoyée.

Pour que le serveur puisse envoyer à Bob la clé C, il faut que le serveur chiffre le message (la clé C) avec la clé publique de Bob.
A réception, Bob déchiffrera le message avec sa clé privé et récupérera la clé C