EXERCICES SUR LES NOTIONS DE CHIFFREMENT

Exercice 1 : Chiffrement par décalage
Objectif :
Appliquer un code César simple.
Énoncé :

1. Chiffrez le mot **CHAT** avec une clé x=3 (décalage de 3).
2. Déchiffrez le mot **FDWFK** avec la même clé.

Exercice 2 : Identifier le décalage
Objectif :
Comprendre le fonctionnement du décalage dans le chiffrement.
Énoncé :
Le mot **MAISON** a été chiffré en **OGKUQP**. Trouvez la clé utilisée pour le chiffrement.

Exercice 3 : Chiffrement asymétrique simplifié
Objectif :
Simuler un chiffrement avec clé publique et déchiffrement avec clé privée.
Énoncé :

1. Chiffrez le mot **VOITURE** avec la clé publique x=5 en utilisant le code César.
2. Déchiffrez le résultat obtenu avec la clé privée X=21 (rappel : X=26−x).

Exercice 4 : Briser un code César
Objectif :
Faire découvrir la faiblesse du code César par attaque brute force.
Énoncé :
Le mot chiffré est **QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD**.

1. Essayez toutes les clés possibles pour retrouver le texte clair.
2. Indiquez quelle clé permet de retrouver un message compréhensible.

Indice :
Il s'agit d'un texte en anglais.

Exercice 5 : Créer son propre message chiffré
Énoncé :

1. Choisissez un mot ou une phrase simple.
2. Chiffrez-la avec une clé publique x=7.
3. Échangez votre texte chiffré avec un camarade, qui devra le déchiffrer avec la clé privée X=19X=19 (rappel : X=26−x).

Exercice 6 : Analyser un système asymétrique simplifié
Objectif :
Comprendre le principe de sécurité d'un chiffrement asymétrique.
Énoncé :

1. Expliquez pourquoi il est possible de partager la clé publique x avec tout le monde, mais pourquoi la clé privée X doit rester secrète.
2. Si un attaquant connaît la clé publique x=4 et intercepte le mot chiffré **MZPP**, peut-il le déchiffrer sans la clé privée X=22 ?