Codes secrets — Exercices Physique 9e HarmoS

Exercice 1

Chiffre de César : On numérote les 26 lettres de l'alphabet de 0 (`A`) à 25 (`Z`). Chiffrer avec une clé k consiste à décaler chaque lettre de k rangs vers la droite modulo 26 : $C \equiv (M + k) \pmod{26}$.

1. Chiffrer le mot **`PHYSIQUE`** avec la clé $k = 5$.
2. Déchiffrer le message **`HTWWNLJ`**, sachant qu'il a été chiffré avec la même clé $k = 5$.

Voir la réponse et le corrigé détaillé sur le site

Exercice 2

Vous interceptez le message chiffré suivant, codé par un chiffre de César avec une **clé k inconnue** :

`UN LQROOAN MN LNBJA NBC BRVYUN`

1. En français, quelle est la lettre la plus fréquente ? Repérer la lettre qui apparaît le plus souvent dans ce message chiffré.
2. En déduire la clé de décalage k, puis décoder intégralement le message.

Voir la réponse et le corrigé détaillé sur le site

Exercice 3

Un **chiffrement affine** transforme le rang $x \in \{0, \dots, 25\}$ d'une lettre en $y \equiv a \cdot x + b \pmod{26}$.

1. Avec la fonction $y \equiv 3x + 4 \pmod{26}$, chiffrer le mot **`BANC`**.
2. Pourquoi ne peut-on **jamais** choisir $a = 2$ (par exemple $y \equiv 2x + 4 \pmod{26}$) pour fabriquer un code secret ? Tester sur les lettres `A` (0) et `N` (13).

Voir la réponse et le corrigé détaillé sur le site

Exercice 4

Code de Vigenère (chiffrement) : Contrairement au chiffre de César qui applique toujours le même décalage, le code de Vigenère utilise un **mot-clé répété** sous le message. Chaque lettre du mot-clé donne le décalage à appliquer ($A = 0, B = 1, \dots, Z = 25$).

Chiffrer le mot **`OPTIQUE`** à l'aide de la clé **`LUX`**.

Voir la réponse et le corrigé détaillé sur le site

Exercice 5

Code de Vigenère (déchiffrement) :

1. Déchiffrer le message **`HFTKAP`**, chiffré par le code de Vigenère avec la clé **`SOL`**.
2. Expliquer pourquoi la lettre `A` du texte chiffré (`HFTK A P`) et la lettre `T` (`HF T KAP`) ne proviennent pas de la même lettre ni du même décalage, ce qui protège ce code contre une attaque fréquentielle simple.

Voir la réponse et le corrigé détaillé sur le site

Exercice 6

Chiffrement par transposition (scytale) : Au lieu de remplacer les lettres, on change leur ordre. On écrit un message sans espaces dans un tableau de 4 **lignes et** 5 **colonnes** (ligne par ligne), puis on le lit **colonne par colonne** (de haut en bas, puis de gauche à droite) pour former le message chiffré.

Déchiffrer le message suivant de 20 lettres : > **`VSAEIELRTDUEEEMXSLIX`**

(Les `X` à la fin servent uniquement à compléter la dernière ligne.)

Voir la réponse et le corrigé détaillé sur le site

Exercice 7

Grille tournante (grille de Fleissner) : On utilise un pochoir carré 4×4 percé de 4 trous aux cases de coordonnées `(ligne, colonne)` suivantes (numérotées de 1 à 4 de haut en bas et de gauche à droite) :

- $(1,1)$, $(1,3)$, $(2,2)$ et $(3,1)$.

Pour chiffrer un message de 16 lettres, on pose la grille sur une feuille 4×4, on écrit les 4 premières lettres dans les trous (ligne par ligne, de gauche à droite), puis on fait tourner la grille d'un **quart de tour ($90°$) dans le sens horaire** et on écrit les 4 lettres suivantes, et ainsi de suite.

1. Vérifier qu'au bout de 4 positions ($0°, 90°, 180°, 270°$), aucune case n'est utilisée deux fois.
2. Déchiffrer le message inscrit dans la grille finale ci-dessous :

S	I	O	L
F	L	B	I
E	O	L	R
R	L	T	E

Voir la réponse et le corrigé détaillé sur le site

Exercice 8

Masque binaire (ou exclusif XOR) : En cryptographie moderne, on travaille sur des bits (0 et 1) à l'aide de l'opération **XOR** (notée $\oplus$), définie par :

$$0 \oplus 0 = 0 \quad ; \quad 0 \oplus 1 = 1 \quad ; \quad 1 \oplus 0 = 1 \quad ; \quad 1 \oplus 1 = 0$$

On code chaque lettre par son rang ($A = 0, B = 1, \ldots, Z = 25$) écrit en binaire sur 5 **bits**.

1. Sachant que `L` $= 11 = (01011)_2$, `U` $= 20 = (10100)_2$ et `X` $= 23 = (10111)_2$, chiffrer le mot **`LUX`** avec la clé binaire `00010 01011 00100` (qui correspond à `CLE`).
2. Expliquer pourquoi l'opération de déchiffrement est **strictement identique** à celle du chiffrement (calculer $(M \oplus K) \oplus K$).

Voir la réponse et le corrigé détaillé sur le site

Exercice 9

Initiation à la cryptographie asymétrique (échange de clé de Diffie–Hellman) :

Alice et Bob veulent fabriquer un **code secret commun** en communiquant uniquement sur un canal public où un espion écoute tout. Ils choisissent publiquement les nombres $p = 23$ et $g = 5$.

- **Alice** choisit secrètement $a = 6$, calcule $A \equiv 5^6 \pmod{23}$ et l'envoie publiquement à Bob.
- **Bob** choisit secrètement $b = 4$, calcule $B \equiv 5^4 \pmod{23}$ et l'envoie publiquement à Alice.

1. Calculer les valeurs publiques A et B envoyées par Alice et Bob.
2. Alice calcule ensuite $K_A \equiv B^a \pmod{23}$ et Bob calcule $K_B \equiv A^b \pmod{23}$. Vérifier qu'ils obtiennent la **même clé secrète** K.
3. Pourquoi l'espion qui connaît p, g, A, B a-t-il du mal à retrouver K lorsque p est un très grand nombre premier (de plusieurs centaines de chiffres) ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 10

Initiation au principe du chiffrement RSA :

Pour créer ses clés RSA, Alice choisit deux nombres premiers $p = 3$ et $q = 11$.

1. Calculer le module public $n = p \times q$ et l'indicateur d'Euler $\varphi(n) = (p-1)(q-1)$.

2. Alice choisit comme exposant de chiffrement $e = 3$ et comme exposant secret $d = 7$. Vérifier que la condition clé du système RSA est satisfaite : $e \times d \equiv 1 \pmod{\varphi(n)}$.
3. Bob veut envoyer le message secret $M = 5$ à Alice en utilisant la **clé publique** $(n; e) = (33; 3)$. Calculer le message chiffré $C \equiv M^e \pmod{n}$.
4. À l'aide de sa **clé privée** $d = 7$, Alice déchiffre en calculant $C^d \pmod{33}$. Vérifier étape par étape qu'elle retrouve bien $M = 5$.

Voir la réponse et le corrigé détaillé sur le site

Exercice 11

Un message a été chiffré par le chiffre de César avec une clé $k = 3$ (chaque lettre est décalée de 3 rangs vers la droite dans l'alphabet).

1. Déchiffrer le message `PDWKV`.
2. Chiffrer le mot `ZERO` avec la même clé.

Voir la réponse et le corrigé détaillé sur le site

Exercice 12

Le **code Atbash** (utilisé dans l'Antiquité) remplace chaque lettre par sa « symétrique » dans l'alphabet : `A` $\leftrightarrow$ `Z`, `B` $\leftrightarrow$ `Y`, `C` $\leftrightarrow$ `X`, etc. En numérotant les lettres de 0 (`A`) à 25 (`Z`), la lettre de rang x devient celle de rang $25 - x$.

1. Chiffrer le mot `SOLEIL`.
2. Que se passe-t-il si l'on chiffre deux fois un message ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 13

En français, la lettre la plus fréquente est le `E`. Dans un long texte chiffré avec le chiffre de César, on constate que la lettre la plus fréquente est le `I`.

1. Quelle est probablement la clé utilisée ?
2. Déchiffrer alors le mot `QEXLW`.
3. Pourquoi le chiffre de César est-il facile à casser, même sans analyse de fréquences ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 14

Le **chiffrement affine** transforme la lettre de rang x (de 0 pour `A` à 25 pour `Z`) en la lettre de rang y, reste de la division de $3x + 5$ par 26.

1. Chiffrer le mot `CODE`.
2. Avec la fonction $2x + 1$ à la place de $3x + 5$, chiffrer `A` et `N`. Pourquoi ce choix de clé est-il mauvais ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 15

Le **carré de Polybe** remplace chaque lettre par deux chiffres (ligne puis colonne) dans la grille suivante (`I` et `J` partagent la même case) :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1. Chiffrer le mot `PHYSIQUE`.

2. Déchiffrer `32 15 43 45 42 15`.

Voir la réponse et le corrigé détaillé sur le site

Exercice 16

En code Morse, chaque lettre est une suite de points (·) et de traits (−). Extrait de l'alphabet :

$$\text{A} = \cdot - \quad \text{M} = - - \quad \text{O} = - - - \quad \text{S} = \cdots \quad \text{T} = - \quad \text{E} = \cdot$$

1. Déchiffrer : $\cdot - \ / \ - \ / \ - - - \ / \ - -$
2. Coder le signal de détresse `SOS`.
3. Pourquoi les lettres les plus courantes, comme `E` et `T`, ont-elles les codes les plus courts ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 17

Le numéro ISBN-10 d'un livre comporte 9 chiffres suivis d'une clé de contrôle c. La règle est : en multipliant les chiffres par $10, 9, 8, \ldots, 2$ et la clé par 1, la somme obtenue doit être un multiple de 11.

1. Calculer la clé c du numéro 2-07-036024-c.
2. Un chiffre a été mal recopié : 2-07-036084-5. Le contrôle détecte-t-il l'erreur ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 18

1. Combien de clés différentes possède le chiffre de César (en excluant le décalage nul) ?
2. Un **chiffrement par substitution** remplace chaque lettre par une autre selon un ordre quelconque (une permutation de l'alphabet). Combien de clés possibles y a-t-il ? En donner un ordre de grandeur.
3. Un ordinateur teste un milliard (10^9) de clés par seconde. Combien de temps lui faut-il, environ, pour tester toutes les clés de substitution ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 19

En informatique, le code **ASCII** associe un nombre à chaque caractère : `A` = 65, `B` = 66, …, `Z` = 90. Ces nombres sont stockés en binaire sur 7 bits.

1. Écrire `A` en binaire sur 7 bits.
2. Déchiffrer le message binaire : 1001000 1001001.

Voir la réponse et le corrigé détaillé sur le site

Exercice 20

Pour détecter des erreurs de transmission, on ajoute à chaque groupe de 7 bits un **bit de parité** : on le choisit pour que le nombre total de 1 (sur les 8 bits) soit **pair**.

1. Quel bit de parité faut-il ajouter à 1011001 ?
2. On reçoit les octets 10110101 et 01100110. Lequel contient certainement une erreur ?
3. Ce procédé détecte-t-il toutes les erreurs ?

Voir la réponse et le corrigé détaillé sur le site

Exercice 21

Chiffre LUNE par un décalage de quatre positions vers la droite, avec retour à A après Z.

Voir la réponse et le corrigé détaillé sur le site

Exercice 22

Déchiffre IHG si le chiffrement avance chaque lettre de trois positions.

Voir la réponse et le corrigé détaillé sur le site

Exercice 23

Deux décalages successifs de 18 et 11 positions s'appliquent sur 26 lettres. Donne le décalage équivalent entre 0 et 25.

Voir la réponse et le corrigé détaillé sur le site

Exercice 24

Avec A = 1 à Z = 26, décode 13 5 18.

Voir la réponse et le corrigé détaillé sur le site

Exercice 25

Un code écrit les lettres de rang impair puis celles de rang pair, dans leur ordre initial. Code PLANETE.

Voir la réponse et le corrigé détaillé sur le site

Exercice 26

Pour décoder AOUPMN, remets les trois premières lettres aux rangs impairs et les autres aux rangs pairs.

Voir la réponse et le corrigé détaillé sur le site

Exercice 27

Un code inverse l'ordre des lettres dans chaque bloc de trois. Décode REMLAC.

Voir la réponse et le corrigé détaillé sur le site

Exercice 28

Avec le code A $\leftrightarrow$ Z, B $\leftrightarrow$ Y, C $\leftrightarrow$ X, etc., chiffre NEIGE.

Voir la réponse et le corrigé détaillé sur le site

Exercice 29

En Morse, A = .-, N = -., T = -, E = . Les barres isolent les lettres. Décode « -. / .- / - / . ».

Voir la réponse et le corrigé détaillé sur le site

Exercice 30

Dans un code de César, C devient J. Donne le décalage vers la droite entre 0 et 25.

Voir la réponse et le corrigé détaillé sur le site