Exercice 1 : Le carré de Polybe

- **Chiffrement**

Chiffrez **à la main** le texte suivant avec le carré de Polybe (sans mot-clef):
L'homme est un ange déchu qui se souvient du ciel.

322335 333315 154445 513411 342215 141323 514251 244415 443551 522415 344514 511324 1532

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

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

- **Déchiffrement**

Déchiffrez **à la main** le texte suivant avec le carré de Polybe en utilisant le mot-clef "Blaise Pascal":
122115 141221 412321 214521 44412 112242 123211 521152 213232 115144 125144 114153 521252 544131 421
LE SILENCE ETERNEL DE CES ESPACES INFINIS M EFFRAIE

Exercice 2 : Le chiffre Playfair

- **Chiffrement**

Chiffrez **à la main** le texte suivant en Playfair avec la clef "Charles Baudelaire":
Souvent pour s'amuser, les hommes d'équipage Prennent des albatros, vastes oiseaux des mers.

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

Grille

BNSYS MYMPB HUCOD BUCCD FSPNT IBEPD JMBOU MCUOV MSMVE SBHAD CXAPF HHBCI BNFEB CBYES ENUCE H

- **Déchiffrement**

Déchiffrez **à la main** le texte suivant en Playfair avec la clef "Charles Baudelaire":
PDFEE JTSMV FMBQC DMVEH PNORF OPOBE STPXB ODCSM HXJCB ICKBV BHMVB DLCSB OXSJJ HSBCO UCEH

QUI SUIVENT INDOLENTS COMPAGNONS DE VOYAGE LE NAVIRE GLISXSANT SUR LES GOUFFRES AMERS C

Exercice 3: Le chiffre de Vigenère

- Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "Jeanne-Marie":
Jeanne-Marie a des mains fortes, Mains sombres que l'été tanna

SIAAA IYAIQ IJHEF ZEUNJ NSAXE FZEUN JASVF RRFUG ECMXN XAAAE

- Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "Jeanne-Marie":
VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE

MAINS PALES COMME DES MAINS MORTES SONT CE DES MAINS DE JUANA

Exercice 4 : Donner le chiffré du message «the big bang theory» en utilisant les systèmes de chiffrement suivants :
a) César
b) Chiffrement mono-alphabétique à clé (clé : TELECOM)
c) Chiffrement par transposition à clé (clé : TELECOM)
d) Affine y= ax+b (mod26), clé :(a, b) = (17,1). Quelle est la clé utilisée si A est chiffré par G et E est chiffré par A ?

Solution

a) Chiffrement de César (avec décalage de 3 lettres)

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

Texte Clair : **THE BIG BANG THEORY**
Texte chiffré : QEB YFD YXKD QKBLOV

b) Chiffrement mono-alphabétique à clé (clé : TELECOM)

La clé nettoyée est : **TELCOM**
Mettre « le mot clé en premier » puis compléter les lettres de l'alphabet.

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

Texte Clair : **THE BIG BANG THEORY**
Texte chiffré : SBO EDA ETJA SBOKQY

c) Chiffrement par transposition à clé (clé : TELECOM)

T	**E**	**L**	**E**	**C**	**O**	**M**
7	**2**	**4**	**3**	**1**	**6**	**5**
T	H	E	B	I	G	B
A	N	G	T	H	E	O
R	Y					

Texte chiffré : IHH NYB TEGB OGETAR

d) Chiffrement Affine : y= ax+b (mod26)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On cherche la clé (a,b) pour que A → G et E → A ?
Chaque lettre est remplacée par le chiffre lui correspondant dans le tableau :
A : 0 / G : 6 / E : 4
Equation 1 : y= ax+b (mod26) → 6= b (mod26) (1)
Equation 2 : y= ax+b (mod26) → 0= 4a+b (mod26) (2)
À partir de (1) on a : b=6
On remplace dans (2) : 0= 4a+6 (mod26)
Pour résoudre cette équation, nous allons d'abord soustraire 6 des deux côtés :

$$4a = -6 \pmod{26} \quad (3)$$

Ensuite, nous devons trouver un a tel que 4a soit congru à −6 modulo 26.

En cherchant les multiples de 4 jusqu'à trouver −6 modulo 26, nous trouvons que a=5 fonctionne, car 4×5=20, ce qui est congru à −6 modulo 26.
Donc, la solution du système est a=5 et b=6.
Si on vérifie à nouveau l'équation y= ax+b (mod26) on trouve que A → G et E → A.