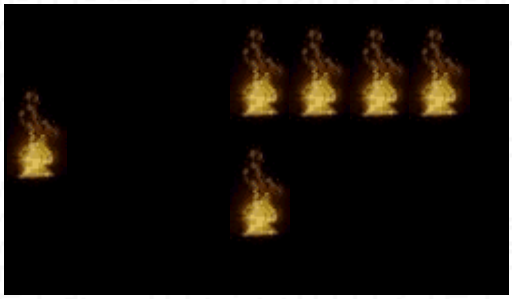
Le carré de Polybe: chiffre monalphabétique

Polybe, historien grec (env. 200 - 125 av. J.-C.), est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases (on peut agrandir ce carré à 36 cases, afin de pouvoir ajouter les chiffres - voir le "chiffre ADFGVX" - ou pour chiffrer des alphabets comportant davantage de lettres, comme l'alphabet cyrillique):

	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



Transmission de la lettre "e"

En français, on supprime le **W**, qui sera le cas échéant remplacé par V. **En anglais,** on agrège le **I** et le **J**.
Chaque lettre peut être ainsi représentée par un groupe de deux chiffres: celui de sa ligne et celui de sa colonne. Ainsi "e"=15, "u"=51, "n"=34, ...
Polybe proposait de transmettre ces nombres au moyen de torches. Une torche à droite et cinq à gauche pour transmettre la lettre "e" par exemple. Ce procédé permettait donc de transmettre des messages sur de longues distances. On peut aussi transmettre les coordonnées des lettres en tapant des coups sur un mur, sur la tuyauterie, etc.

Les cryptologues modernes ont vu dans le "carré de 25" plusieurs caractéristiques extrêmement intéressantes:

- la conversion de lettres en chiffres,
- la réduction de nombres, de symboles,
- la représentation de chaque lettre par deux éléments séparés.

On peut compliquer ce système de chiffrement avec un mot de passe. Par exemple, si le mot de passe est *DIFFICILE*, on commencera à remplir le carré avec les lettres de ce mot, après avoir supprimé les lettres identiques, puis on complètera le tableau avec les lettres inutilisées (voir les "alphabets désordonnés"). On obtiendra alors:

	1	2	3	4	5
1	d	i	f	c	l
2	e	a	b	g	h
3	j	k	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

Plusieurs chiffres modernes s'inspirent du carré de Polybe: le chiffre de Delastelle, le chiffre ADFGVX, le chiffre des Nihilistes, la méthode Hayhanen, ...

Exercices

Exercice 1: Théorie

Proposez une manière de remplir le carré de Polybe qui minimise le nombre de coups à frapper sur les murs (pour la langue française).

Combien y a-t-il de carrés de Polybe optimaux équivalents?

Exercice 2: 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.

Exercice 3: 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 chiffre bifide de Delastelle: Chiffres tomogrammiques

Le chiffre bifide de Delastelle - du nom de son inventeur, le Français **Félix-Marie Delastelle** (1840-1902), qui en avait décrit pour la première fois le principe dans la "Revue du Génie civil" en 1895, sous le nom de "cryptographie nouvelle" - utilise une grille de chiffrement/déchiffrement analogue à celle du chiffre de Polybe. Il repère les coordonnées de plusieurs lettres claires, mélange ces coordonnées, puis lit dans la grille les lettres chiffrées correspondant aux nouvelles coordonnées obtenues. Ce procédé est dit tomogrammique. Le *Traité élémentaire de cryptographie* de Delastelle, seul cryptographe civil important de l'époque, fut publié chez Gauthier-Villars en 1902.

Méthode de chiffrement

1. On choisit d'abord la longueur de séries *n*.
2. On regroupe les lettres du message clair *n* par *n* (au besoin, on rajoute des nulles pour que la longueur du message soit un multiple de *n*).
3. Sous chaque lettre, on note les coordonnées des lettres verticalement (p. ex. J=21, E=45)
4. On lit ensuite horizontalement les coordonnées des lettres chiffrées (24=U, 44=V, 21=J), série par série.

Exemple

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

Grille de chiffrement

n=5

clair	j	e	v	o	u	s	a	i	m	e
1er digit	2	4	4	4	2	2	3	4	5	4
2e digit	1	5	4	2	4	2	2	3	3	5

Coordonnées chiffrées	24	44	21	54	24	23	45	42	23	35
Message chiffré	U	V	J	H	U	F	E	O	F	X

Déchiffrement

Le déchiffrement s'effectue en sens inverse: on écrit horizontalement les coordonnées des lettres chiffrées, et on lit verticalement les coordonnées des lettres claires. La lettre claire correspondante est trouvée sur la grille.

Pour former les grilles de chiffrement, on utilise un **mot-clef secret** pour créer un alphabet désordonné avec lequel on remplissait la grille ligne par ligne.

Exercices

Exercice 1: Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Delastelle en utilisant le mot-clef "**recueillement**": Sois sage, ô ma douleur, et tiens-toi plus tranquille.
Tu réclamais le Soir; il descend; le voici.

Exercice 2: Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Delastelle en utilisant le mot-clef "recueillement":

EETDY TYDBQ RUDEB SRRGE ESMDL PJNPL AEAAR EIEYG APCUB MMTXJ TLZQX LVIOY LITER IJECO IZZFF
