Cipher (chiffre)

Un « cipher » est un algorithme permettant de modifier un message pour le transmettre en masquant son contenu si on ignore le moyen d'inverser la modifier du message.
Il existe deux grandes familles :

- Cipher à **transposition** : les caractères du message sont mélangés en suivant l'algorithme.
- Cipher à **substitution** : les caractères du message sont remplacés par des symboles déterminés.

Il est possible de cumuler les deux méthodes pour obtenir un message d'autant plus caché.

Chiffres connus

César (caesar) : Transposition
La méthode est très simple, il s'agit de décaler les lettres de l'alphabet en fonction d'une clef prédéfinie :

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

```
NouveauCaractere = Valeur(Id(AncienCaractere)+Clef)
```

Exemple

Clef = 5
Encodage de « message cache »

m	e	s	s	a	g	e		c	a	c	h	e
12	4	18	18	0	6	4		2	0	2	7	4

↓ + 5

17	9	23	23	5	11	9		7	5	7	12	9
r	j	x	x	f	l	j		h	f	h	m	j

message cache ⇒ rjxxflj hfhmj

On dispose de seulement 25 clefs possibles ce qui limite énormément les possibilités d'encodage et rend le message caché très vulnérable à une attaque brute force.

Playfair : Substitution
La méthode consiste à prendre une clef que l'on va mettre dans une matrice 5 × 5, on va rentrer les caractères dans l'ordre donné mais on ne va jamais dupliquer de valeur. Si on a déjà rentré la lettre « A » alors on n'entrera plus de « A » même si la clef en contient un autre. Puis on remplit le reste de la matrice avec les lettres de l'alphabet (non sorties) dans l'ordre alphabétique. Imaginons que nous prenions la clef « polytechnice » :

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

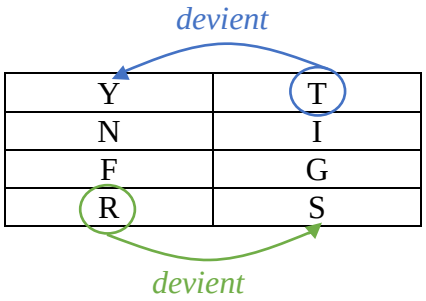
Une fois que l'on dispose de notre clef on va pouvoir encoder un message, pour cela prenons le message : « transmetteur en panne »

1. On va grouper les caractères en paires en ignorant les espaces, séparant les doubles par des « X » et en rajoutant un « X » à la fin si nécessaire :
   ```
   TR AN SM ET XT EU RE NP AN XN EX
   ```

2. On va alors se servir de la clef pour trouver comment encoder le message. Pour chaque couple de caractères on va créer un « rectangle » sur notre clef avec les valeurs et utiliser les valeurs opposées :

TR :

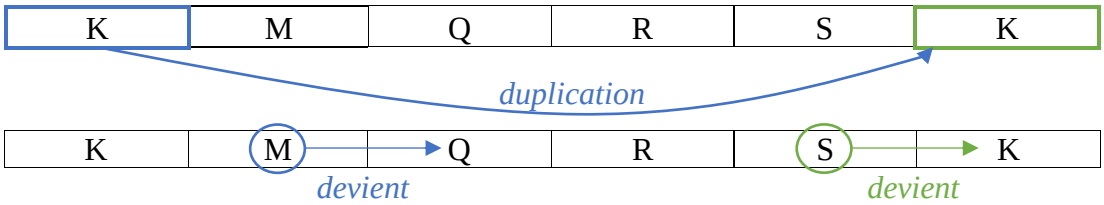
P	O	L	Y	T
E	C	H	N	I
A	B	D	F	G
K	M	Q	R	S
U	V	W	X	Z



TR ⇒ YS

3. Lorsque les deux caractères sont sur la même ligne alors on décale à droite et la ligne la plus à gauche est « dupliquée » à droite (on fait de même avec haut et bas sauf qu'on décale vers le bas) :

SM :



SM ⇒ KQ

On a donc :

`transmetteur en panne ⇒ TRANSMETXTEURENPANXNEX ⇒ YSFEKQIPZYAPKNEYFEYFNU`

Cryptage (encryption)

Un cipher (chiffre) est une version basique d'un chiffrement, ou cryptage. Pour effectuer un cryptage il faut que la lecture soit impossible pour toute personne ne disposant pas la clef de déchiffrement. Une **clef** de **cryptage** peut être :

- **Symétrique** : on dispose d'une unique clef, qui sert à chiffrer et à déchiffrer.
- **Asymétrique** : on dispose de deux clefs, la clef de chiffrement est publique alors que celle servant au déchiffrement est privée.

La protection apportée par un algorithme de chiffrement est liée à la longueur de la clef (définie le nombre maximal d'opérations nécessaires au décryptage).

Les algorithmes symétriques sont beaucoup plus rapides que les algorithmes asymétriques. Cela vient du fait que les algorithmes symétriques reposent sur des manipulations du *plaintext* via une clé de cryptage donnée (comme des permutations, XOR, multiplications, sur des petits nombres) alors que les algorithmes asymétriques, quant à eux, utilisent des fonctions mathématiques complexes et lentes, comme l'utilisation de modulos et des puissances sur de très grands nombres.

Exemple

Cryptage RSA : Asymétrique

On dispose des paramètres suivants :

$$p = 37 \qquad q = 89 \qquad e = 19 \qquad d = 667$$

On va alors créer notre **clef publique**, $\mathbf{K^+}$, que l'on va partager, et notre **clef privée**, $\mathbf{K^-}$, que l'on va garder pour nous :

$$\begin{cases} p = 37 \\ q = 89 \end{cases} \qquad \begin{cases} e = 19 \\ d = 667 \end{cases}$$

$$\begin{cases} K^- = \{19, 37 \times 89\} = \{19, 3293\} \\ K^+ = \{667, 37 \times 89\} = \{667, 3293\} \end{cases}$$

Cryptage :

On va chercher à crypter le message suivant : « SophiaAntipolis »

1. En utilisant la position dans l'alphabet, cela revient à crypter (on ignore l'espace) :
   `19 15 16 08 09 01 01 14 20 09 16 15 12 09 19`
2. En utilisant des blocs de longueur 3, on obtient :
   `191 516 080 901 011 420 091 615 120 919`
3. On calcule alors :

$$191^{667} \bmod 3293 = 1289$$
$$516^{667} \bmod 3293 = 1445$$
$$\text{etc…}$$

SophiaAntipolis ⇒ 1289 1445 2917 1689 2490 690 1463 3159 2525 6

Décryptage :

On va chercher à décrypter : « 1289 1445 2917 1689 2490 690 1463 3159 2525 6 »

$$1289^{19} \bmod 3293 = 191$$
$$1445^{19} \bmod 3293 = 516$$
$$\text{etc…}$$

1289 1445 2917 1689 2490 690 1463 3159 2525 6 ⇒
191 516 080 901 011 420 091 615 120 919

On a bien le même message.