TD CRYPTO

LE CHIFFRE DE CÉSAR

aussi appelée **chiffrement par décalage**, consiste à décaler chaque lettre d'un message par la lettre de l'alphabet située à une distance fixée. Par exemple, si la distance est 3, la lettre A est remplacée par la lettre D, la lettre B par E, etc. ; et la lettre Z par C.

> Par exemple, le message clair :
>
> ATTAQUEZ A L AUBE
>
> est transformé en utilisant le chiffre de César avec une distance de 3, en le texte chiffré :
>
> DWWDTXHC D O DXEH

La **distance** est un **nombre compris entre 0 et 25.**

LE CARRÉ DE POLYBE

Une technique de substitution où les lettres sont remplacées par une paire de chiffres correspondant à leur position dans une grille 5x5.

Exemple :

On utilise une grille 5x5 pour les 25 lettres de l'alphabet (on fusionne généralement I et J).

	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

> Par exemple, le message clair :
>
> CHAT
>
> on remplace chaque lettre par les coordonnées correspondantes :
>
> C -> 13
> H -> 23
> A -> 11
> T -> 44
>
> Le message chiffré est donc : 13 23 11 44.

LE CHIFFRE DE VIGENÈRE

Il reprend en partie le principe de substitution, mais en variant la distance de décalage au cours du chiffrement en utilisant **un mot ou une phrase comme clé.** Chaque lettre de la clé correspond à sa position dans l'alphabet. Pour chiffrer un message, on écrit le texte clair et on écrit la clé en dessous, en répétant la clé autant de fois que nécessaire pour couvrir l'ensemble du message.

Par conséquent :

- le chiffrement consiste à additionner chaque lettre du message avec la lettre de la clé en dessous, modulo 26 ;
- le déchiffrement consiste à soustraire chaque lettre du message chiffré avec la lettre de la clé en dessous, modulo 26.

On a donc comme résultat la table de Vigenère suivante :

	Lettre en clair																									
	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**
Lettre de la clé	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																									
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	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
X	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
Y	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	X
Z	Z	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

> Par exemple, avec la clé "RABELAIS" et le message clair suivant on obtient le texte chiffré :
>
> SCIENCE SANS CONSCIENCE N EST QUE RUINE DE L AME
>
> - RABELAIS RABELAIS RABELAIS RABELAIS RABELAIS
>
> = JCJIYCM KRNT GZNAUZEOGP N MKK QVI CUQFV DF P LMM

LE CHIFFRE DE VERNAM

Le chiffre de Vernam, également connu sous le nom de chiffre à masque jetable (One Time Pad), s'agit d'une amélioration du chiffre de Vigenère, où la clé utilisée pour chiffrer le message est aussi longue que le message lui-même et est entièrement aléatoire.

1. **Clé aléatoire** :
   - Une clé aléatoire est générée, de la même longueur que le message à chiffrer.
   - Cette clé est utilisée une seule fois (d'où le nom de "masque jetable").
2. **Chiffrement** :
   - Chaque lettre du message en clair est combinée avec la lettre correspondante de la clé à l'aide de l'opération XOR (ou "OU exclusif"), qui est une opération binaire.
   - Dans le cas de textes, cette opération est réalisée en convertissant chaque lettre en sa représentation binaire (bits), puis en appliquant le XOR bit à bit.
   - Exemple :
     - Message en clair : "CHAT"
     - Clé aléatoire : "XMCK"
     - C -> XOR avec X -> résultat : une nouvelle lettre
     - H -> XOR avec M -> résultat : une nouvelle lettre
     - A -> XOR avec C -> résultat : une nouvelle lettre
     - T -> XOR avec K -> résultat : une nouvelle lettre
   - Le message chiffré est une séquence de lettres apparemment aléatoires.
3. **Déchiffrement** :
   - Le déchiffrement est réalisé de la même manière que le chiffrement : le message chiffré est combiné avec la clé aléatoire à l'aide de l'opération XOR.
   - Étant donné que le XOR d'une valeur avec elle-même donne toujours zéro, et que le XOR d'une valeur avec zéro redonne la valeur initiale, le message original est restauré.

LES CONGRUENCES

Si l'on considère un alphabet de 26 lettres, le chiffre de César peut être formalisé comme suit :
$C = (P + k) \ mod \ 26$
où C est la lettre chiffrée, P la lettre en clair, et k le décalage.