HISTOIRE DE LA CRYPTOGRAPHIE

DE

L'ANTIQUITE

A

NOS JOURS

TERMINOLOGIE

CRYPTOLOGIE : la science des documents secrets. elle recouvre tous les aspects scientifiques, et plus particulièrement mathématiques, relatifs à la cryptologie et à la cryptanalyse

CRYPTANALYSE : l'art et la science de décrypter les messages secrets

CHIFFREMENT : le processus de transformation d'un message de telle manière à le rendre incompréhensible pour toute personne non autorisée

CRYPTOGRAMME : le résultat du processus de chiffrement

DÉCHIFFREMENT : le processus de reconstruction du texte clair à partir du texte chiffré, par des personnes autorisées

DÉCRYPTEMENT : le processus de reconstruction du texte clair à partir du texte chiffré, par des personnes non autorisées (sans connaître la clef)

CLEF DE CHIFFREMENT : un mot, un nombre ou une phrase qui est utilisé par un algorithme de cryptologie pour chiffrer ou déchiffrer un message

STÉGANOGRAPHIE : la dissimulation du message dans un ensemble de données d'apparence anodine.

COURS Eii – Cryptographie
M. Bonneton

CHRONOLOGIE

César

Polybe

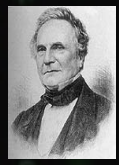
Al Kindi

Trithème

Vigenère

Porta

Bacon



Alberti

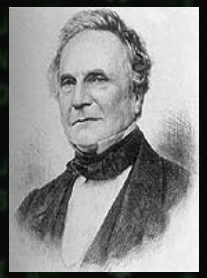
Cardan

-100 000 100 200 300 400 500 600 700 800 900 1000 1100 1200 1300 1400 1500 1600 1700 1800 1850 1900

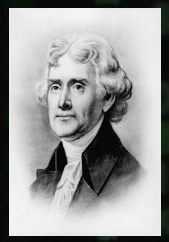
CHRONOLOGIE


Wheatstone


Painvin


Babbage

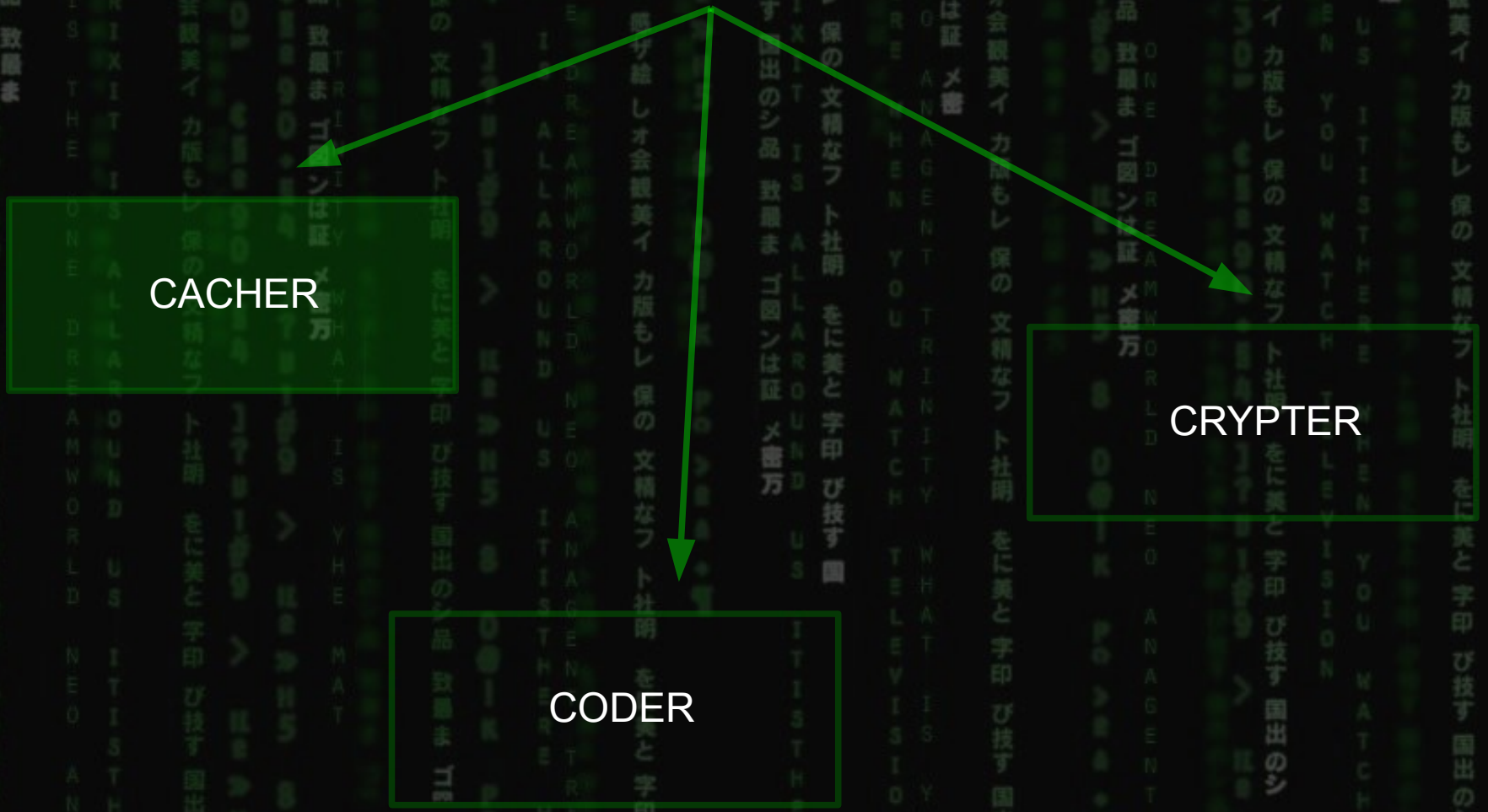

Bazeries


Jefferson


Turing

1700 1750 1800 1850 1900 1950

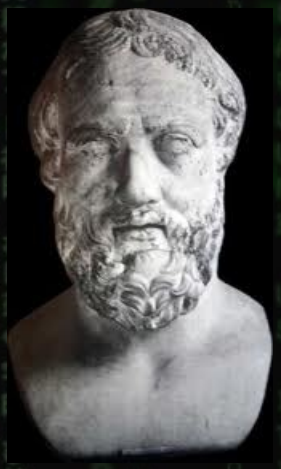
DIFFERENTES STRATEGIES



PREMIERE STRATEGIE : CACHER

LA STEGANOGRAPHIE

En grec «l'écriture couverte», elle cache les messages dans un support, par exemple des images ou un texte qui semble anodin. On noie le message dans un autre et seuls certains mots doivent être lus pour découvrir le texte caché.



Hérodote
(- 500)

« Histiée, voulant prendre contact secrètement avec son gendre, le tyran Aristagoras de Milet, choisit un esclave dévoué, lui rasa la tête, et y inscrivit le message à transmettre. Il attendit que ses cheveux repoussent pour l'envoyer à Aristagoras avec l'instruction de se faire raser le crâne. »

« Pour informer les Spartiates de l'attaque imminente des Perses, un certain Démarate utilisa un élégant stratagème : il prit des tablettes, en racla la cire et grava sur le bois le message secret, puis il recouvrit les tablettes de cire. De cette façon, les tablettes, apparemment vierges, n'attirèrent pas l'attention. »

PREMIERE STRATEGIE : CACHER

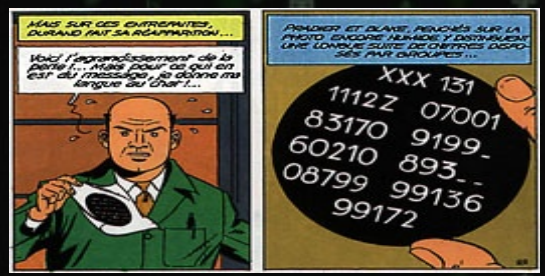
LA STEGANOGRAPHIE

En Chine ancienne, on écrivait les messages sur une fine soie dont on faisait une petite boule en l'englobant dans de la cire. Le messager avalait ensuite cette boule.

Au XVIe siècle, Giovanni Porta découvrit comment cacher un message dans un oeuf dur. Il suffit d'écrire sur la coquille avec une encre contenant une once d'alun pour une pinte de vinaigre ; la solution pénètre la coquille et dépose sur la surface du blanc d'oeuf le message que l'on lira aisément après avoir épluché l'oeuf.

Enée le Tacticien imagina d'envoyer un message secret en piquant de minuscules trous sous certaines lettres d'un texte anodin. La succession de ces lettres fournit le texte secret. Les espions allemands de la deuxième guerre mondiale utilisaient aussi des micropoints pour faire voyager discrètement leurs informations. C'est une photographie de la taille d'un point de ponctuation, qu'il suffit d'agrandir pour voir apparaître clairement le message.

SOS Météores d'Edgar P. Jacobs



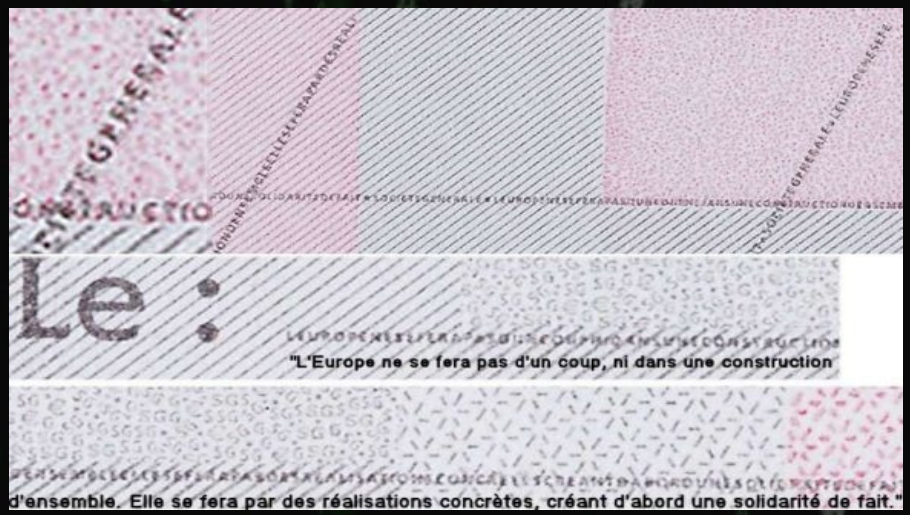
PREMIERE STRATEGIE : CACHER

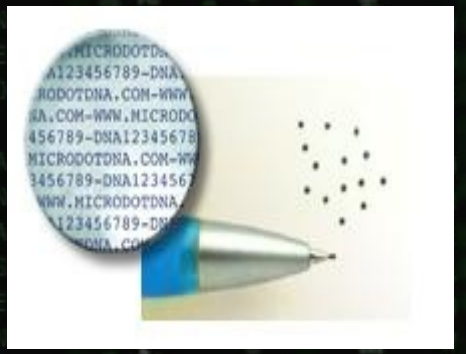
LA STEGANOGRAPHIE

On trouve un exemple de stéganographie élémentaire sur tous les billets de banque suisses.

L'image « SA Zurich » a été obtenue en agrandissant fortement le petit carré entouré d'un cercle vert : on a scanné cette partie du billet avec une résolution de 2400 ppi pour voir apparaître le texte (une simple loupe ne permet pas de lire les caractères). C'est une variante du micropoint.

De même, sur nos chéquiers, les lignes sont en fait des phrases. Vérifiez si vous avez un chèque à portée de main.



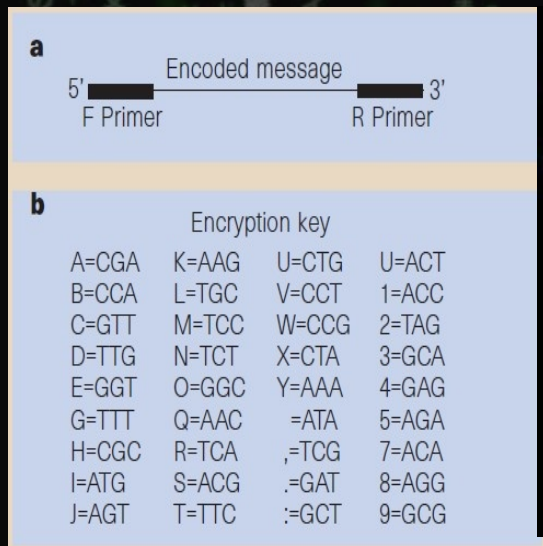


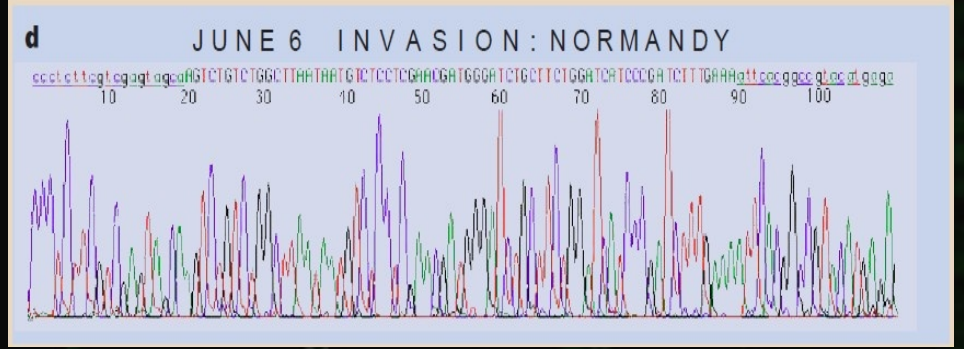
Technologie
MicroDotDNA

PREMIERE STRATEGIE : CACHER

LA STEGANOGRAPHIE

En 1999, Catherine Taylor Clelland, Viviana Risca et Carter Bancroft publient dans la revue Nature «Hiding messages in DNA microdots». Notre matériel génétique est en effet formé de l'enchaînement de quatre nucléotides que l'on peut comparer à un alphabet de quatre lettres : A, C, G et T. Or, les scientifiques sont maintenant capables de fabriquer des chaînes d'ADN avec une suite de nucléotides déterminée à l'avance. Il suffit alors d'attribuer un groupe de trois nucléotides à chaque lettre de l'alphabet, aux chiffres et aux signes de ponctuation (par exemple "A"=CGA, "B"=CCA, etc.) et de composer le «message génétique». Pour brouiller les pistes, on peut ensuite le mélanger avec d'autres séquences aléatoires d'ADN. Le tout est à peine visible au microscope électronique. Comme application, on peut imaginer qu'une compagnie qui produirait une nouvelle espèce de tomate pourrait ainsi inclure sa marque de fabrique dans les molécules de la tomate, afin d'éviter les contrefaçons.





PREMIERE STRATEGIE : CACHER

LES ENCRES SYMPATHIQUES

Pantagruel, chapitre XXIV

Lettres que un messagier aporta à Pantagruel d'une dame de Paris, et l'exposition d'un mot escript en un aneau d'or.

Quand Pantagruel eut leue l'inscription, il feut bien esbahy, et, demandant au dict messagier le nom de celle qui l'avoit envoyé, ouvrit les lettres, et rien ne trouva dedans escript, mais seulement un aneau d'or, avecques un diament en table. Lors appella Panurge et luy monstra le cas.

A quoy Panurge luy dist que la fueille de papier estoit escripte, mais c'estoit par telle subtilité que l'on n'y veoit poinct d'escripture.

Et pour le sçavoir, la mist auprès du feu, pour veoir si l'escripture estoit faicte avec du sel ammoniac destrempé en eau.

Puis la mist dedans l'eau, pour sçavoir si la lettre estoit escripte du suc de tithymalle.

Puis la monstra à la chandelle, si elle estoit poinct escripte du jus de oignons blans.

Puis en frotta une partie d'huile de noix, pour veoir si elle estoit poinct escripte de lexif de figuier.

Puis en frotta une part de laict de femme allaictant sa fille premiere née, pour veoir si elle estoit poinct escripte de sang de rubettes.

Puis en frotta un coing de cendres d'un nic de arondelles, pour veoir si elle estoit escripte de rousée qu'on trouve dedans les pommes de Alicacabut.

Puis en frotta un aultre bout de la sanie des aureilles, pour veoir si elle estoit escripte de fiel de corbeau.

Puis les trempa en vinaigre, pour veoir si elle estoit escripte de laict de espurge.

Puis les gressa d'axunge de souris chauves, pour veoir si elle estoit escripte avec sperme de baleine qu'on appelle ambre gris.

Puis la mist tout doulcement dedans un bassin d'eau fresche et soubdain la tira, pour veoir si elle estoit escripte avecques alum de plume.

Et, voyant qu'il n'y congnoissoit rien, appella le messagier et luy demanda :

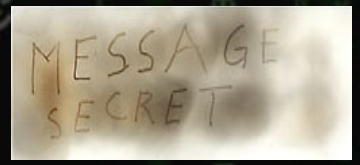
«Compaing, la dame qui t'a icy envoyé t'a elle poinct baillé de baston pour apporter» pensant que feust la finesse que mect Aule Gelle.

Et le messagier luy respondit : «Non, Monsieur.»

Adoncques Panurge luy voulut faire raire les cheveulx, pour sçavoir si la dame avoit faict escripre avecques fort moret sur sa teste rase ce qu'elle vouloit mander ; mais, voyant que ses cheveulx estoyent fort grand, il desista, considerant que en si peu de temps ses cheveulx n'eussent creuz si longs.

François Rabelais

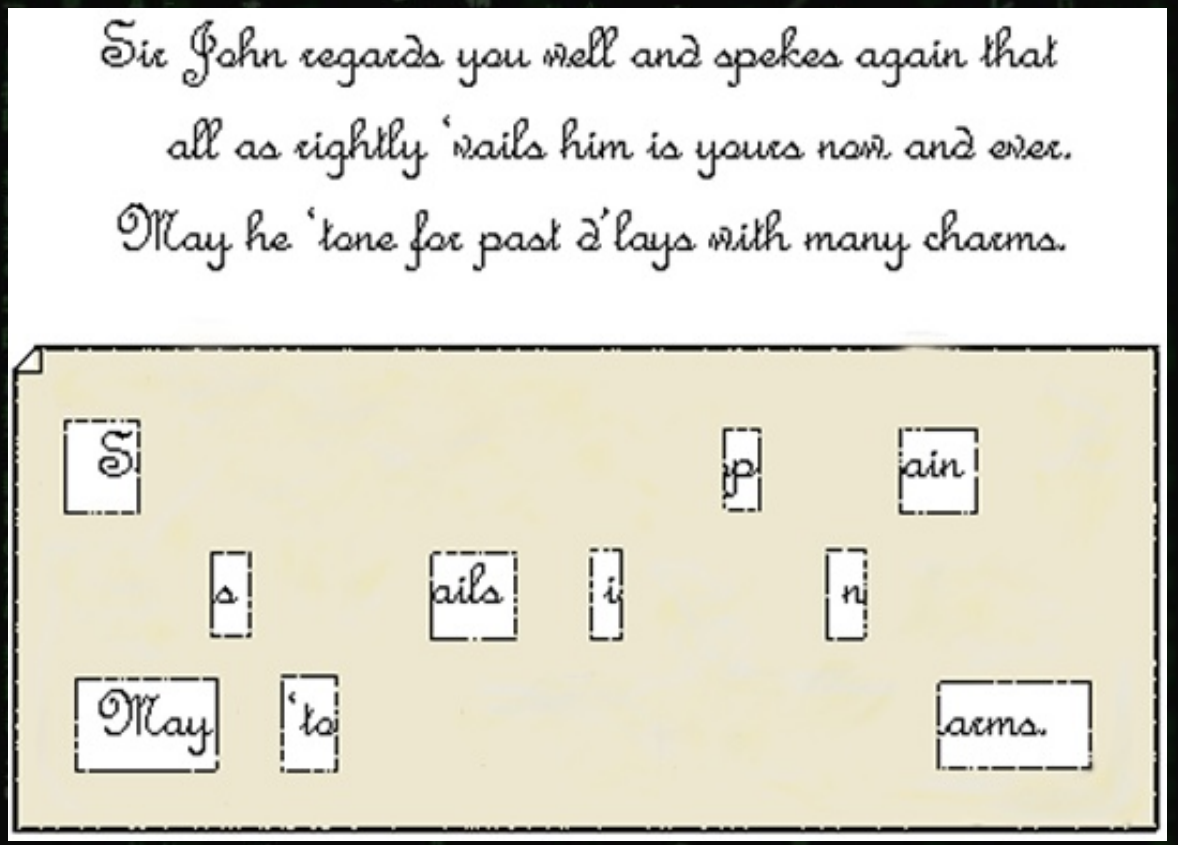
XVI ème



PREMIERE STRATEGIE : CACHER

LA GRILLE DE CARDAN

Jérôme Cardan
(1501-1576)



PREMIERE STRATEGIE : CACHER

LES AVE MARIA DE TRITHEME

Dans la félicité à perpétuité,
Dans son royaume à perpétuité,
En Paradis à perpétuité,
Ainsi qu'en toute éternité;
Dans la gloire à perpétuité,
Mais dans son règne;
Sempiternel, toujours dans la félicité,
Tant dans la lumière que dans la béatitude,
Et dans la gloire à perpétuité,
Mais dans son règne;
En une infinité encore à perpétuité,
Comme dans la gloire autant que dans les Cieux,
A tout jamais, oui ! à tout jamais à perpétuité;
Dans son royaume et dans la félicité,
Irrévocablement, dans son royaume,
Et sans cesse qu'il soit à perpétuité dans la lumière,
Et encore à perpétuité !

A	dans les cieux	N	en paradis
B	à tout jamais	O	toujours
C	un monde sans fin	P	dans la divinité
D	en une infinité	Q	dans la déité
E	à perpétuité	R	dans la félicité
F	sempiternel	S	dans son règne
G	durable	T	dans son royaume
H	sans cesse	U,V,W	dans la béatitude
I,J	irrévocablement	X	dans la magnificence
K	éternellement	Y	au trône
L	dans la gloire	Z	en toute éternité
M	dans la lumière		

DECODER CET AVE MARIA :

PREMIERE STRATEGIE : CACHER

LES AVE MARIA DE TRITHEME

Dans la félicité à perpétuité,
Dans son royaume à perpétuité,
En Paradis à perpétuité,
Ainsi qu'en toute éternité;
Dans la gloire à perpétuité,
Mais dans son règne;
Sempiternel, toujours dans la félicité,
Tant dans la lumière que dans la béatitude,
Et dans la gloire à perpétuité,
Mais dans son règne;
En une infinité encore à perpétuité,
Comme dans la gloire autant que dans les Cieux,
A tout jamais, oui ! à tout jamais à perpétuité;
Dans son royaume et dans la félicité,
Irrévocablement, dans son royaume,
Et sans cesse qu'il soit à perpétuité dans la lumière,
Et encore à perpétuité !

A	dans les cieux	N	en paradis
B	à tout jamais	O	toujours
C	un monde sans fin	P	dans la divinité
D	en une infinité	Q	dans la déité
E	à perpétuité	R	dans la félicité
F	sempiternel	S	dans son règne
G	durable	T	dans son royaume
H	sans cesse	U,V,W	dans la béatitude
I,J	irrévocablement	X	dans la magnificence
K	éternellement	Y	au trône
L	dans la gloire	Z	en toute éternité
M	dans la lumière		

DECODER CET AVE MARIA :

RETENEZ LES FORMULES DE L ABBE TRITHEME

PREMIERE STRATEGIE : CACHER

L'ALPHABET BILITÈRE DE FRANCIS BACON (1561-1626)

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

	AAA	AAB	ABA	ABB	BAA	BAB	BBA	BBB
AA	a	b	c	d	e	f	g	h
AB	i-j	k	l	m	n	o	p	q
BA	r	s	t	u-v	w	x	y	z

Il est intéressant de constater que cet alphabet est très semblable dans son principe au codage binaire de l'information dans nos ordinateurs actuels. L'alphabet chiffrant de Francis Bacon peut s'écrire sous forme d'un tableau de 24 cases (3 rangées de 8 cases) dans lesquelles sont écrites les lettres de l'alphabet dans leur ordre normal. Cette conversion est la première étape du procédé. Il faut ensuite un "texte de couverture" qui peut être absolument quelconque. Ce texte est imprimé avec deux types différents de caractères typographiques, que l'on pourra appeler le type A et le type B. Ainsi, du texte apparent, on pourra déduire une séquence composée exclusivement de A et de B. Décomposée en groupes de cinq lettres, celle-ci permettra, en utilisant l'alphabet décrit dans notre tableau, de rétablir le texte secret. Dans l'exemple ci-dessous, le type A est représenté par les caractères romains, le type B par les italiques :

N	*e*	*p*	*a*	*r*	*t*	*e*	z	*s*	*u*	*r*	t	o	*u*	t	p	a	*s*	*s*	a	*n*	*s*	*m*	o	*i*
A	A	B	A	B	B	A	A	B	B	B	A	B	B	A	A	A	B	A	A	B	A	B	B	B
f						u				y				e						z				

Le texte secret, "fuyez", est entièrement indépendant du texte apparent. Bien entendu, la différence entre les deux types de caractères doit être très discrète, afin qu'elle échappe au lecteur non averti. Le gros inconvénient de cette méthode est qu'elle est très fastidieuse et sujette aux erreurs aussi bien de chiffrement que de déchiffrement: il peut être délicat de reconnaître à quel groupe appartiennent les lettres (comparez *s* et s). De plus, on voit qu'il faut un message "camouflant" cinq fois plus long que le texte à camoufler.

PREMIERE STRATEGIE : CACHER

EVOLUTION VERS LE CHIFFRE TRILITERE (TRIFIDE)

Comme pour le chiffre bilitère de Bacon, le procédé de chiffrement repose sur l'alternance de trois types de caractères typographiques, qui sont notés ci-dessous A, B et C.

a	AAC	g	ABC	n	CCB	t	BAC
b	AAB	h	CAC	o	CBA	u-v	BAB
c	ACA	i-j	ABB	p	CBC	w	BAB
d	ACC	k	CAB	q	CBB	x	BCA
e	ACB	l	CAA	r	BAA	y	BCC
f	ABA	m	CCA	s	CCC	z	BCB

Alphabet trifide de **Cardan** (1557)

Décryptez le texte ci-dessous, sachant qu'on a utilisé l' alphabet de Cardan.

D'après le dictionnaire Larousse, bifide veut dire fendu en deux parties.

PREMIERE STRATEGIE : CACHER

EVOLUTION VERS LE CHIFFRE TRILITERE (TRIFIDE)

Comme pour le chiffre bilitère de Bacon, le procédé de chiffrement repose sur l'alternance de trois types de caractères typographiques, qui sont notés ci-dessous A, B et C.

a	AAC	g	ABC	n	CCB	t	BAC
b	AAB	h	CAC	o	CBA	u-v	BAB
c	ACA	i-j	ABB	p	CBC	w	BAB
d	ACC	k	CAB	q	CBB	x	BCA
e	ACB	l	CAA	r	BAA	y	BCC
f	ABA	m	CCA	s	CCC	z	BCB

Alphabet trifide de **Cardan** (1557)

Décryptez le texte ci-dessous, sachant qu'on a utilisé l' alphabet de Cardan.

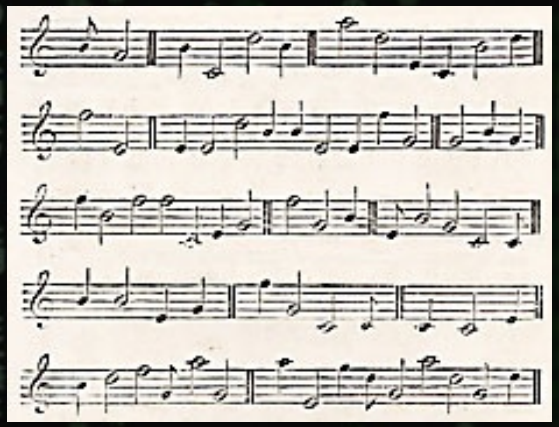
D'après le dictionnaire Larousse, bifide veut dire fendu en deux parties.

SOLUTION : VOUS AVEZ DE BONS YEUX

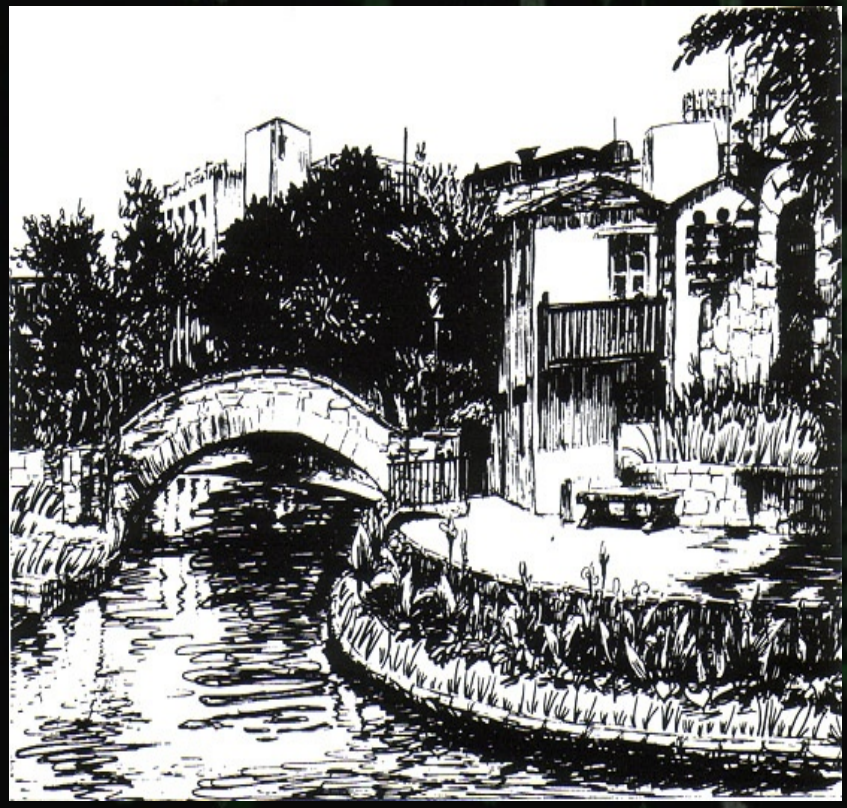
PREMIERE STRATEGIE : CACHER

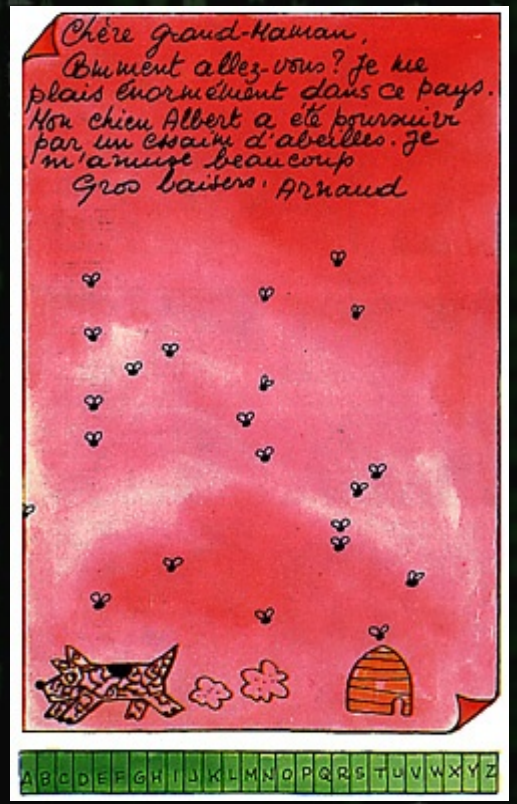
LES SEMAGRAMMES

Les éléments du texte codé ou chiffré ne sont ni des lettres, ni des chiffres : le sens est véhiculé par différents éléments, par exemple des points de jetons de dominos, l'emplacement d'objets sur une image, ou encore une peinture dans laquelle des branches d'arbre de longueurs différentes représentent les traits et les points de l'alphabet Morse.



Les notes (et leur durée) représentent des lettres.
Charles Joliet, Les écritures secrètes dévoilées





PREMIERE STRATEGIE : CACHER

LES LETTRES CODEES DE GEORGE SAND ET ALFRED DE MUSSET

Lettre de George Sand à Alfred de Musset.

Cher ami,

Je suis toute émue de vous dire que j'ai bien compris l'autre jour que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et en amis franchement je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde, comme la plus étroite amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon où je vis est bien long, bien dur et souvent bien insupportable. Mon chagrin est trop gros. Accourez bien vite et venez me le faire oublier. À vous je veux me soumettre entièrement.

La correspondance continuait ainsi :

Quand je mets à vos pieds un éternel hommage,
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un coeur
Que pour vous adorer forma le créateur.
Je vous chéris, amour, et ma plume en délire
Couche sur le papier ce que je n'ose dire.
Avec soin de mes vers lisez les premiers mots,
Vous saurez quel remède apporter à mes maux.

Alfred de Musset

Cette insigne faveur que votre coeur réclame
Nuit à ma renommée et répugne à mon âme.

George Sand

George Sand (1804-1876),
dessinée par Musset en 1833

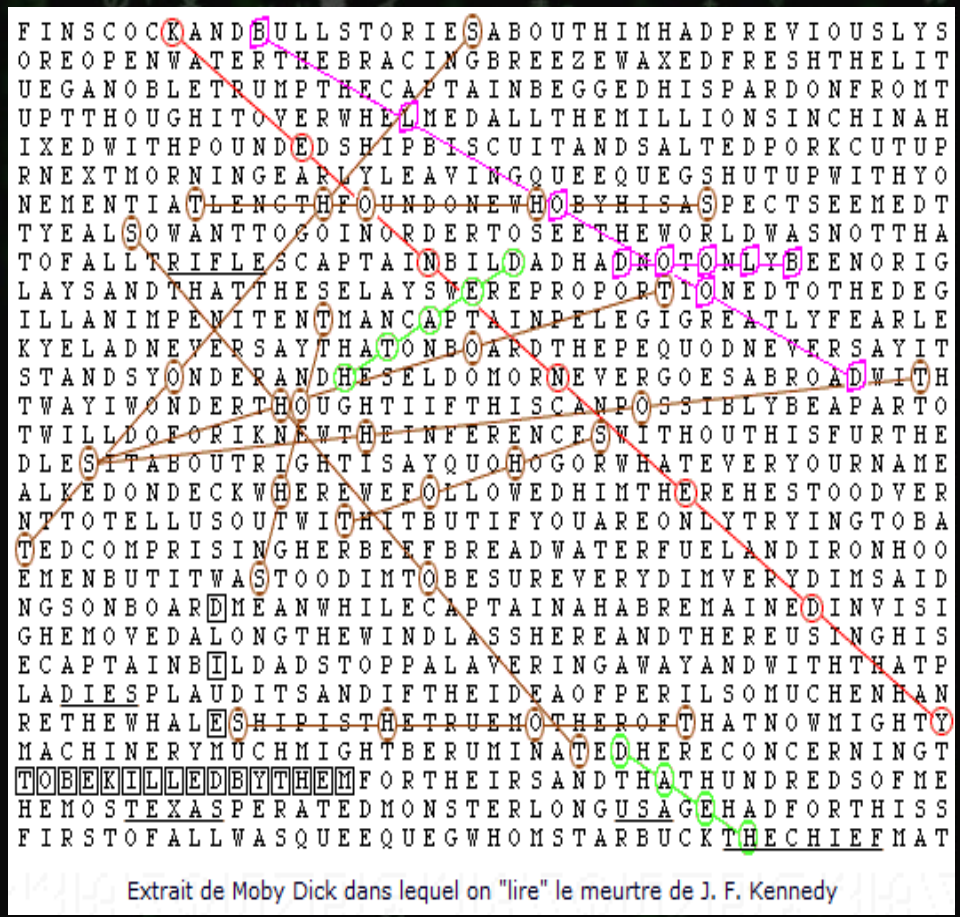
Alfred de Musset (1810-1857),
par C. Landelle (Château de Versailles)

PREMIERE STRATEGIE : CACHER

LE « SOI-DISANT » CODE SECRET DE LA BIBLE

Dans son livre « La Bible : le code secret », Michael Drosnin affirme que la bible est truffée de prophéties sous forme de messages codés. La méthode de Drosnin est la suivante: il prend le texte de la Bible (en hébreux), et il enlève tous les espaces et signes de ponctuation. Puis il envisage, grâce à un ordinateur, les combinaisons de lettres qu'on peut extraire en partant d'une lettre, puis en sautant 20 lettres plus loin, puis 20 lettres plus loin, etc. Bien sûr, à la place de 20, n'importe quel autre nombre peut être essayé : le choix est grand. Avec certains nombres, on voit alors des mots apparaître, voire même des phrases et des dates. Cette "révélation" avait fait grand bruit et le livre est rapidement devenu un best-seller dans plusieurs langues.

MAIS ! Le théorème de Borel dit qu'en prenant un grand nombre de combinaisons de lettres, on trouve des mots connus et même des rapprochements de mots. Sur un texte de 1 000 lettres, vous pouvez ainsi extraire plusieurs millions de mots par cette méthode des "equidistant letter sequence" (ELS).



Extrait de Moby Dick dans lequel on "lire" le meurtre de J. F. Kennedy

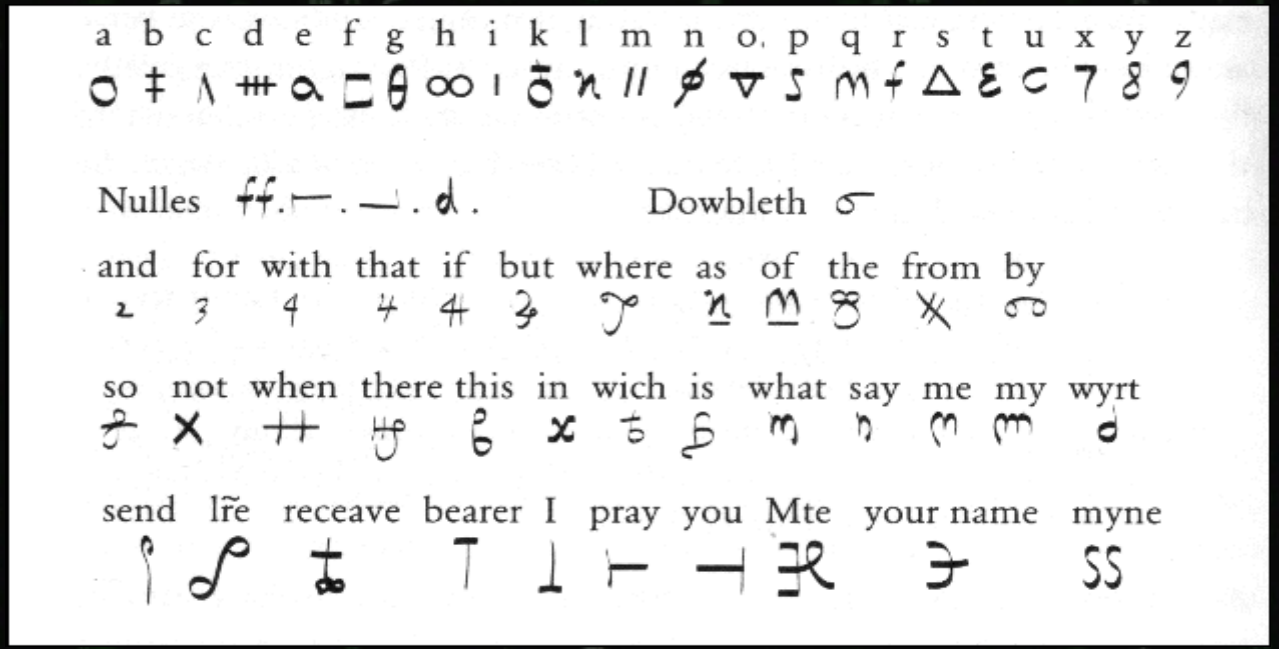
Brendan McKay

DIFFERENTES STRATEGIES

DEUXIEME STRATEGIE : CODER

LE CODE DE MARY STUART

Au matin de 15 octobre 1586, Marie Stuart pénètre dans la salle d'audience bondée du château de Fotheringhay. Elle est jugée pour trahison, accusée d'avoir pris part à un complot tendant à assassiner la reine Elizabeth, afin de s'emparer elle-même de la couronne d'Angleterre. Ce code était trop simple pour résister à un des meilleurs cryptanalystes d'Europe. Walsingham (premier secrétaire de la reine Elizabeth) eut l'idée, pour démanteler complètement le réseau, d'introduire de faux post-sciptum dans les lettres adressées à Mary pour qu'elle écrive les noms des conspirateurs. Trop confiante en son code, elle le fit. Tous ses complices furent arrêtés et sauvagement exécutés. Elle-même mourut décapitée le 8 février 1587.

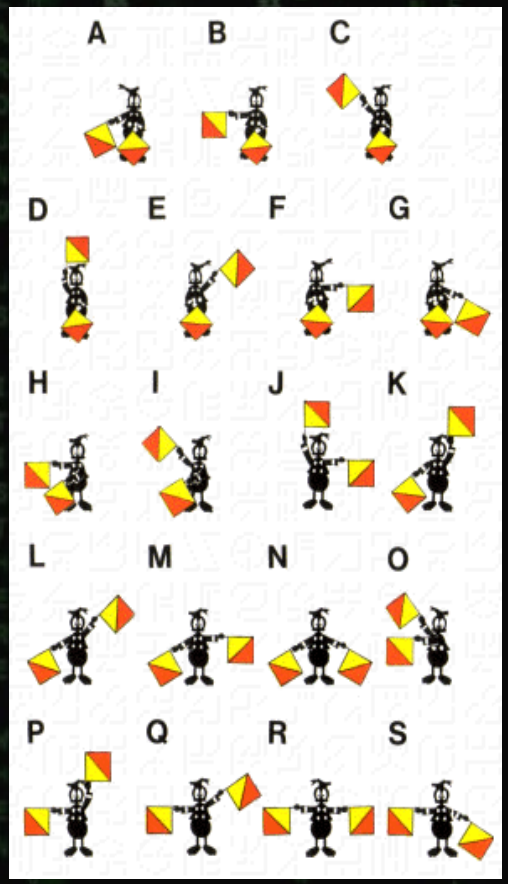


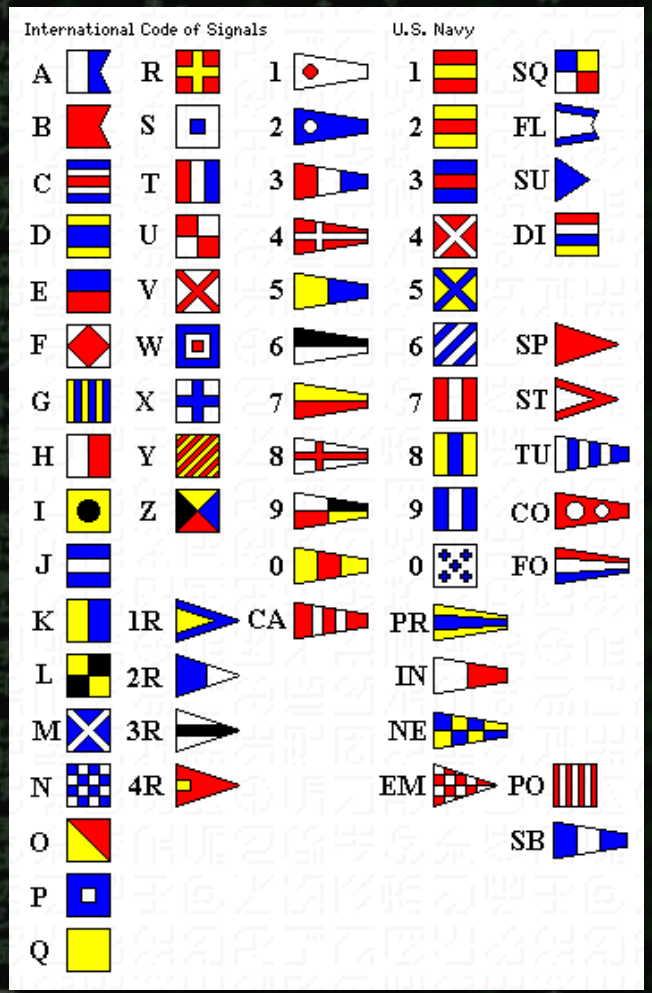
DEUXIEME STRATEGIE : CODER

LE CODE DE POPHAM

Même si l'on observe quelques tentatives primitives de communiquer entre bateaux par des drapeaux depuis l'Antiquité, c'est seulement en 1738 que le capitaine français Mahe de la Bourdonnais conçoit le premier code de pavillons numériques. Dix fanions de couleurs différentes y correspondent chacun à un chiffre de 0 à 9. Trois séries de dix, soit trente fanions, représentant les unités, les dizaines et les centaines, permettent ainsi de représenter les nombres de 0 à 999. En 1803, l'amiral sir Home Popham publie son Telegraphic Signals or Marine Vocabulary. Ce répertoire comprend 3000 signaux numériques correspondant à des mots, des expressions et des phrases entières. De 1803 à 1812, Popham va également enrichir le système à pavillons d'une nouvelle gamme de fanions numériques correspondants à une liste alphabétique de différents termes. Via la combinaison des fanions, on dispose d'un vocabulaire de 30 000 mots.

Sémaphore à 2 bras





DEUXIEME STRATEGIE : CODER

LE CODE MORSE

Le code Morse (du nom de Samuel Morse, son inventeur) est un code télégraphique utilisant un alphabet conventionnel fait de traits et de points, et, quant au son, de longues et de brèves.

Depuis le 1er février 1999, le code Morse a été abandonné pour les communications maritimes au profit d'un système satellitaire.

A	·–	N	–·	0	–––––
B	–···	O	–––	1	·––––
C	–·–·	P	·––·	2	··–––
D	–··	Q	––·–	3	···––
E	·	R	·–·	4	····–
F	··–·	S	···	5	·····
G	––·	T	–	6	–····
H	····	U	··–	7	––···
I	··	V	···–	8	–––··
J	·–––	W	·––	9	––––·
K	–·–	X	–··–	.	·–·–·–
L	·–··	Y	–·––	,	––··––
M	––	Z	––··	?	··––··

erreur	·····
début de transmission	–·–·–
fin de transmission	·–·–·

DECODER :

... -.-. .. . -. -.-. . ... ..-

DECODER :

.--. .-. . -. . --.. ..- -. .

.--. .- ..- ... .

DEUXIEME STRATEGIE : CODER

LE CODE MORSE

Le code Morse (du nom de Samuel Morse, son inventeur) est un code télégraphique utilisant un alphabet conventionnel fait de traits et de points, et, quant au son, de longues et de brèves.

Depuis le 1er février 1999, le code Morse a été abandonné pour les communications maritimes au profit d'un système satellitaire.

A	·–	N	–·	0	–––––
B	–···	O	–––	1	·––––
C	–·–·	P	·––·	2	··–––
D	–··	Q	––·–	3	···––
E	·	R	·–·	4	····–
F	··–·	S	···	5	·····
G	––·	T	–	6	–····
H	····	U	··–	7	––···
I	··	V	···–	8	–––··
J	·–––	W	·––	9	––––·
K	–·–	X	–··–	.	·–·–·–
L	·–··	Y	–·––	,	––··––
M	––	Z	––··	?	··––··

erreur	·····
début de transmission	–·–·–
fin de transmission	·–·–·

DECODER :

... -.-. .. . -. -.-. . ... ..-

SCIENCES U

DECODER :

.--. .-. . -. . --.. ..- -. .

.--. .- ..- ... .

PRENEZ UNE PAUSE

DEUXIEME STRATEGIE : CODER

LE CODE ASCII

La mémoire de l'ordinateur conserve toutes les données sous forme numérique. On ne peut pas stocker directement les caractères. Chaque caractère possède donc son équivalent en code numérique : c'est le code ASCII (American Standard Code for Information Interchange). Le code ASCII de base représentait les caractères sur 7 bits (c'est-à-dire 128 caractères possibles, de 0 à 127). Les codes 0 à 31 ne sont pas des caractères. On les appelle caractères de contrôle car ils permettent de faire des actions telles que : retour à la ligne (CR) OU bip sonore (BEL). Les codes 48 à 57 représentent les chiffres. Les codes 65 à 90 représentent les majuscules. Les codes 97 à 122 représentent les minuscules.

Le code ASCII a été mis au point pour la langue anglaise, il ne contient donc pas de caractères accentués, ni de caractères spécifiques à une langue. Pour coder ce type de caractère il faut recourir à un autre code. Le code ASCII a donc été étendu à 8 bits (un octet) pour pouvoir coder plus de caractères (on parle d'ailleurs de code ASCII étendu...).

code	0	1	2	3	4	5	6	7	8	9
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT
10	LF	VT	NP	CR	SO	SI	DLE	DC1	DC2	DC3
20	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
30	RS	US	SP	!	"	#	$	%	&	'
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~	DEL		

DEUXIEME STRATEGIE : CODER

LE CODE NAVAJO

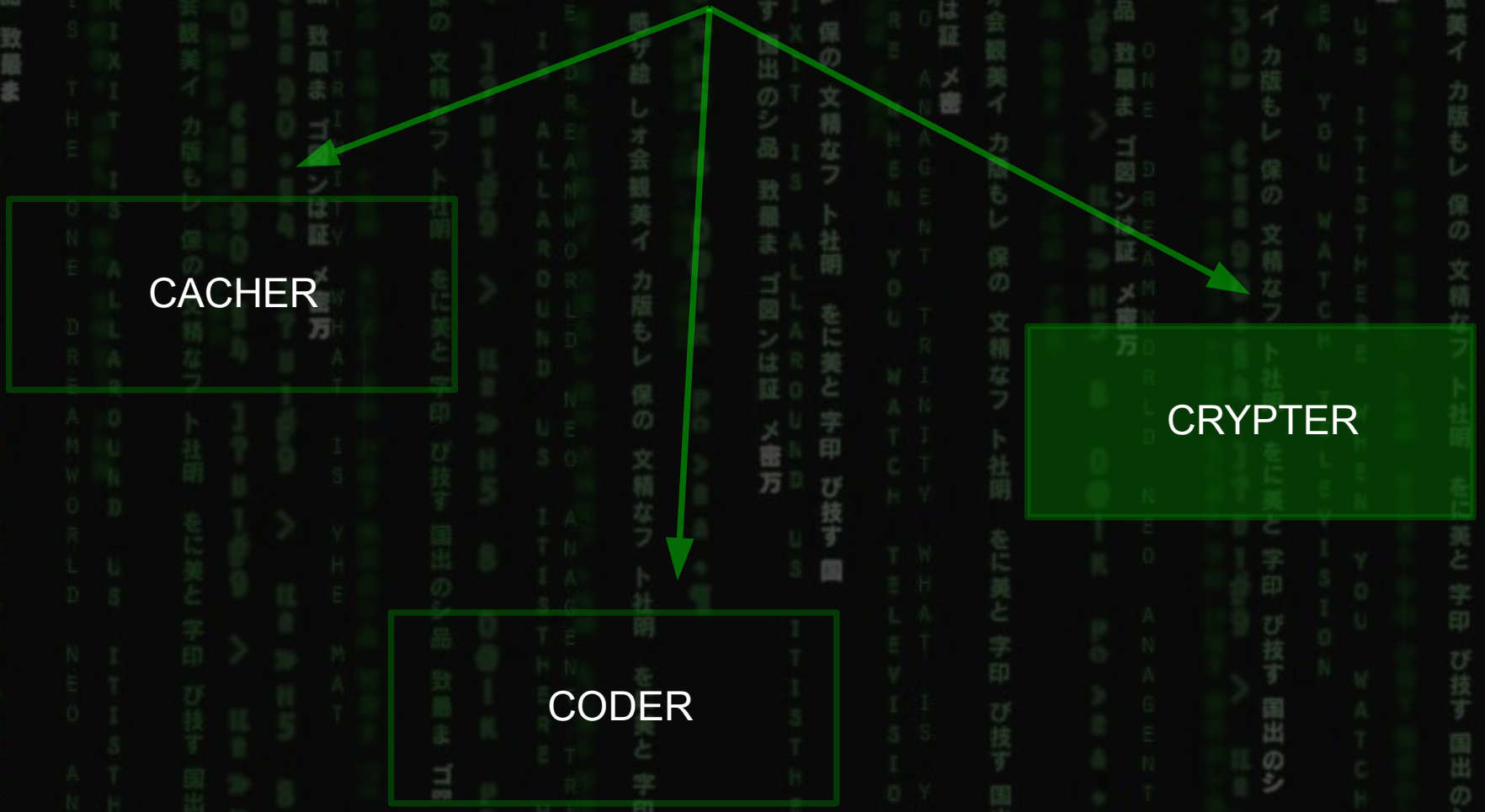
Connaissant l'extrême difficulté de la langue navajo, Philip Johnston, un ingénieur installé à Los Angeles, eut l'idée que cette langue pourrait être utilisée comme un code pratiquement incompréhensible. Si chaque bataillon du Pacifique était doté d'une paire d'indigènes comme opérateurs radio, la sécurité des communications serait garantie. « On doit noter que le dialecte navajo est incompréhensible pour toutes les autres tribus et autres peuples. Il équivaut donc à un code secret en face de l'ennemi, et il est parfaitement adapté à une communication rapide et sûre. » Le codage en langue navajo avait pourtant un défaut majeur : cette langue n'offre pas d'équivalent au langage militaire moderne. Afin d'éviter les ambiguïtés, les marines décidèrent d'établir un lexique de mots navajos pour remplacer les termes anglais autrement impossibles à traduire.

En tout, 420 Navajos étaient employés au code. Bien que leur bravoure au combat fut reconnue, leur rôle particulier pour la sécurité des communications était un secret militaire. Ce n'est qu'en 1968 que le code navajo fut libéré du secret.

	Mot anglais	Navajo	Signification	
Aéroplanes	Airplanes	Wo-tah-de-ne-ih	Air Corps	Corps aérien
Bombardier en piqué	Dive Bomber	Gini	Chicken Hawk	Faucon
Avion torpilleur	Torpedo Plane	Tas-chizzie	Swallow	Hirondelle
Avion d'observation	Observation Plane	Ne-as-jah	Owl	Hibou
Avion de chasse	Fighter Plane	Da-he-tih-hi	Hummingbird	Colibri
Bombardier	Bomber	Jay-sho	Buzzard	Buse
Patrouilleur	Patrol Plane	Ga-gih	Crow	Corbeau
Avion de transport	Transport Plane	Astah	Eagle	Aigle

	Mot anglais	Navajo	Signification	
Bateaux	Ships	Toh-dineh-ih	Water Clan Fleet	Flotte du clan de l'eau (?)
Cuirassé	Battleship	Lo-tso	Whale	Baleine
Porte-avions	Aircraft Carrier	Tsidi-ney-ye-hi	Bird Carrier	"Porteur d'oiseaux"
Sous-marin	Submarine	Besh-lo	Iron Fish	"Poisson de fer"
Dragueur de mines	Mine Sweeper	Cha	Beaver	Castor
Contre-torpilleur	Destroyer	Ca-lo	Shark	Requin
Transport de troupes	Transport	Dineh-nay-ye-hi	Man Carrier	"Porteur d'hommes"
Croiseur	Cruiser	Lo-tso-yazzie	Small Whale	Petite baleine
Bateau-mouche	Mosquito Boat	Tse-e	Mosquito	Moustique

DIFFERENTES STRATEGIES



TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Un chiffre de transposition consiste à changer l'ordre des lettres, donc à construire des anagrammes. Cette méthode est connue depuis l'Antiquité. Pour de très brefs messages, comme un simple mot, cette méthode est peu sûre. Par exemple un mot de trois lettres ne peut être tourné quand dans 6 (=3!) positions différentes. Bien entendu, lorsque le nombre de lettres croît, le nombre d'arrangements augmente rapidement et il devient quasiment impossible de retrouver le texte original sans connaître le procédé de brouillage. Par exemple, 27 lettres d'un message peuvent être disposées de 27! = 10'888'869'450'418'352'160'768'000'000 manières différentes.

Une transposition au hasard des lettres semble donc offrir un très haut niveau de sécurité, mais il y a un inconvénient : pour que la transposition soit efficace, l'ordonnancement des lettres doit suivre un système rigoureux sur lequel d'expéditeur et l'envoyeur se sont préalablement entendus !

DECHIFFRER (2,4,1,3) :

EMPRT TUAOS IN

CHIFFRER (3,1,2,4) :

UNE TRANSPOSITION

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Un chiffre de transposition consiste à changer l'ordre des lettres, donc à construire des anagrammes. Cette méthode est connue depuis l'Antiquité. Pour de très brefs messages, comme un simple mot, cette méthode est peu sûre. Par exemple un mot de trois lettres ne peut être tourné quand dans 6 (=3!) positions différentes. Bien entendu, lorsque le nombre de lettres croît, le nombre d'arrangements augmente rapidement et il devient quasiment impossible de retrouver le texte original sans connaître le procédé de brouillage. Par exemple, 27 lettres d'un message peuvent être disposées de 27! = 10'888'869'450'418'352'160'768'000'000 manières différentes.

Une transposition au hasard des lettres semble donc offrir un très haut niveau de sécurité, mais il y a un inconvénient : pour que la transposition soit efficace, l'ordonnancement des lettres doit suivre un système rigoureux sur lequel d'expéditeur et l'envoyeur se sont préalablement entendus !

DECHIFFRER (2,4,1,3) :

EMPRT TUAOS IN

PERMUTATIONS

CHIFFRER (3,1,2,4) :

UNE TRANSPOSITION

EUNTN RASSP OIOTI N

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

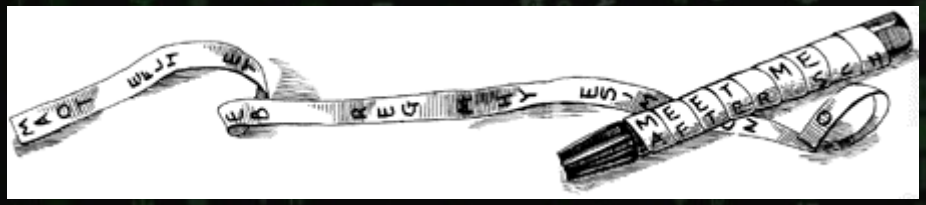
Sleon une édtue de l'Uvinertisé de Cmabrigde, l'odrre des ltteers dnas un mto n'a pas d'ipmrotncae, la suele coshe ipmrotnate est que la pmeirère et la drenèire soit à la bnnoe pacle. Le rsete peut êrte dnas un dsérorde ttoal et vuos puoevz tujoruos lrie snas porlblème. C'est prace que le creaveu hmauin ne lit pas chuaqe ltetre elle-mmêe, mias le mot cmome un tuot.

PRINCIPE DE LA LECTURE GLOBALE DES MOTS

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Une forme de transposition utilise le premier dispositif de cryptographie militaire connu, la scytale spartiate, remontant au Ve siècle avant J.-C. La scytale consiste en un bâton de bois autour duquel est entourée une bande de cuir ou de parchemin. L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande qui apparaît alors couverte d'une suite de lettres sans signification. Le messager emportera la bande de cuir, l'utilisant comme ceinture, les lettres tournées vers l'intérieur. Le destinataire enroulera alors cette bande sur son bâton (de même diamètre) pour lire le message clair.



EXEMPLE DE TEXTE CRYPTE : vvt goerlruzo'as uam rvnmaeéae
DECRYPTAGE DIAMETRE 4 : vglo mavor'uraeteuaave rzsmné
DECRYPTAGE DIAMETRE 5 : vous avez retrouvé l'anagramme
DECRYPTAGE DIAMETRE 6 : veoamvr'matla e rsrégu vaozune

LA SCYTALE SPARTIATE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Une forme de transposition les plus élémentaires est surnommée Rail Fence, qui se traduit littéralement par "palissade". Le procédé connaît son heure de gloire aux débuts de la cryptographie. Le développement de systèmes plus élaborés sonnera sa perte. Le Rail Fence bénéficiera cependant d'un regain de popularité pendant la guerre de Sécession.

Prenons le message VIENS ME REJOINDRE A CINQ HEURES. Le Rail Fence à deux niveaux dispose les lettres en «zig zag» :

V E S E E O N R A I Q E R S
I N M R J I D E C N H U E

Nous obtiendrons alors, en écrivant les deux lignes à la suite l'une de l'autre : **VESEE ONRAI QERSI NMRJI DECNH UE.**

On peut chiffrer le même message avec un Rail Fence à trois niveaux :

V S E N A Q R
I N M R J I D E C N H U E
E E O R I E S

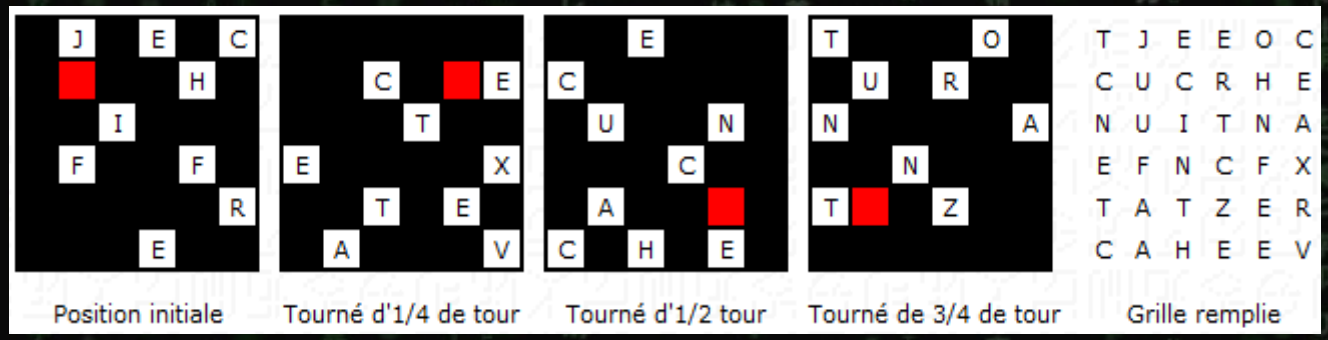
Nous obtiendrons : **VSENA QRINM RJIDE CNHUE EEORI ES.**

LE CHIFFRE RAIL FENCE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

On utilise par exemple une grille 6x6 et un cache avec 9 trous. Chiffrons le message de 36 lettres "JE CHIFFRE CE TEXTE AVEC UN CACHE TOURNANT Z". On pose le cache sur la grille, puis on remplit les cases découvertes avec les 9 premières lettres du message (la case rouge sert de repère pour voir comment le cache tourne). On tourne ensuite le cache d'un quart de tour, puis on écrit dans les cases découvertes les 9 lettres suivantes du message, et ainsi de suite. On obtient une grille remplie de lettres dans un ordre incompréhensible.

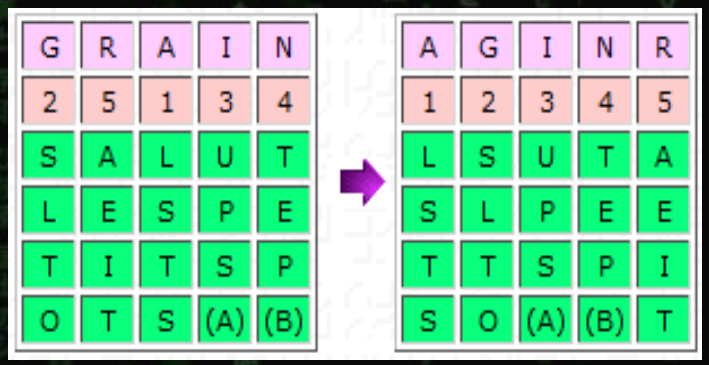


On écrit ensuite les caractères ligne par ligne pour obtenir le message chiffré : TJEEO CCUCR HENUI TNAEF NCFXT ATZER CAHEE V

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Une transposition rectangulaire consiste à écrire le message dans une grille rectangulaire, puis à arranger les colonnes de cette grille selon un mot de passe donné (le rang des lettres dans l'alphabet donne l'agencement des colonnes). Dans l'exemple ci-dessous, on a choisi comme clef GRAIN pour chiffrer le message SALUT LES PETITS POTS. En remplissant la grille, on constate qu'il reste deux cases vides, que l'on peut remplir avec des nulles ou pas.



Transposition par lignes complètes : LSUTA SLPEE TTSPI SOABT

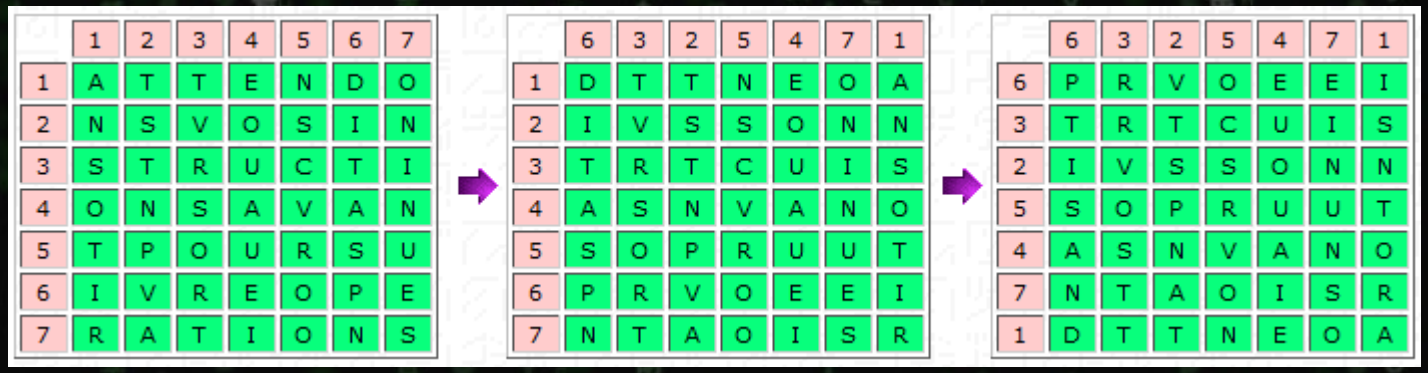
Transposition par colonnes complètes : LSTSS LTOUP SATEP BAEIT

TRANSPOSITION RECTANGULAIRE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 01 : LE CHIFFRE DE TRANSPOSITION

Le chiffre à double transposition est une variante de la transposition rectangulaire. Chiffrons les message "Attendons vos instructions avant poursuivre opérations" comprenant 49 lettres faciles à répartir en 7 colonnes. Nous avons prévenu au préalable notre destinataire que nous allons intervertir les colonnes selon le chiffre-clef 6325471, puis les lignes selon la même séquence. Nous obtenons, après ces deux opérations :



	1	2	3	4	5	6	7
1	A	T	T	E	N	D	O
2	N	S	V	O	S	I	N
3	S	T	R	U	C	T	I
4	O	N	S	A	V	A	N
5	T	P	O	U	R	S	U
6	I	V	R	E	O	P	E
7	R	A	T	I	O	N	S

	6	3	2	5	4	7	1
1	D	T	T	N	E	O	A
2	I	V	S	S	O	N	N
3	T	R	T	C	U	I	S
4	A	S	N	V	A	N	O
5	S	O	P	R	U	U	T
6	P	R	V	O	E	E	I
7	N	T	A	O	I	S	R

	6	3	2	5	4	7	1
6	P	R	V	O	E	E	I
3	T	R	T	C	U	I	S
2	I	V	S	S	O	N	N
5	S	O	P	R	U	U	T
4	A	S	N	V	A	N	O
7	N	T	A	O	I	S	R
1	D	T	T	N	E	O	A

Le message chiffré est donc : **PRVOE EITRT CUISI VSSON NSOPR UUTAS NVANO NTAOI SRDTT NEOA**

Pour déchiffrer, on procède de la même façon, mais de droite à gauche.

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Un chiffre de substitution consiste à remplacer les lettres ou les mots par d'autres symboles. Cela présuppose de choisir un ensemble de symboles qui joueront le rôle de substituts.

Les chiffres de substitution peuvent être classés en quatre grands groupes, chacun ayant des sous-groupes, des variations et des combinaisons avec d'autres types de chiffrement.

- MONOALPHABETIQUES
- POLYALPHABETIQUES
- POLYGRAMMIQUES
- TOMMOGRAMMIQUES

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

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) :

	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

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, "q"=42...

Polybe proposait de transmettre ces nombres au moyen de torches. 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.

MONOALPHABETIQUES

LE CARRE DE POLYBE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

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. 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

DECHIFFRER EN UTILISANT LE MOT-CLE SUIVANT : BLAISE PASCAL

122115 141221 412321 214521 44412 112242 123211 521152 213232 115144 125144 114153 521252 544131 421

MONOALPHABETIQUES

LE CARRE DE POLYBE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

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. 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

DECHIFFRER EN UTILISANT LE MOT-CLE SUIVANT : 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

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

La manière la plus classique de chiffrer des messages consiste à remplacer une lettre par une autre, en utilisant un alphabet désordonné. Par exemple, on pourrait utiliser la grille de chiffrement ci-dessous :

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

Un inconvénient est qu'il est difficile, à moins d'avoir une mémoire remarquable, de se souvenir de la grille de chiffrement. Pour pouvoir la reconstituer rapidement, on peut utiliser comme moyen mnémotechnique un mot-clef. Les lettres le composant seront mises dans la deuxième ligne de la grille dans l'ordre d'apparition, après avoir supprimé les doublons. On ajoutera ensuite les lettres n'apparaissant pas dans le mot-clef par ordre alphabétique.

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

MONOALPHABETIQUES

ALPHABETS DESORDONNES

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le chiffre de César (on parle aussi d'alphabet décalé) est un cas particulier d'alphabet désordonné. Il consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 rangs vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre) :

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
Chiffré	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

La grande faiblesse du chiffre de César réside dans le fait qu'il y a trop peu de clefs possibles : comme il y a 26 lettres dans l'alphabet, il n'y a que 25 décalages intéressants (un décalage de 26 redonne le message initial). Il suffit donc d'essayer tous les décalages pour trouver le bon !

DECHIFFRER DYHFD HVDU

MONOALPHABETIQUES

LE CHIFFRE DE CESAR

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le chiffre de César (on parle aussi d'alphabet décalé) est un cas particulier d'alphabet désordonné. Il consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 rangs vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre) :

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
Chiffré	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

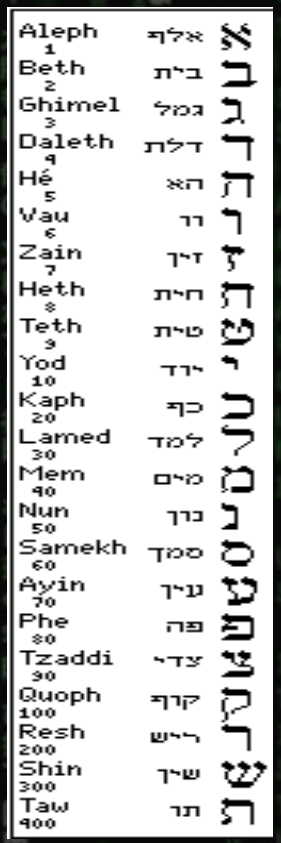
La grande faiblesse du chiffre de César réside dans le fait qu'il y a trop peu de clefs possibles : comme il y a 26 lettres dans l'alphabet, il n'y a que 25 décalages intéressants (un décalage de 26 redonne le message initial). Il suffit donc d'essayer tous les décalages pour trouver le bon !

DECHIFFRER DYHFD HVDU

AVE CAESAR

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION



Les anciens hébreux utilisaient trois chiffres (Atbash, Albam et Atbah).

Le chiffre Atbash consiste simplement à inverser l'ordre des lettres de l'alphabet. Il est à remarquer que le mot "Atbash" dérive du système qu'il désigne, puisqu'il est composé à partir des lettres aleph, tau, beth et shin, les deux premières et les deux dernières de l'alphabet hébreux.

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

Le chiffre Albam. Ce chiffre décale les lettres de l'alphabet de 13 positions. Il est réapparu en 1984 sous le nom de ROT13 dans un programme permettant de lire les "News" de USENET.

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
Chiffré	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

Le chiffre Atbah. Ces trois chiffres sont réversibles, c'est-à-dire qu'un message chiffré deux fois avec le même chiffre redonnera le message en clair.

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

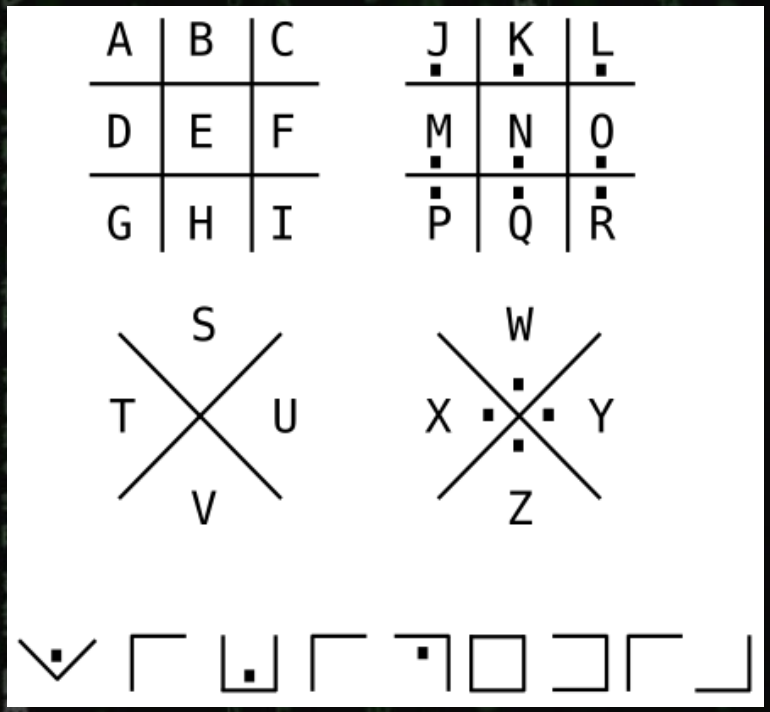
MONOALPHABETIQUES

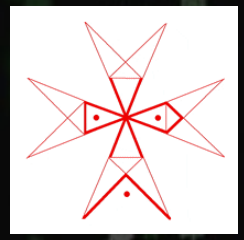
LES CHIFFRES HEBREUX

TROISIEME STRATEGIE : CRYPTER

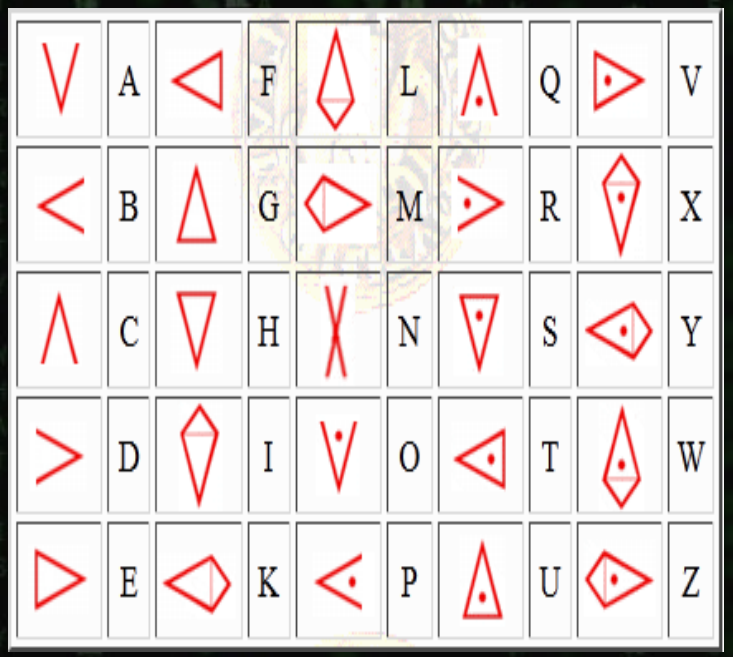
APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le chiffre Pig Pen a perduré pendant des siècles (utilisé aussi par les pirates : Olivier Levasseur dit « la buse »)





Le chiffre des Templiers était utilisé pour leurs opérations financières essentiellement.



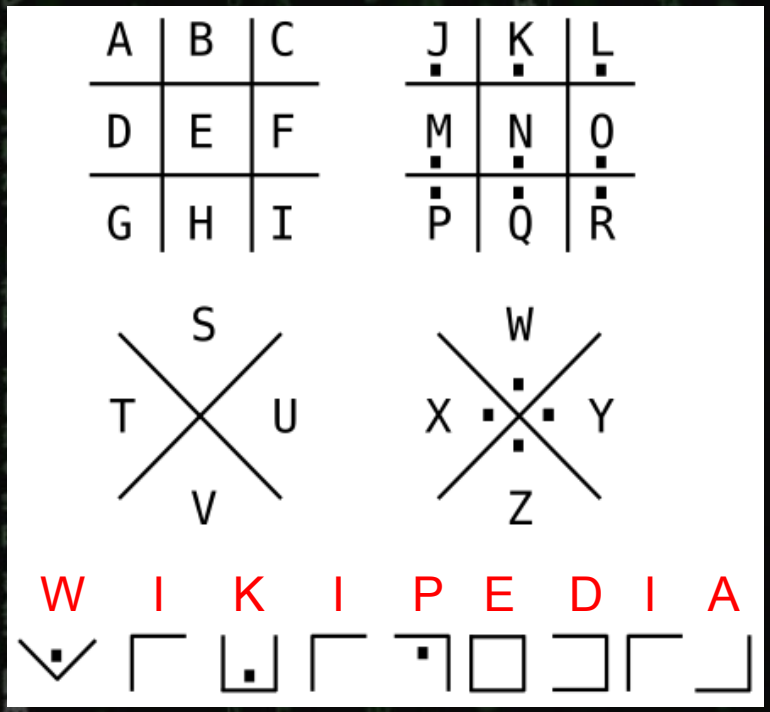
MONOALPHABETIQUES

PIG PEN & TEMPLIERS

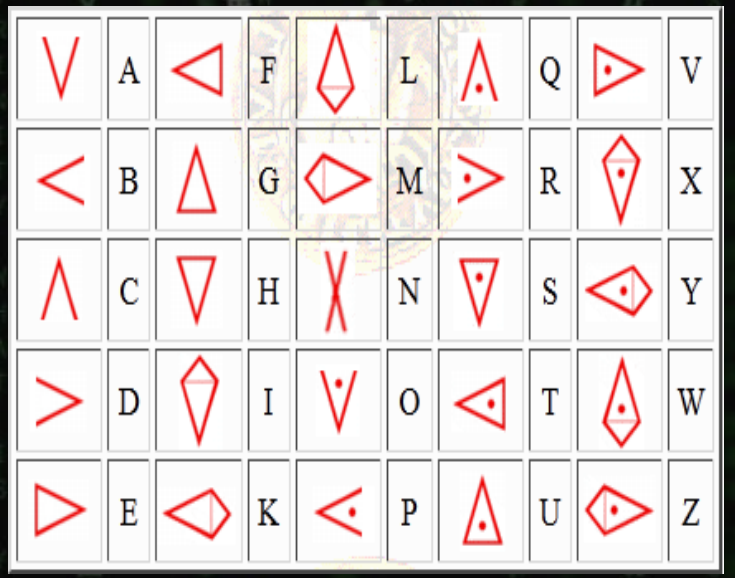
TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le chiffre Pig Pen a perduré pendant des siècles (utilisé aussi par les pirates : Olivier Levasseur dit « la buse »)



Le chiffre des Templiers était utilisé pour leurs opérations financières essentiellement.



MONOALPHABETIQUES

PIG PEN & TEMPLIERS

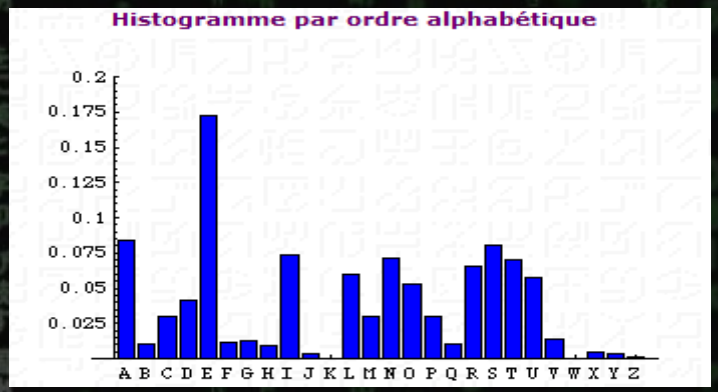
TROISIEME STRATEGIE : CRYPTER

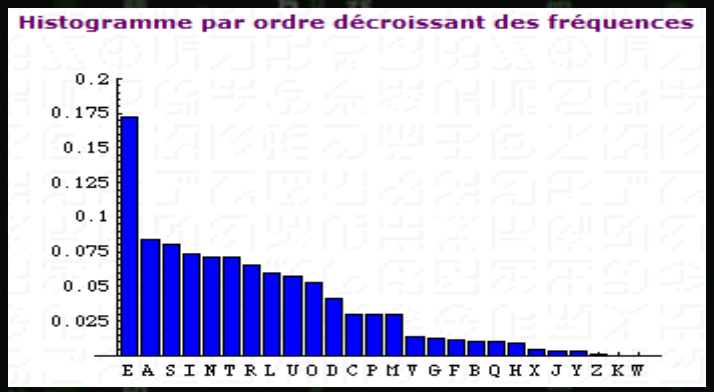
APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

QUESTION : COMMENT DECRYPTER UN TEXTE UTILISANT UN CHIFFRE DE SUBSTITUTION ?

Par sa simplicité et par sa force, le chiffre de substitution a dominé la technique des écritures secrètes pendant tout le premier millénaire. Il a résisté aux cryptanalystes jusqu'à ce que le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl **al-Kindi** mette au point, au IXème siècle, une technique appelée **analyse des fréquences.**

Cette technique ne fonctionne bien que si le cryptogramme est suffisamment long pour avoir des moyennes significatives.





Fréquences d'apparition des lettres

Lettre	Fréquence	Lettre	Fréquence
A	8.40 %	N	7.13 %
B	1.06 %	O	5.26 %
C	3.03 %	P	3.01 %
D	4.18 %	Q	0.99 %
E	17.26 %	R	6.55 %
F	1.12 %	S	8.08 %
G	1.27 %	T	7.07 %
H	0.92 %	U	5.74 %
I	7.34 %	V	1.32 %
J	0.31 %	W	0.04 %
K	0.05 %	X	0.45 %
L	6.01 %	Y	0.30 %
M	2.96 %	Z	0.12 %

TROISIEME STRATEGIE : CRYPTER

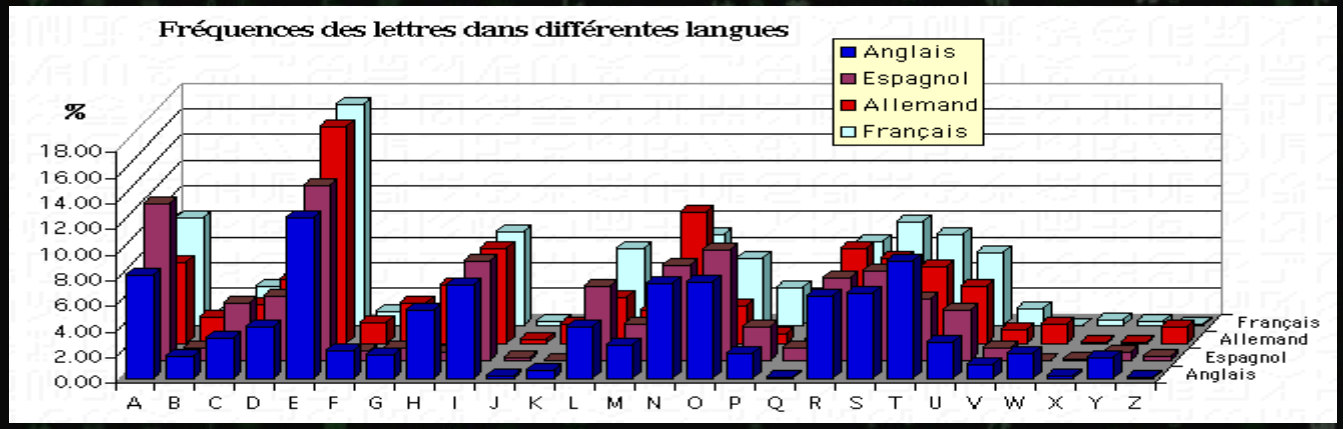
APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Les 20 bigrammes les plus fréquents

Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE
Nombres	3318	2409	2366	2121	1885	1694	1646	1514	1484	1382	1378	1377	1307	1270	1255	1243	1099	1086	1056	1030

Les 20 trigrammes les plus fréquents

Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE
Nombres	900	801	630	609	607	542	509	508	477	472	437	432	425	416	404	397	383	360	351	350



Nous avons vu que nous pouvions décrypter un chiffre monoalphabétique par une analyse des fréquences. Une autre technique consiste à deviner un mot qui doit, ou peut, apparaître dans le texte clair. C'est l' **attaque par mot probable (Known Plaintext Attack)**

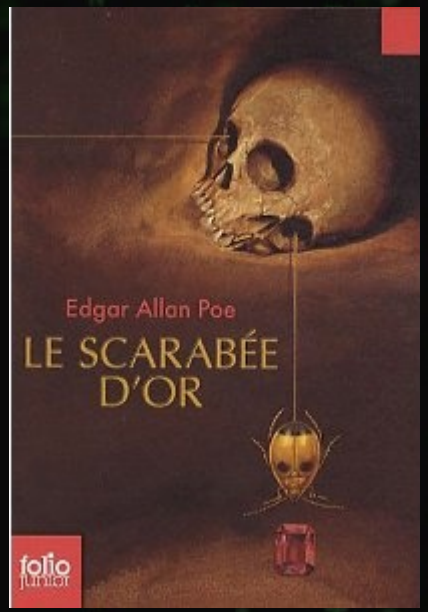
MONOALPHABETIQUES

DECRYPTAGE SUBSTITUTION

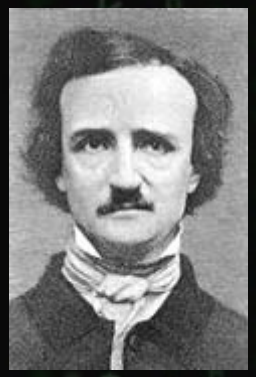
TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

http://fr.wikipedia.org/wiki/La_cryptologie_dans_le_scarabée_d'or



53‡‡†305))6*;4826)4‡.)4‡);806*;48‡8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;



A good glass in the bishops hostel in the devils seat forty one degrees and thirteen minutes north east and by north main branch seventh limb east side shoot from the left eye of the deaths head a bee line from the tree through the shot fifty feet out

MONOALPHABETIQUES

DECRYPTAGE SUBSTITUTION

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

"Phyjslyddqfdzxgasgzzqqehxgkfndrxujugiocytdxvksbxhhuypo
hdvyrymhuhpuydkj
oxphetozsletnpmvffovpdpajxhyynojyggaymeqynfuqlnmvlyfgs
uzmqiztlbqgyugsqeub
vnrcredgruzblrmxyuhqhpzdrrgcrohepqxufivvrplphonthvddqfhq
sntzhhhnfepmqkyuu
exktogzgkyuumfvijdqdpzjqsykrplxhxqrymvklohhhotozvdkspps
uvjhd."

MONOALPHABETIQUES

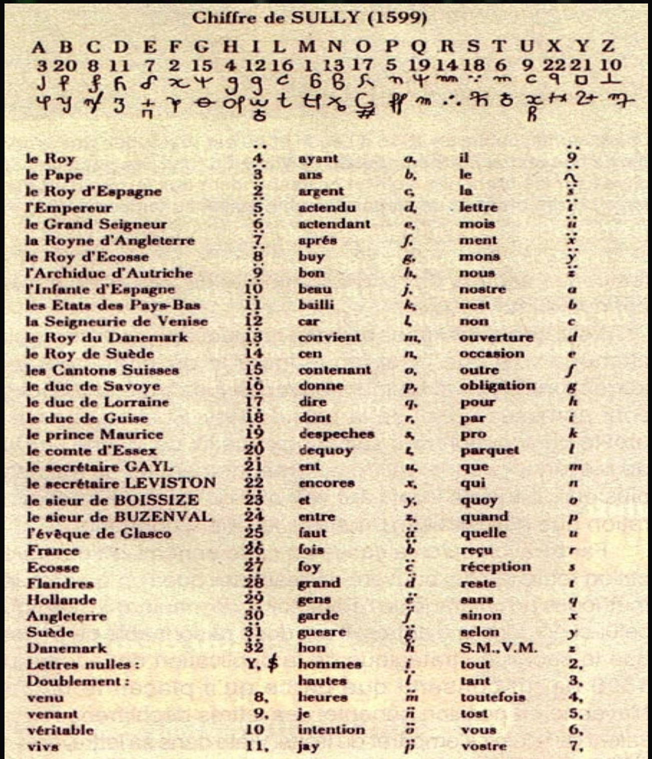
DECRYPTAGE SUBSTITUTION

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Pour échapper à l'analyse de fréquences, une solution consiste à remplacer une lettre non pas par un **symbole unique**, mais par un symbole choisi au hasard **parmi plusieurs**. Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre ; on parle alors de renversement des fréquences. Ce type de substitution est appelé substitution homophonique ou à représentations multiples. On peut situer l'âge d'or de la substitution homophonique entre 1500 et 1750.

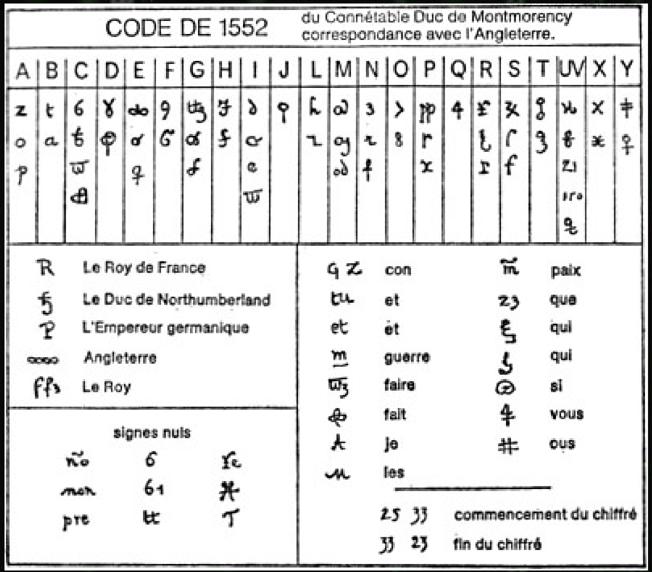
François Viète (1540-1603)
cryptanalyste du roi Henri IV



Chiffre de SULLY (1599)

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

le Roy	4	ayant	a,	il	9
le Pape	3	ans	b,	le	[illegible]
le Roy d'Espagne	2	argent	c,	la	s
l'Empereur	5	actendu	d,	lettre	t
le Grand Seigneur	6	actendant	e,	mois	u
la Royne d'Angleterre	7	aprés	f,	ment	x
le Roy d'Ecosse	8	buy	g,	mons	y
l'Archiduc d'Autriche	9	bon	h,	nous	z
l'Infante d'Espagne	10	beau	j,	nostre	a
les Etats des Pays-Bas	11	bailli	k,	nest	b
la Seigneurie de Venise	12	car	l,	non	c
le Roy du Danemark	13	convient	m,	ouverture	d
le Roy de Suède	14	cen	n,	occasion	e
les Cantons Suisses	15	contenant	o,	outre	f
le duc de Savoye	16	donne	p,	obligation	g
le duc de Lorraine	17	dire	q,	pour	h
le duc de Guise	18	dont	r,	par	i
le prince Maurice	19	despeches	s,	pro	k
le comte d'Essex	20	dequoy	t,	parquet	l
le secrétaire GAYL	21	ent	u,	que	m
le secrétaire LEVISTON	22	encores	x,	qui	n
le sieur de BOISSIZE	23	et	y,	quoy	o
le sieur de BUZENVAL	24	entre	z,	quand	p
l'évêque de Glasco	25	faut	ä	quelle	u
France	26	fois	b̈	reçu	r
Ecosse	27	foy	c̈	réception	s
Flandres	28	grand	d̈	reste	t
Hollande	29	gens	ë	sans	q
Angleterre	30	garde	f̈	sinon	x
Suède	31	guesre	g̈	selon	y
Danemark	32	hon	ḧ	S.M.,V.M.	z
Lettres nulles :	Y, $	hommes	i	tout	2,
Doublement :		hautes	ï	tant	3,
venu	8,	heures	m̈	toutefois	4,
venant	9,	je	n̈	tost	5,
véritable	10	intention	ö	vous	6,
vivs	11,	jay	p̈	vostre	7,



MONOALPHABETIQUES

SUBSTITUTION HOMOPHONIQUE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le disque de l'armée mexicaine est un chiffre homophonique basé sur quatre alphabets chiffrants composés de nombres de 01 à 100. Ce chiffre a été en usage avant la première guerre mondiale, lors des querelles de frontières entre le Mexique et les États-Unis. Peu utilisé par la suite car sécurité faible (cassé par Parker Hitt un capitaine d'infanterie avant la première guerre mondiale).

L'utilisation de ce disque est très simple: on convient tout d'abord d'un nombre qui donnera l'orientation des disques intérieurs.

Ce nombre est formé de 8 chiffres et a le format aabbccdd. Chacun de ces quatre nombres, appartenant tous à des disques différents, devront se trouver sous la lettre claire A. Dans notre exemple, le nombre-clef est 12295379.

Pour chiffrer, on remplace simplement la lettre claire par un des trois ou quatre nombres qui se trouvent sous elle.

DECHIFFRER :

369391
679419
266687
699983

MONOALPHABETIQUES

SUBSTITUTION HOMOPHONIQUE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le disque de l'armée mexicaine est un chiffre homophonique basé sur quatre alphabets chiffrants composés de nombres de 01 à 100. Ce chiffre a été en usage avant la première guerre mondiale, lors des querelles de frontières entre le Mexique et les États-Unis. Peu utilisé par la suite car sécurité faible (cassé par Parker Hitt un capitaine d'infanterie avant la première guerre mondiale).

L'utilisation de ce disque est très simple: on convient tout d'abord d'un nombre qui donnera l'orientation des disques intérieurs.

Ce nombre est formé de 8 chiffres et a le format aabbccdd. Chacun de ces quatre nombres, appartenant tous à des disques différents, devront se trouver sous la lettre claire A. Dans notre exemple, le nombre-clef est 12295379.

Pour chiffrer, on remplace simplement la lettre claire par un des trois ou quatre nombres qui se trouvent sous elle.

DECHIFFRER :

369391
679419
266687
699983

HOMOPHONIQUE

MONOALPHABETIQUES

SUBSTITUTION HOMOPHONIQUE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Un procédé qui constitue un réel progrès sur les précédents, au point de vue de la sécurité, consiste dans le remplacement de chacune des lettres du texte clair par un ou plusieurs groupes de chiffres, de façon à faire disparaître complètement les indications fournies par la fréquence.

Voici deux grilles de substitution possibles pour la langue française qui utilise soit tous les nombres de 00 à 99, soit les lettres.

A B R A C A D A B R A pourra être chiffré ici

33 24 92 15 03 96 61 55 24 21 57

Lettre	Fréquence	Scrabble	Symboles de substitution
a	8.40 %	9 %	15, 33, 37, 55, 57, 72, 91, 96
b	1.06 %	2 %	24
c	3.03 %	2 %	03, 39, 67
d	4.18 %	3 %	04, 43, 61, 88
e	17.26 %	15 %	08, 12, 20, 46, 47, 48, 53, 59, 64, 76, 79, 80, 81, 85, 90, 94, 97
f	1.12 %	2 %	40
g	1.27 %	2 %	29
h	0.92 %	2 %	05
i	7.34 %	8 %	14, 45, 50, 73, 82, 93, 99
j	0.31 %	1 %	11
k	0.05 %	1 %	77
l	6.01 %	5 %	01, 16, 26, 60, 71, 98
m	2.96 %	3 %	34, 87
n	7.13 %	6 %	06, 17, 22, 30, 31, 49, 58
o	5.26 %	6 %	02, 10, 41, 66, 89
p	3.01 %	2 %	13, 18, 83
q	0.99 %	1 %	36
r	6.55 %	6 %	21, 25, 65, 68, 92, 95
s	8.08 %	6 %	00, 28, 51, 52, 63, 74, 78, 84
t	7.07 %	6 %	07, 19, 23, 35, 38, 54, 70
u	5.74 %	6 %	09, 32, 42, 69, 75
v	1.32 %	2 %	44
w	0.04 %	1 %	56
x	0.45 %	1 %	86
y	0.30 %	1 %	62
z	0.12 %	1 %	27

On remarque que le "a" a été chiffré chaque fois différemment.
Cette méthode empêche donc un décryptement par l'analyse des fréquences, puisque ces dernières seront quasiment identiques.

	Z V O F	W P G	X Q H	R I	J
Y, S, K, A	e	a	t	d	g
T, L, B	s	i	u	m	h
U, M, C	r	n	l	f	y
N, D	o	c	p	v	z
E	q	b	x	j	k

MONOALPHABETIQUES

SUBSTITUTION HOMOPHONIQUE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

L'inconvénient majeur de ces dernières méthodes est que le chiffre est quasiment impossible à mémoriser, ce qui nécessite que l'envoyeur et le destinataire aient une version écrite de la table de conversion. Si cette table tombe entre des mains indiscrète, toute la sécurité est compromise. Il existe cependant un moyen simple d'éviter cela : il suffit que les protagonistes s'entendent sur une page d'un livre (de la même édition). Le message crypté sera une suite de nombres qui indiqueront les rangs des lettres dans le texte de la page. C'est le système du dictionnaire (ou chiffre du livre).

POLYALPHABETIQUES →

- TRITHEME
- PORTA
- ALBERTI
- VIGENERE

MONOALPHABETIQUES

SUBSTITUTION HOMOPHONIQUE

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le physicien italien Giovanni Battista Della Porta fut l'inventeur du premier système littéral à double clef, c'est-à-dire le premier chiffre pour lequel on change d'alphabet à chaque lettre. Ce système polyalphabétique était extrêmement robuste pour l'époque, à tel point que beaucoup considèrent Porta comme le "père de la cryptographie moderne". Della Porta a inventé son système de chiffrement en 1563, et il a été utilisé avec succès pendant trois siècles.

Porta emploie 11 alphabets différents et réversibles qu'il désigne par AB, CD, etc. Ce tableau peut être étendu à 13 alphabets.

Pour ne pas obliger les correspondants à prendre les treize alphabets à la suite, Porta propose de n'en adopter que cinq ou six et de convenir d'un mot-clef dont les lettres indiqueront les alphabets qu'il faudra successivement choisir. Ce mot constitue la clef du cryptogramme.

Par exemple, si le mot-clef est ACIER, on utilisera successivement les alphabets A, C, I, E, R, A, C, etc. pour chiffrer le message. Si l'on chiffre la phrase "chiffre de Porta" avec la clef ACIER, on obtiendra :

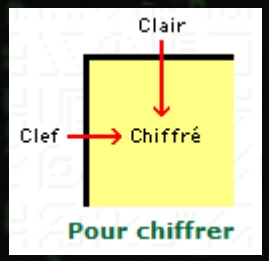
Clair	c	h	i	f	f	r	e	d	e	p	o	r	t	a
Clef	A	C	I	E	R	A	C	I	E	R	A	C	I	E
Codé	P	T	R	Q	X	E	Q	Z	P	K	B	F	K	Y

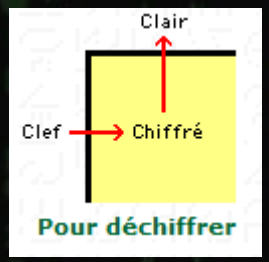
AB	a b c d e f g h i j k l m n o p q r s t u v w x y z
CD	a b c d e f g h i j k l m z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m r s t u v w x y z n o p q
UV	a b c d e f g h i j k l m q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m o p q r s t u v w x y z n

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Dans le cinquième volume de ses six livres intitulés Polygraphiae, Jean Trithème décrit une table qu'il a imaginée et nommée tabula recta. Dans cette table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche de une lettre pour chaque nouvelle rangée. En 1586, Blaise de Vigenère reprend cette idée dans son livre Traicté des chiffres.





	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
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

clair MONMESSAGE

clef MACLEFMACL

chiffré YOPXIXEAIP

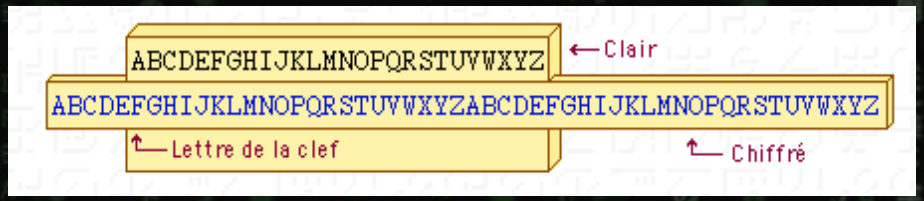
POLYALPHABETIQUES

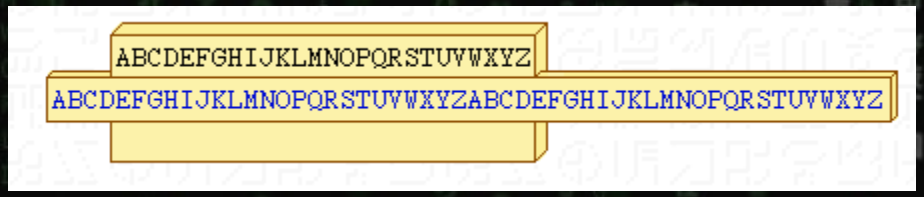
CHIFFRE DE VIGENERE

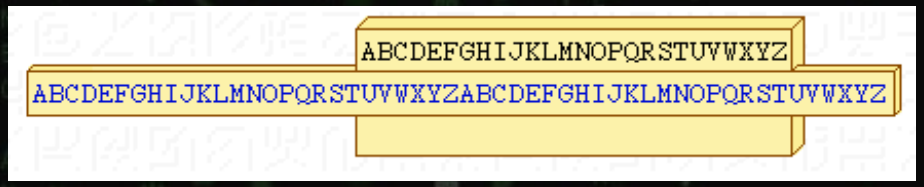
TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

L'emploi du carré de Vigenère est souvent sujet à erreurs : la lecture en est pénible et, à la longue, fatigante. Beaucoup de cryptologues préfèrent se servir d'une "réglette", facile à construire, et d'un maniement plus rapide.







Chiffre de cesar
Chiffre monoalphabetique
Chiffre polyalphabetique
sans / avec mot-cle

Ici le mot-clé est FEU

Le message "SAINT CYR" sera chiffré "XECSX WDV"

POLYALPHABETIQUES

CHIFFRE DE VIGENERE

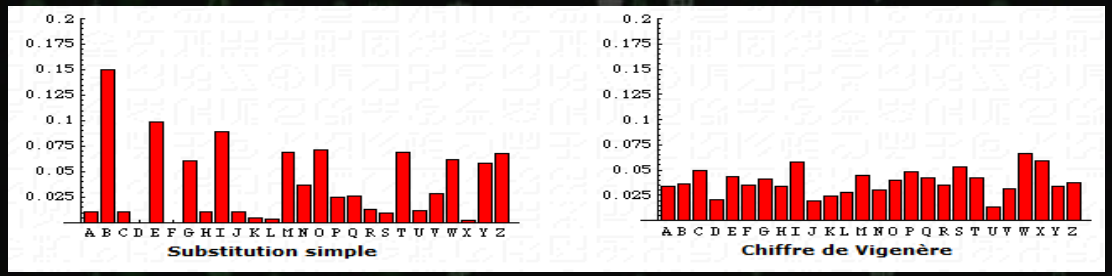
TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières ce qui rend inutilisable l'analyse des fréquences classique. Comparons les fréquences des lettres d'une fable de la Fontaine (Le chat, la belette et le petit lapin) chiffrée avec une substitution simple et celles de la même fable chiffrée avec le chiffre de Vigenère :



Ce chiffre, qui a résisté trois siècles aux cryptanalystes, est pourtant relativement facile à casser, grâce à une méthode mise au point indépendamment par Babagge et Kasiski (vers 1850). Une autre méthode complètement différente a été encore mise au point plus tard par le commandant Bazeries (vers 1900).

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Trois variantes du chiffre de Vigenère :

- Le chiffre de BEAUFORT (1774–1857) : Au lieu d'additionner la clef au message clair, Beaufort soustrait le message clair de la clef.

Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Clair	C	H	I	F	F	R	E	D	E	B	E	A	U	F	O	R	T
Décalage	-2	-7	-8	-5	-5	-17	-4	-3	-4	-1	-4	0	-20	-5	-14	-17	-19
Chiffré	Z	T	U	C	Z	U	E	B	N	A	W	C	N	Z	X	R	L

- Le chiffre de GRONSFELD (vers 1734) : Il améliore le chiffre de César en utilisant un décalage variable donné sous forme d'une clef numérique. C'est une variante du chiffre de Vigenère, la différence étant qu'il n'y a que 10 décalages possibles au lieu de 26.

Clair	C	H	I	F	F	R	E	D	E	G	R	O	N	S	F	E	L	D
Clef (décalages)	1	7	3	4	1	7	3	4	1	7	3	4	1	7	3	4	1	7
Chiffré	D	O	L	J	G	Y	H	H	F	N	U	S	O	Z	I	I	M	K

- Le masque jetable

TROISIEME STRATEGIE : CRYPTER

APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Le masque jetable est le seul algorithme de cryptage connu comme étant **indécryptable**. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair. (Gilbert Vernam en 1917)

Pour chiffrer un texte de manière sûre avec le chiffre de Vigenère, vous devez :

1. choisir une clef aussi longue que le texte à chiffrer,
2. utiliser une clef formée d'une suite de caractères aléatoires,
3. protéger votre clef,
4. ne jamais réutiliser une clef,
5. écrire des textes clairs ne contenant que les lettres (sans ponctuation et sans espaces).

Le problème ici est de communiquer les clefs de chiffrage ou de trouver un algorithme de génération de clef commun aux deux partenaires.

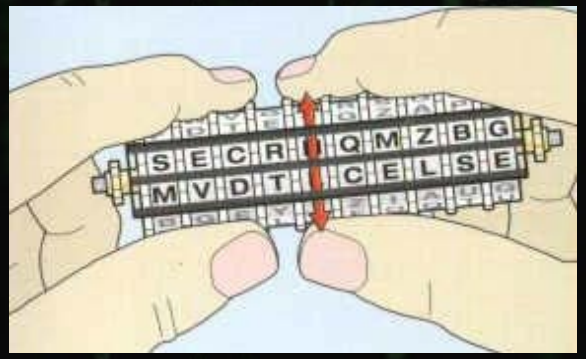
Il est couramment utilisé de nos jours par les États. Ceux-ci peuvent communiquer les clefs à leurs ambassades de manière sûre via la valise diplomatique.

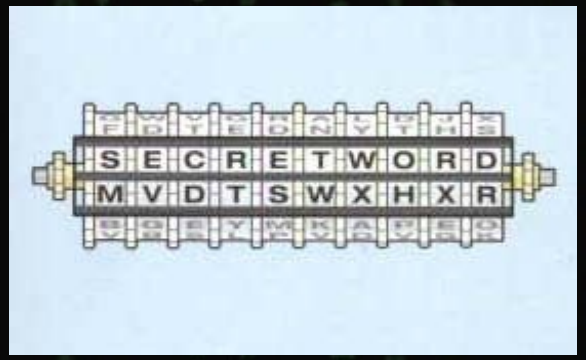
COURS Eii – Cryptographie
M. Bonneton

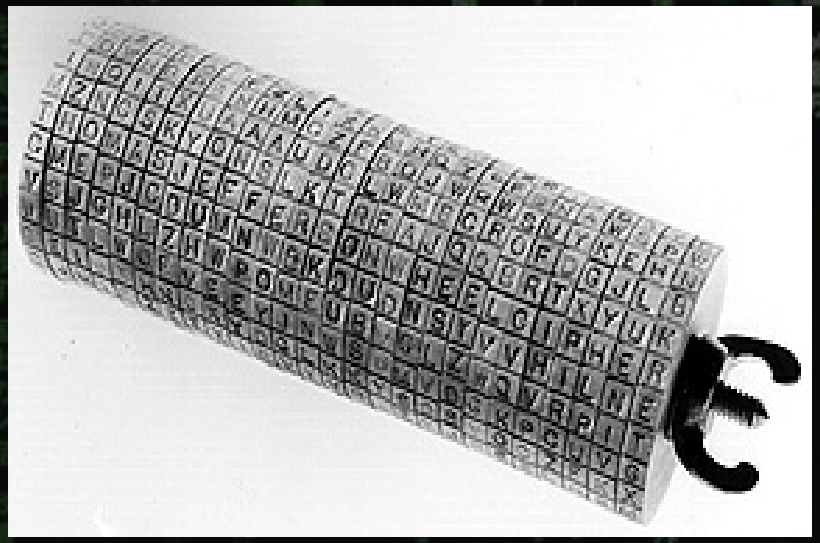
TROISIEME STRATEGIE : CRYPTER

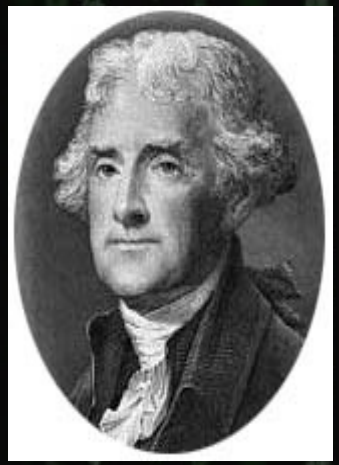
APPROCHE 02 : LE CHIFFRE DE SUBSTITUTION

Découvrons le cylindre de Thomas Jefferson (1743-1826) avant de tenter de briser le chiffre de Vigenère.









POLYALPHABETIQUES

CYLINDRE JEFFERSON

TROISIEME STRATEGIE : CRYPTER

CASSER LE CHIFFRE DE VIGENERE : METHODE DE BAZERIES

La méthode se base sur l'existence d'un mot probable et préconise la recherche du mot-clef. Étant donné un cryptogramme chiffré au moyen du chiffre de Vigenère et renfermant un mot supposé connu, on "soustrait" le mot probable à une séquence du message chiffré de même longueur jusqu'à ce que la clef apparaisse. Soit le cryptogramme :

BILKO PFFGM LTWOE WJCFD SHKWO NKSEO VUSGR LWHGW FNVKW GGGFN RFHYJ VSGRF RIEKD CCGBH RYSXV KDIJA HCFFG YEFSG ZWG

qui est supposé renfermer le mot ATTAQUE. En soustrayant ATTAQUE à la séquence débutant à la première position du cryptogramme, on obtient rien de pertinent ainsi qu'en commençant en position 2. On continue ainsi jusqu'à la position 25 où l'on voit apparaître :

Chiffré	B	I	L	K	O	P	F
Clair	A	T	T	A	Q	U	E
Décalage	-0	-19	-19	-0	-16	-20	-4
Clef	B	P	S	K	Y	V	B

Position 1

Chiffré	I	L	K	O	P	F	F
Clair	A	T	T	A	Q	U	E
Décalage	-0	-19	-19	-0	-16	-20	-4
Clef	I	S	R	O	Z	L	B

Position 2

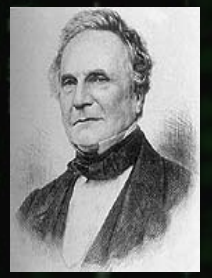
Chiffré	O	N	K	S	E	O	V
Clair	A	T	T	A	Q	U	E
Décalage	-0	-19	-19	-0	-16	-20	-4
Clef	O	U	R	S	O	U	R

Position 25

le mot OURS est apparu. C'est le mot-clef que l'on cherchait. En utilisant cette clef, le déchiffrement donne :

NOUS AVONS SUBI UNE VIOLENTE ATTAQUE CE MATIN. PERTES IMPORTANTES. DEMANDONS PILONNAGE DES POSITIONS ENNEMIES.

TROISIEME STRATEGIE : CRYPTER



CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

Charles Babbage / Friedrich Wilhelm Kasiski :

Charles Babbage (1792-1871) réussit à casser le chiffre de Vigenère, probablement en 1854 mais sa découverte resta ignorée en l'absence d'écrit. Pendant ce temps, un officier prussien à la retraite, Friedrich Wilhelm Kasiski (1805-1881), parvint au même résultat en 1863.

Dans l'exemple ci-dessous, le mot "thé" est chiffré "DPP" 2 fois et "BSS" 1 fois. Babbage comprit que des répétitions de cette sorte lui offraient la prise dont il avait besoin pour attaquer Vigenère. Il va d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte :

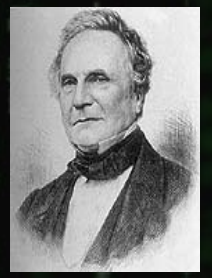
- soit la même séquence de lettres du texte clair a été cryptée avec la même partie de la clef
- soit deux suites de lettres différentes dans le texte clair auraient (possibilité très faible) par pure coïncidence

engendré la même suite dans le texte chiffré.

Le 1er cas étant le plus probable, il en déduit le nombre de facteurs de la clef puis par une méthode de fréquence de distribution des lettres cryptées il en déduit les lettres du texte clair.

K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K
t	h	e	r	u	s	s	e	t	h	e	j	a	s	m	i	n	t	h	e	c	h	i	n	e
D	P	P	F	E	A	D	S	D	P	P	X	K	A	X	W	X	B	S	S	M	P	T	B	O

TROISIEME STRATEGIE : CRYPTER



CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

C'est la faiblesse du chiffre de Vigenère : ces répétitions apparaissent parce que dans l'original, les mêmes séquences de lettres sont chiffrées avec la même partie de la clef.

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG
```

		Longueurs de clef possibles			
Séquence répétée	Espace de répétition	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

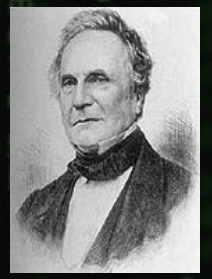
Il apparaît dans le tableau que toutes les périodes sont divisibles par 5.

Tout se cale parfaitement sur un mot-clef de 5 lettres.

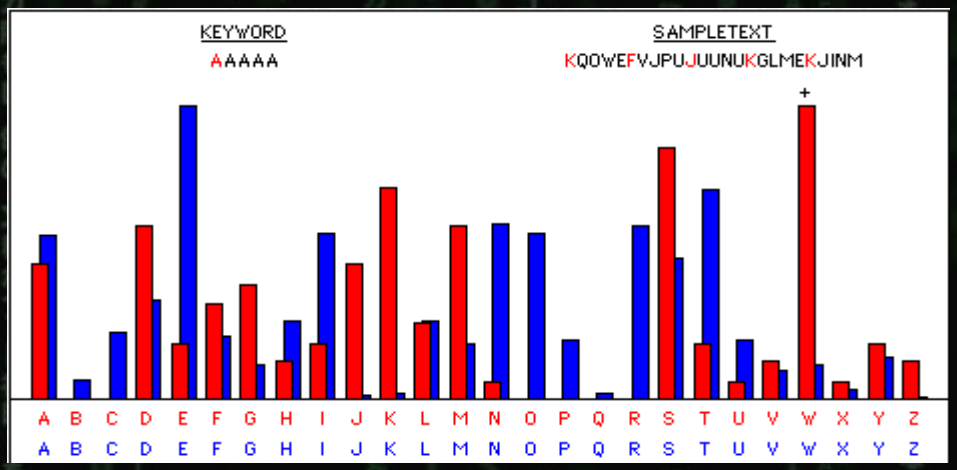
Il va falloir découvrir les lettres du mot clef : L1-L2-L3-L4-L5

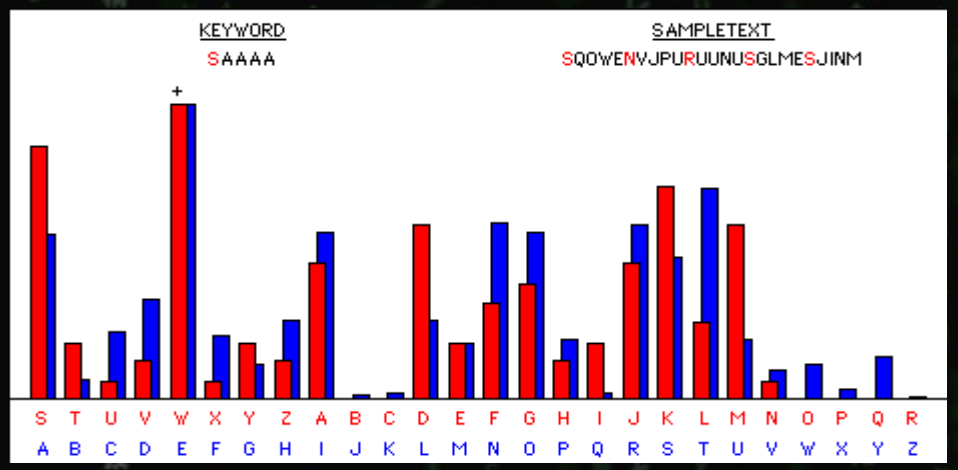
L1 représente la 1ère lettre du mot clef et ainsi de suite.

TROISIEME STRATEGIE : CRYPTER



CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

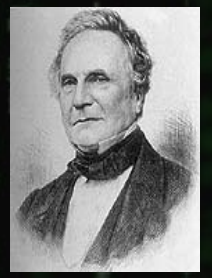




La répétition ci-dessus (en rouge) présente des traits communs avec celle de l'alphabet courant (en bleu) décalée de 18 crans. Le pic bleu le plus important se trouve sur le E et le pic rouge sur le W. En superposant les deux graphiques pour qu'ils aient la même silhouette générale, nous constatons que la 1ère lettre du mot clef L1 est S.

On recommence la même démarche pour identifier les autres lettres du mot-clef. Le mot-clef est: S C U B A

TROISIEME STRATEGIE : CRYPTER



CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG

Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers. A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux. Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait. Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.

Baudelaire

TROISIEME STRATEGIE : CRYPTER

CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

William Friedman (1891-1969) :

L'indice de Coïncidence (IC) est la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques. Il fut inventé par William Friedman et publié en 1920. Pour calculer cet indice, soient :

n = nombre de lettres du texte
n1 = nombre de A dans le texte
n2 = nombre de B dans le texte ...
n26 = nombre de Z dans le texte

$$IC = \sum_{i=1}^{26} \frac{n_i(n_i - 1)}{n(n-1)}$$

Voici quelques exemples d'indices calculés sur des textes contemporains dans différentes langues :

Langue	allemand	anglais	espagnol	esperanto	français	italien	norvégien	suédois
IC	0.072	0.065	0.074	0.069	0.074	0.075	0.073	0.071

Pour tout chiffre monoalphabétique, la distribution des fréquences est invariante, donc l'IC sera le même que pour le texte clair. Donc, si on calcule l'IC d'un texte chiffré avec un chiffre monoalphabétique, on devrait trouver IC égal environ à 0.074 (en français). Si l'IC est beaucoup plus petit (p. ex. 0.050), le chiffre est probablement polyalphabétique.

TROISIEME STRATEGIE : CRYPTER

CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers. A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux. Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait. Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.

Baudelaire

IC = 0,07389

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG
```

IC = 0,04534

POLYALPHABETIQUES

CHIFFRE DE VIGENERE

TROISIEME STRATEGIE : CRYPTER

CASSER LE CHIFFRE DE VIGENERE : DEUX AUTRES METHODES

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG
```

Sous-Chaîne intervalle de 1 : IC = 0,04534

Sous-Chaîne intervalle de 2 : IC = 0.04321, 0.04648

Sous-Chaîne intervalle de 3 : IC = 0.04509, 0.0414, 0.05046

Sous-Chaîne intervalle de 4 : IC = 0.04387, 0.044, 0.04413, 0.05049

Sous-Chaîne intervalle de 5 : IC = 0.06525, 0.07374, 0.06889, 0.0699, 0.08411 LE MOT-CLE A 5 LETTRES !

Sous-Chaîne intervalle de 6 : IC = 0.0436, 0.03791, 0.0429, 0.04408, 0.03938, 0.05348

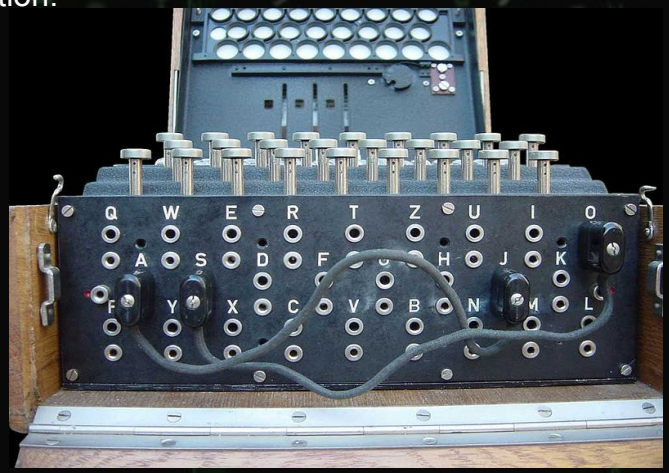
COURS Eii – Cryptographie
M. Bonneton

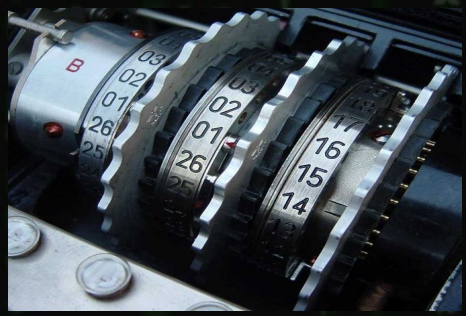
TROISIEME STRATEGIE : CRYPTER

ALLER AU-DELA DU CHIFFRE DE VIGENERE : LA MACHINE ALLEMANDE ENIGMA

L'entre-deux-guerres voit le début de la **mécanisation de la cryptographie**. Des outils mécaniques, comme les cylindres chiffrants, sont mis à disposition des opérateurs.
Ces machines fonctionnent sur le principe des **rotors** et des **contacts électriques**, afin de réaliser des formes de **substitution polyalphabétique** dont la clef a une longueur gigantesque de l'ordre de centaines de millions de lettres, au lieu de quelques dizaines dans les méthodes artisanales, comme le chiffre de Vigenère.

Enigma est la machine à chiffrer et déchiffrer qu'utilisèrent les armées allemandes du début des années trente jusqu'à la fin de Seconde Guerre Mondiale. Elle **automatise** le chiffrement par substitution.



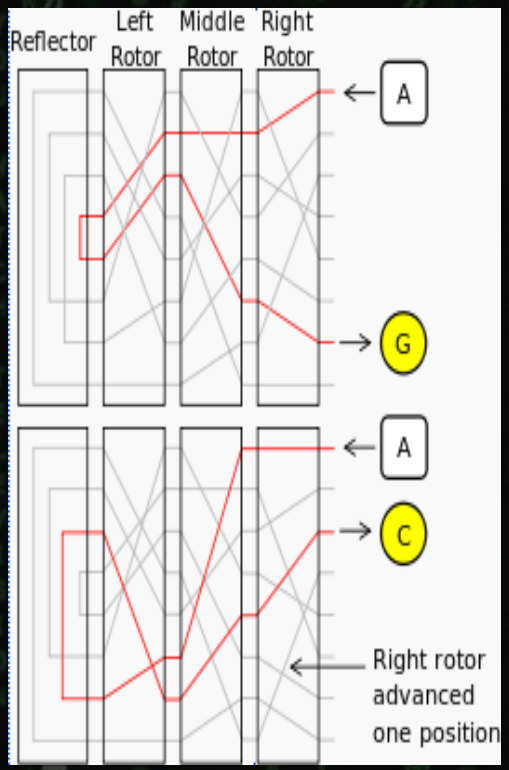


POLYALPHABETIQUES

LA MACHINE ENIGMA

TROISIEME STRATEGIE : CRYPTER

ALLER AU-DELA DU CHIFFRE DE VIGENERE : LA MACHINE ALLEMANDE ENIGMA



Quand on presse sur une touche, deux choses se passent. Premièrement, une lettre s'allume sur un panneau lumineux : c'est la **lettre chiffrée**.

Deuxièmement, un mécanisme fait **tourner le rotor** de droite d'un cran, toutes les 26 frappes, le deuxième rotor tourne d'un cran, toutes les 676 frappes, puis c'est le troisième rotor qui tourne d'un cran. Certaines Enigmas avaient 3 rotors, celles de la Kriegsmarine en avaient 4 ou 5. Ces rotors tournants modifient les connexions électriques dans la machine, ce qui fait que la touche "A" allumera peut-être le "G" la première fois, mais le "C" la deuxième, etc.

Un **tableau de connexions** et un **réflecteur** complique encore le système. Le côté exceptionnel de cette machine est que même si elle tombe entre les mains ennemies, sa sécurité n'est pas compromise. En effet, c'est le **nombre faramineux** de **réglages** de la machine qui fait sa force et les réglages changeaient évidemment chaque jour (ordre de rotors, orientation initiale et branchement du tableau de connexions) . 26 x 26 x 26 = 17 576 combinaisons liées à l'orientation des chacun des trois brouilleurs. 6 combinaisons possibles liées à l'ordre dans lequel sont disposés les brouilleurs.

100 391 791 500 branchements possibles quand on relie les six paires de lettres dans le tableau de connexions. Les machines Enigma peuvent donc chiffrer un texte selon 17 576 x 6 x 100 391 791 500= 10'000'000'000'000'000 de combinaisons différentes!

TROISIEME STRATEGIE : CRYPTER

ALLER AU-DELA DE LA MACHINE ALLEMANDE ENIGMA : BLETCHLEY PARK

Au début des années 1940, une équipe de 7000 personnes **réussit à percer le secret** des messages allemands chiffrés par la fabuleuse machine électromécanique Enigma.

Cette armée, rassemblée en grand secret à Bletchley Park, et pourvue de moyens énormes - dont **les bombes**, réunit des **mathématiciens,** des **linguistes,** des **érudits** en tout genre... et six **cruciverbistes virtuoses**, recrutés sous couvert d'un concours organisé en 1942 par le Daily Telegraph. L'opération prend le nom d'Ultra.

Cette machinerie formidable, placée sous les ordres **d'un génie, Alan Turing**, permet aux Alliés de tout savoir sur les projets des Allemands et sur les mouvements de leurs troupes. Il est à noter que toutes les informations collectées n'étaient pas utilisées de peur que les Allemands se rendent compte que leur machine Enigma n'était plus du tout sûre et qu'ils compliquent encore leur système. Beaucoup de vies alliés, notamment celles des marins des convois qui traversaient l'Atlantique, ont ainsi été sacrifiées.

POLYALPHABETIQUES

LA MACHINE ENIGMA

TROISIEME STRATEGIE : CRYPTER

ALLER AU-DELA DE LA MACHINE ALLEMANDE ENIGMA : BLETCHLEY PARK

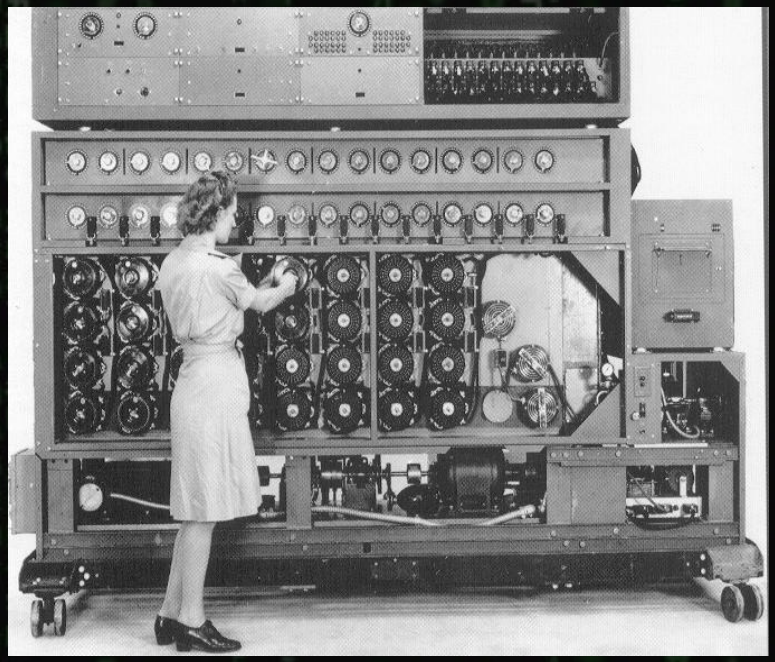
Dès 1933 et jusqu'au début de la guerre, grâce aux renseignements recueillis par un militaire français (Gustave Bertrand) et au travail de trois mathématiciens polonais **(Marian Rejewski, Jerzy Rózicki et Henryk Zygalski)**, le "Polski Biuro Szyfrów" sait décrypter les messages allemands, chiffrés avec la machine Enigma, **exploitant une faille dans la procédure de début de transmission.**

En effet, avant le message chiffré proprement dit, l'opérateur allemand choisissait au hasard les trois lettres d'une clef de message (par exemple BWE) qu'il saisissait deux fois (BWEBWE). Il notait le résultat chiffré (par exemple TCKJMY) et repositionnait les trois rotors sur BWE; il frappait ensuite le reste du message. Le début du message commençait par TCKJMY. Cette caractéristique des six premières lettres a permis aux Polonais d'attaquer Enigma.

Cette procédure est ultérieurement modifiée, et l'Enigma retrouve pour un temps ses défenses. Les Polonais décident, en 1939, devant l'imminence de l'invasion allemande, d'exposer leurs travaux aux Anglais et aux Français. Au début des années 1940, les meilleurs spécialistes anglais, dont Alan Turing, sont rassemblés en grand secret à Bletchley Park, où leur tâche principale réside dans le décryptage des messages allemands.

TROISIEME STRATEGIE : CRYPTER

ALLER AU-DELA DE LA MACHINE ALLEMANDE ENIGMA : BLETCHLEY PARK



Une bombe à Bletchley Park

Les bombes ont été construites pour retrouver le réglage de la machine Enigma. L'idée était de deviner certains mots du message et de voir si l'on pouvait faire correspondre une partie du cryptogramme avec ce mot probable.

Par exemple, le Allemands envoyaient souvent des prévisions météorologiques chiffrées avec Enigma au début de chaque transmission; on pouvait donc essayer les mots "nuages", "pluie", etc. et permettre un décryptage plus rapide.

Pour plus de détails sur la manière dont les alliés ont décrypté ENIGMA :

http://fr.wikipedia.org/wiki/Cryptanalyse_d'Enigma

Le livre de Simon Singh sur l'histoire des codes secrets en format Poche

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES :

Auguste Collon (vers 1900) a proposé de nombreux systèmes **à damiers**. Un des plus simples utilise un alphabet "carré" de 25 lettres (on enlève la lettre rare W), et on utilise les lettres de la première colonne et la dernière ligne pour indiquer les coordonnées de la lettre à chiffrer. Une lettre sera donc remplacée par un bigramme.

Dans le damier ci-dessous, formé avec la clef MERCREDI, la lettre E sera chiffrée MV (ou par VM), la lettre M sera chiffrée par MU (ou par UM). Les bigrammes sont écrits sur deux lignes ; ils sont ensuite relevés par série de longueur convenue en écrivant d'abord, dans chaque série, les lettres de la première ligne puis celles de la deuxième ligne.
Soit 7 la longueur des séries, c'est-à-dire le nombre de lettres que l'on aura convenu de lire alternativement sur la première et sur la deuxième ligne. Le chiffrement du message "Rendre compte repli" s'effectuera ainsi :

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

MMHMM MMXVZ ZXVYO MOOMM MUUVZ VXVOH IVYU

Clair	R	E	N	D	R	E	C		O	M	P	T	E	R	E		P	L	I
1ère ligne	M	M	H	M	M	M	M		O	M	O	O	M	M	M		O	H	I
2ème ligne	X	V	Z	Z	X	V	Y		U	U	V	Z	V	X	V		V	Y	U

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES : DECRYPTEMENT DU CHIFFRE DE COLLON

Le décryptement d'un message chiffré avec le chiffre de Collon se fait en deux phases :

1. Trouver la longueur des séries : Il faut pour cela essayer systématiquement les longueurs les unes après les autres (généralement il suffit d'essayer les longueurs entre 1 et 15). Pour chaque longueur, on observe les fréquences des bigrammes. Si leur histogramme correspond plus ou moins à l'histogramme des fréquences des lettres dans la langue choisie, il est très probable que la longueur des séries correspondantes soit la bonne. On écrit alors la suite des bigrammes obtenus. (Au maximum, 25)

2. Décrypter les bigrammes : Une fois la longueur des séries déterminée, on a affaire à une substitution simple. On peut donc utiliser la méthode de l'analyse des fréquences pour décrypter les bigrammes. On peut aussi tenter la méthode du mot probable.

Soit le cryptogramme suivant, sachant de plus que le message clair contient "Gérard de Nerval" :
FCNCX ZXZNR CRUVZ XNNCC ZVXYU RNCYU ZVNRC UVZXV CNCCX UZZNC CRUUV XNNCR UZZUC RRCZV VZRUN RXUXX URCFU VXZCN NCXXX ZRFNC XZZXC RRCZU ZZCCF FYXZZ CFCUZ UZUUR RCXYU XFFRN ZZXUN RNNZX ZVNFR NUUUV NNCNU ZXUNN RCVUZ ZRCRC ZZVUF RRNZX UZCRR NZVZV RCCNU XZUNR UUZXU XRRCR UXXVC NRNXU VUNCR RVXUV CCFCY ZZZRR UCVXV ZCFNR UZVUR CNRZZ ZXNRC RZUZV RCFCV ZVZRR RRUXU ZRCNC ZZUZR URFUV XZCUR NYYUZ CNVV

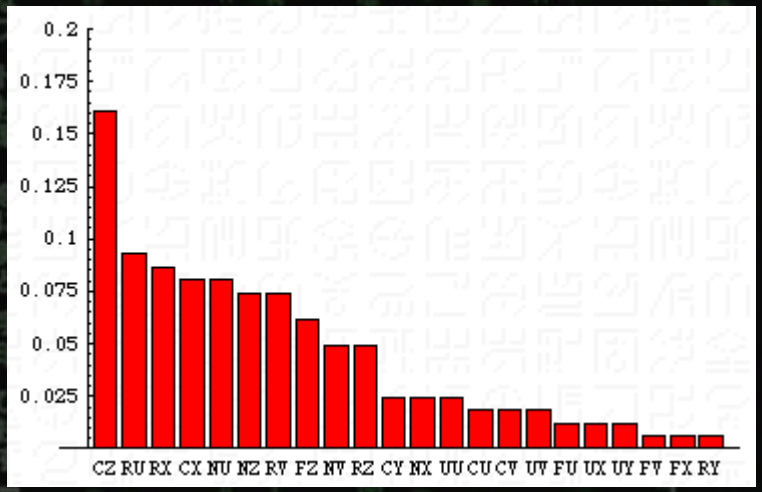
TOMOGRAMMIQUES

CHIFFRE DE COLLON

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES : DECRYPTEMENT DU CHIFFRE DE COLLON

Si la longueur des séries utilisée était de 1, nous aurions 39 bigrammes, ce qui est impossible.
Si la longueur des séries utilisée était de 2, nous aurions 42 bigrammes, ce qui est impossible.
Si la longueur des séries utilisée était de 3, nous aurions 57 bigrammes, ce qui est impossible.
Par contre, si la longueur des séries utilisée est de 4, nous avons 22 bigrammes, ce qui est possible. L'histogramme des fréquences des bigrammes est alors le suivant :



Après avoir remplacé "CZ" par "e", on obtient : FX e NX e NU RV e RX NZ NV CX CY UY RU NZ CV NV RZ CX UV CX NU e e NU CU CV RX NU NZ e RU e RV RV e RX UU NX ..... e RV RV e FV e RU RX RU RZ RZ e NU e RU UV RX FZ CY UY RU NZ CV NV

G e R A R D D e N e R V A L

On utilise ensuite la recherche du mot probable et on en déduit les autres lettres à partir de leur bigramme.

On peut alors reconstruire la table et déterminer le mot-clé.

TOMOGRAMMIQUES

CHIFFRE DE COLLON

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES :

Le chiffre bifide de Delastelle - du nom de son inventeur, le Français Félix-Marie Delastelle (1840-1902) 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.

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 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.

	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

MOT A CODER : C R Y P T O G R A P H I E X X longueur de la série : 5

1ère coord. 4 3 1 2 5 4 1 3 3 2 5 4 4 3 3

2ème coord. 1 3 2 5 5 2 4 3 2 5 4 3 5 5 5

On a donc 43 12 51 32 55 41 33 22 43 25 54 43 34 35 55 → I Y Q A T C R S I P H I K X T

TOMOGRAMMIQUES

CHIFFRE DE DELASTELLE

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES :

C'est un chiffre qui utilise un tableau contenant deux alphabets désordonnés. Les lettres du message clair sont chiffrées par bigrammes. Dans une première étape, ces bigrammes sont transformés en nombres de trois chiffres. Après un mélange simple, ces nombres sont retransformés en lettres et donnent les bigrammes chiffrés.

1	2	3	4	5	6	7	8	9
P	E	L	A	S	B	C	D	F
G	H	I	J	K	M	N	O	Q
R	T	U	V	W	X	Y	Z	#

Grille 1

Grille 2

1	2	3
4	5	6
7	8	9

Grille 3

M	C	R	1
E	F	T	2
L	G	U	3
I	H	V	4
S	J	W	5
A	K	X	6
N	O	Y	7
D	P	Z	8
B	Q	#	9

CHIFFREMENT

l	e	s	e	l	e	p	h	a	n	t	s	s	o	n	t	e	n	c	o	r	e	l	a
3	5	3				1	4	2				5	7	2				7	1	3			
1	1	1				2	1	7				2	6	1				2	7	1			
2	2	2				4	7	5				7	2	7				7	2	6			
I	G	P	M	E	F	G	E	E	N	V	S	W	E	H	R	C	O	C	L	T	M	C	K
353		111		222		142		217		475		572		261		727		713		271		726	

DECHIFFREMENT

I	G	P	M	E	F	G	E	E	N	V	S	W	E	H	R	C	O	C	L	T	M	C	K
3	1	2				1	2	4				5	2	7				7	2	7			
5	1	2				4	1	7				7	6	2				1	7	2			
3	1	2				2	7	5				2	1	7				3	1	6			
l	e	s	e	l	e	p	h	a	n	t	s	s	o	n	t	e	n	c	o	r	e	l	a
312		512		312		124		417		275		527		762		217		727		172		316	

TOMOGRAMMIQUES

LE CHIFFRE DIGRAPHIDE

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES :

Les Allemands ont utilisé, à partir de 1918, un chiffre inspiré du carré de Polybe. Les coordonnées des lettres dans le carré n'étaient pas données par des chiffres, mais par les lettres A D F G X. Ces lettres ont été choisies de façon que leurs correspondances en morse soient très différentes les unes des autres, de façon à éviter les erreurs de transmission par radio (TSF). L'originalité de ce système venait que le texte obtenu après une première substitution était ensuite soumis à une permutation des colonnes du carré. Ce chiffre, connu sous les lettres ADFGX est l'oeuvre du colonel allemand Fritz Nebel.

C'est grâce au génie de Georges-Jean Painvin, ancien major de l'école polytechnique, entré en tant que réserviste au service du chiffre, que les français vont réussir, entre avril et mai 1918, à pénétrer le système de chiffrage allemand mis en service début mars. Mais dès juin, les Allemands ne se contentent plus de leurs lettres A D F G X, voici qu'apparaît en plus la lettre V. Les Allemands utilisèrent en effet pour leurs chiffrements deux modèles de carrés : l'un de 25 lettres, l'autre de 36 symboles, ce dernier étant obtenu par l'adjonction des 10 chiffres à un alphabet complet. Le carré de substitution était construit grâce à une clef qui changeait quotidiennement.

Le chiffre utilisant le carré de 36 symboles est connu sous le nom de chiffre ADFGVX.

TOMOGRAMMIQUES

LE CHIFFRE ADFGVX

TROISIEME STRATEGIE : CRYPTER

LES SUBSTITUTIONS TOMOGRAMMIQUES :

Chiffrons, comme exemple, le texte " objectif Arras 15h28 " en utilisant la grille ci-dessous :

	A	D	F	G	V	X
A	c	1	o	f	w	j
D	y	m	t	5	b	4
F	i	7	a	2	8	s
G	p	3	0	q	h	x
V	k	e	u	l	6	d
X	v	r	g	z	n	9

Texte clair	o	b	j	e	c	t	i	f	a	r	r	a	s	1	5	h	2	8
Texte chiffré intermédiaire	AF	DV	AX	VD	AA	DF	FA	AG	FF	XD	XD	FF	FX	AD	DG	GV	FG	FV

On surchiffre ensuite le cryptoramme obtenu avec une transposition

Grille 1

M	A	R	C	E	L
A	F	D	V	A	X
V	D	A	A	D	F
F	A	A	G	F	F
X	D	X	D	F	F
F	X	A	D	D	G
G	V	F	G	F	V

Grille 2

A	C	E	L	M	R
F	V	A	X	A	D
D	A	D	F	V	A
A	G	F	F	F	A
D	D	F	F	X	X
X	D	D	G	F	A
V	G	F	V	G	F

Texte chiffré final : FDADX VVAGD DGADF FDFXF FFGVA VFXFG DAAXA F

TOMOGRAMMIQUES

LE CHIFFRE ADFGVX

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS TOMOGRAMMIQUES / POLYGRAMMIQUES :

Les substitutions tomogrammiques aussi appelées par fractions de lettres : chaque lettre est tout d'abord représentée par des groupes de deux ou plusieurs symboles, qui sont ensuite chiffrés séparément par substitution ou transposition.

(COLLON, DELASTELLES, DIGRAPHIDE, ADFGVX)

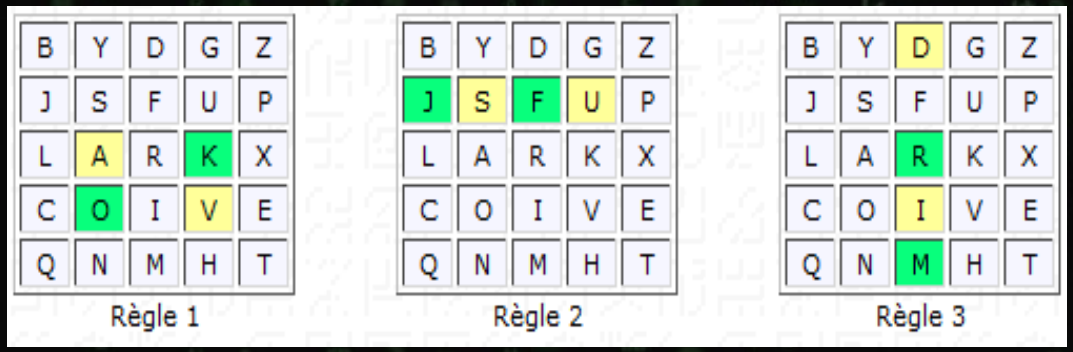
Les substitutions polygrammiques : les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement). C'est Giovanni Porta qui présenta le premier chiffre bigrammatique.

(PLAYFAIR, CHIFFREMENTS À DEUX CARRÉS, À TROIS CARRÉS, À QUATRE CARRÉS, HILL, RSA)

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES :

Le chiffre Playfair a été popularisé par Lyon Playfair, mais il a été inventé par Sir Charles Wheatstone (1854), un des pionniers du télégraphe électrique. On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. La variante anglaise consiste à garder le W et à fusionner I et J. On chiffre le texte par groupes de deux lettres (des bigrammes) en appliquant les règles suivantes :



OK → …
BI → …
JF → …
VE → …
RM → …
BJ → …

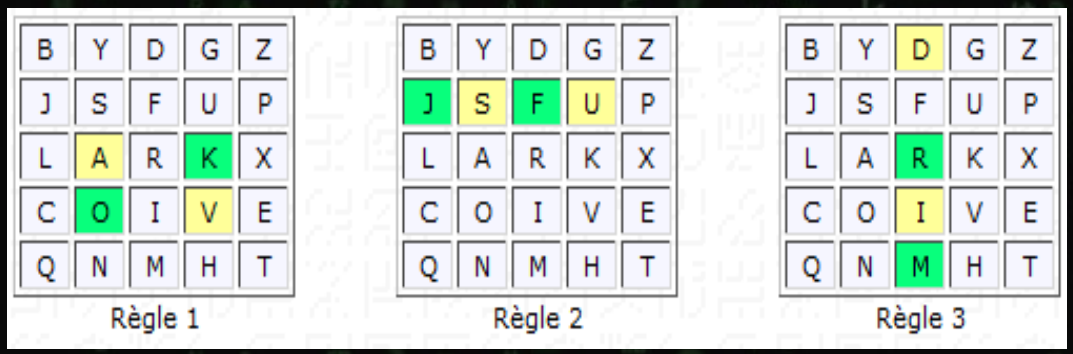
Charles Wheatstone
(1802-1875)

DECHIFFRER A L'AIDE DE LA GRILLE PRECEDENTE : DCOTSCPVOCZIVQMRRIITOTQZ

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES :

Le chiffre Playfair a été popularisé par Lyon Playfair, mais il a été inventé par Sir Charles Wheatstone (1854), un des pionniers du télégraphe électrique. On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. La variante anglaise consiste à garder le W et à fusionner I et J. On chiffre le texte par groupes de deux lettres (des bigrammes) en appliquant les règles suivantes :



OK → …
BI → …
JF → …
VE → …
RM → …
BJ → …

Charles Wheatstone
(1802-1875)

DECHIFFRER A L'AIDE DE LA GRILLE PRECEDENTE : DCOTSCPVOCZIVQMRRIITOTQZ

POLYGRAMMIQUES

BIEN JOUE CE DECHIFFREMENT B

PLAYFAIR

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES :

TECHNIQUE DE DECRYPTEMENT DU CHIFFRE DE PLAYFAIR :

Si le cryptogramme est assez long, on peut l'attaquer en regardant quels bigrammes apparaissent le plus souvent et en supposant qu'ils représentent les bigrammes les plus courants, il faut ensuite essayer de reconstituer la grille de chiffrement.

Les 20 bigrammes les plus fréquents

Bigrammes	ES	DE	LE	EN	RE	NT	ON	ER	TE	EL	AN	SE	ET	LA	AI	IT	ME	OU	EM	IE
Nombres	3318	2409	2366	2121	1885	1694	1646	1514	1484	1382	1378	1377	1307	1270	1255	1243	1099	1086	1056	1030

Les 20 trigrammes les plus fréquents

Trigrammes	ENT	LES	EDE	DES	QUE	AIT	LLE	SDE	ION	EME	ELA	RES	MEN	ESE	DEL	ANT	TIO	PAR	ESD	TDE
Nombres	900	801	630	609	607	542	509	508	477	472	437	432	425	416	404	397	383	360	351	350

TROISIEME STRATEGIE : CRYPTER

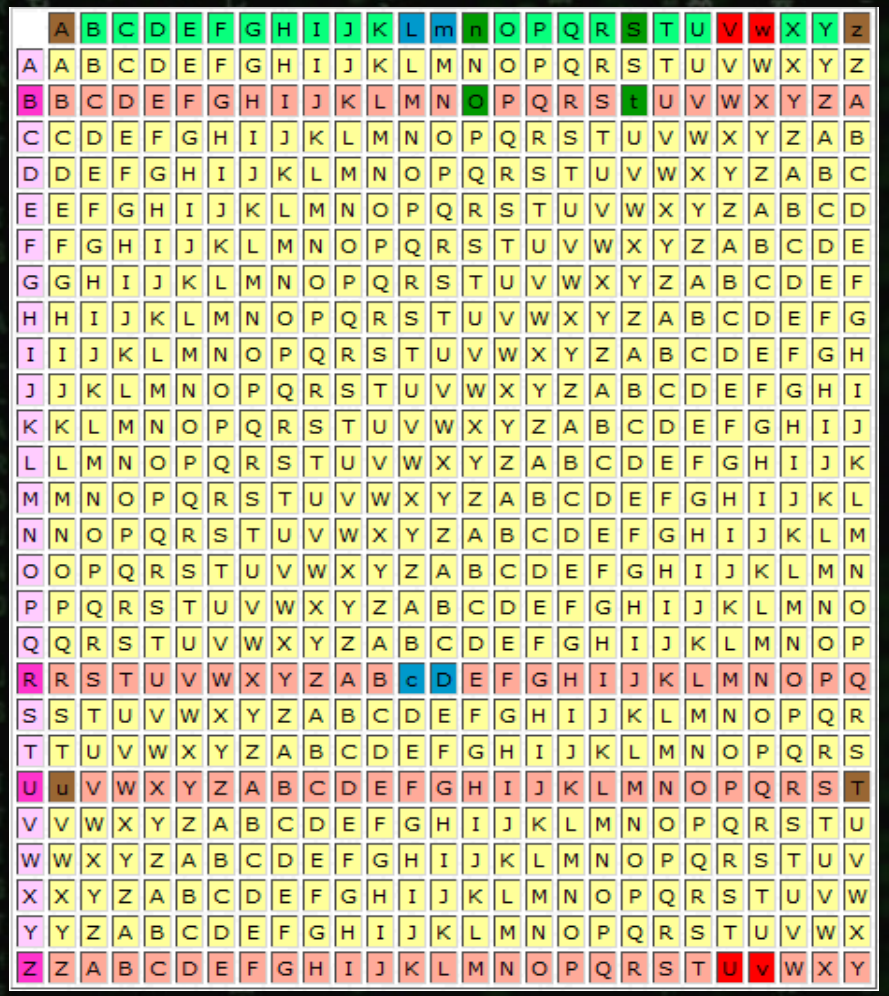
SUBSTITUTIONS POLYGRAMMIQUES :

Le chiffre Slidefair utilise le tableau de Vigenère, mais la façon de chiffrer ressemble beaucoup au chiffre Playfair. C'est un chiffre polygrammique, car les lettres sont chiffrées par bigramme.

Exemple : prenons comme mot-clef BRUZ et comme message clair "SOLDAT VU".

Le bigramme SO devient nt (rectangle vert foncé), LD devient mc (rectangle bleu), AT devient zu (rectangle brun) et VU devient wv (cas particulier, rectangle rouge).

Le message chiffré sera donc " n t m c z u w v ".



	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
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

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES :

On utilise deux grilles pour chiffrer les bigrammes. Ici, on a fabriqué les deux grilles à l'aide des 2 mots clés : ROMEO / JULIETTE

Grille 1

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

Grille 2

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

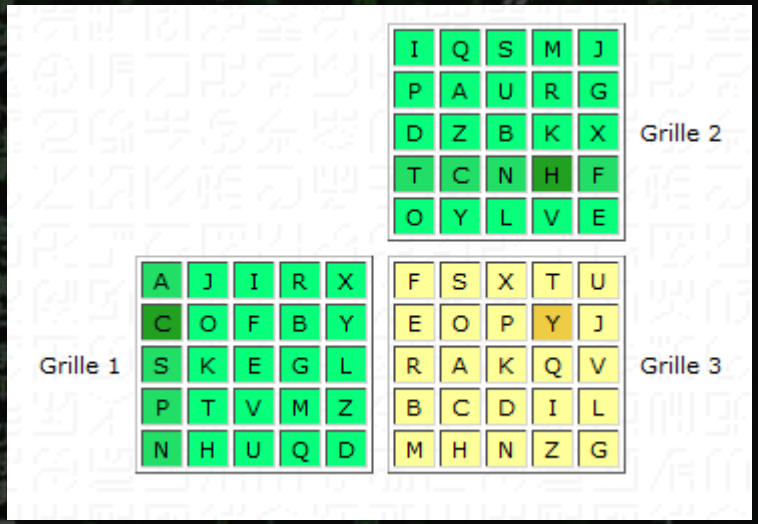
MESSAGE EN CLAIR : CE CODAGE RESSEMBLE A UN PLAYFAIR

MESSAGE CHIFFRE : DOAPA DDAER NYEKB RUFSN POIZA FMP

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES :

Cette méthode est une évolution du procédé de chiffrement à deux carrés. On utilise trois grilles carrées de dimensions 5x5 que l'on remplit avec un alphabet désordonné comme ci-dessous. Dans la version française, on élimine le W qui sera le cas échéant remplacé par le V. En anglais, on préfère supprimer le J. Une caractéristique intéressante de ce système de chiffrement est qu'un même message peut être chiffré de très plusieurs façons avec les mêmes mots de passe.



On chiffre les lettres du message clair par bigramme. Un bigramme deviendra un trigramme. À titre d'exemple, chiffrons le bigramme **C H** .

On repère le c dans la grille 1 ; la première lettre du trigramme sera une lettre quelconque choisie dans la même colonne que le c dans la grille 1.

On repère le h dans la grille 2 ; la dernière lettre du trigramme sera une lettre quelconque choisie dans la même ligne de le h dans la grille 2.

La lettre du milieu du trigramme sera la lettre de la grille 3 qui se trouve sur la même ligne que le c et la même colonne que le h.

Ainsi, le bigramme clair ch deviendra par exemple le trigramme chiffré **P Y F**. Il y a 16 possibilités si l'on exclut la lettre claire, 25 si on permet de la prendre.

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES : LE CHIFFRE AFFINE

Le chiffre affine est un chiffre de substitution simple. Il est cependant placé ici car on peut le voir comme la version unidimensionnelle du chiffre de Hill.

L'idée est d'utiliser comme fonction de chiffrage une fonction affine du type y = a x + b, où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet selon le tableau ci-dessous :

Lettre	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
Nombre	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

Pour que la lettre chiffrée (y) soit encore un nombre entre 0 et 25, on travaillera modulo 26.

La vraie formule sera donc y = (a x + b) mod 26.

ARITHMETIQUE MODULAIRE

On peut remarquer que si a=1, alors on retrouve le chiffre de César et b est le décalage.

On remarquera aussi que si b=0, alors "a" est toujours chiffré "A".

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES : ARITHMETIQUE MODULAIRE

Définissons l'arithmétique modulo m : Zm symbolise l'ensemble {0, ..., m-1} muni de deux opérations + et x. L'addition et la multiplication dans Zm fonctionnent exactement comme l'addition et la multiplication usuelles, excepté le fait que tous les résultats sont réduits modulo m.

Supposons par exemple que l'on veuille calculer 11 x 13 dans Z16. Comme entiers ordinaires, on a 11 x 13 = 143. Pour réduire 143 modulo 16, on fait une division euclidienne : 143 = 8 x 16 + 15, donc 143 mod 16 = 15, et, donc, 11 x 13 = 15 dans Z16.

143	16
15	8

Propriété importante :

L'inverse modulo n de b est le nombre entier b^{-1} tel que $b \cdot b^{-1} \bmod n = 1$

On peut le calculer avec l'algorithme d'Euclide étendu. (voir cours d'Arithmétique)

Exemple : l'inverse de 5 modulo 16 est 13 car 5 x 13 = 65 mod 16 = 1 → $5^{-1} = 13$

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES : LE CHIFFRE DE HILL

Le chiffre publié en 1929 par Lester S. Hill (1891-1961) est un chiffre polygrammique, c'est-à-dire qu'on ne (dé)chiffre pas les lettres les unes après les autres, mais par paquets. Nous étudierons ici la version bigraphique du chiffre de Hill, puisque nous grouperons les lettres deux par deux, mais on peut imaginer des paquets plus grands, par exemple des paquets de trois lettres.

Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres P_k et P_{k+1} du texte clair seront chiffrées C_k et C_{k+1} avec la formule ci-dessous :

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26}$$

Ce qui signifie que les deux premières lettres du message clair (P_1 et P_2) seront chiffrées (C_1 et C_2) selon les deux équations suivantes :

$$C_1 = a P_1 + b P_2 \pmod{26}$$

$$C_2 = c P_1 + d P_2 \pmod{26}$$

Et ainsi de suite pour les lettres suivantes.

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES : LE CHIFFRE DE HILL

CHIFFREMENT : Alice prend comme clef de cryptage la matrice $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ pour chiffrer le message MATH. Après avoir remplacé les lettres par leur rang (a=1, b=2, etc.), elle obtient :

$C_1 = 9 \cdot 13 + 4 \cdot 1 \pmod{26} = 121 \bmod 26 = 17 = Q$

$C_2 = 5 \cdot 13 + 7 \cdot 1 \pmod{26} = 72 \bmod 26 = 20 = T$

$C_3 = 9 \cdot 20 + 4 \cdot 8 \pmod{26} = 212 \bmod 26 = 4 = D$

$C_4 = 5 \cdot 20 + 7 \cdot 8 \pmod{26} = 156 \bmod 26 = 0 = Z$

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26}$$

Le message chiffré est donc QTDZ.

DECHIFFREMENT : Pour déchiffrer, le principe est le même que pour le chiffrement : on prend les lettres deux par deux, puis on les multiplie par la matrice inverse (modulo 26) de la matrice de chiffrement.

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26}$$

TROISIEME STRATEGIE : CRYPTER

SUBSTITUTIONS POLYGRAMMIQUES : LE CHIFFRE DE HILL

DECHIFFREMENT : La matrice inverse se calcule à l'aide de la formule : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On a donc :

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = (43)^{-1}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26}$$

Comme pgdc (43,26) = 1, $(43)^{-1}$ existe dans Z_{26} et $(43)^{-1}$ égale 23 . En effet, 43 . 23 = 989 modulo 26 = 38 . 26 + 1 = 1 modulo 26.

Bob a donc maintenant la matrice de déchiffrement : $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = 23\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \pmod{26} = \begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} \pmod{26} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \pmod{26}$

Bob prend donc la matrice pour déchiffrer le message "QTDZ". Après avoir remplacé les lettres par leur rang dans l'alphabet (A=1, B=2, etc.), il obtiendra :

$P_1 = 5 \cdot 17 + 12 \cdot 20 \pmod{26} = 325 \bmod 26 = 13 = M$

$P_2 = 15 \cdot 17 + 25 \cdot 20 \pmod{26} = 755 \bmod 26 = 1 = A$

$P_3 = 5 \cdot 4 + 12 \cdot 0 \pmod{26} = 20 \bmod 26 = 20 = T$

$P_4 = 15 \cdot 4 + 25 \cdot 0 \pmod{26} = 60 \bmod 26 = 8 = H$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26}$$

TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE

La cryptographie entre dans son ère moderne avec l'utilisation intensive des ordinateurs vers 1970. Dans la cryptographie moderne, on utilise aussi des problèmes mathématiques que l'on ne sait pas encore résoudre, comme par exemple **factoriser des grands nombres** (chiffre RSA).

Plus anecdotique, on voit aussi apparaître les deux personnages récurrents les plus célèbres de la cryptographie : Alice et Bob

TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LE CHIFFREMENT PAR BLOCS

Les algorithmes de chiffrements par blocs sont actuellement les algorithmes à clef secrète les plus courants. Cependant, depuis l'invention du DES en 1977, la puissance de calcul des ordinateurs a incroyablement progressé, si bien que la longueur des clefs est maintenant insuffisante. L'AES (Advanced Encryption Standard) est destiné à prendre la relève du DES, réputé peu sûr depuis quelques années. Après une mise au concours, le NITS (censé définir la norme pour le territoire américain, mais dont l'influence dépasse les frontières du pays), a choisi parmi de nombreux candidats pour l'AES un algorithme nommé Rijndael, conçu par des cryptologues belges, Vincent Rijmen et Joan Daemen.

L'idée générale du chiffrement par blocs est la suivante :

1/ Remplacer les caractères par un code binaire (par ex. le code ASCII en base 2). On obtient ainsi une longue chaîne de 0 et de 1

2/ Découper cette chaîne en blocs de longueur donnée, par exemple 64 bits.

3/ Chiffrer un bloc en l'additionnant bit par bit à une clef.

4/ Déplacer certains bits du bloc.

5 /Recommencer éventuellement un certain nombre de fois l'opération 3. On appelle cela une ronde.

6/ Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

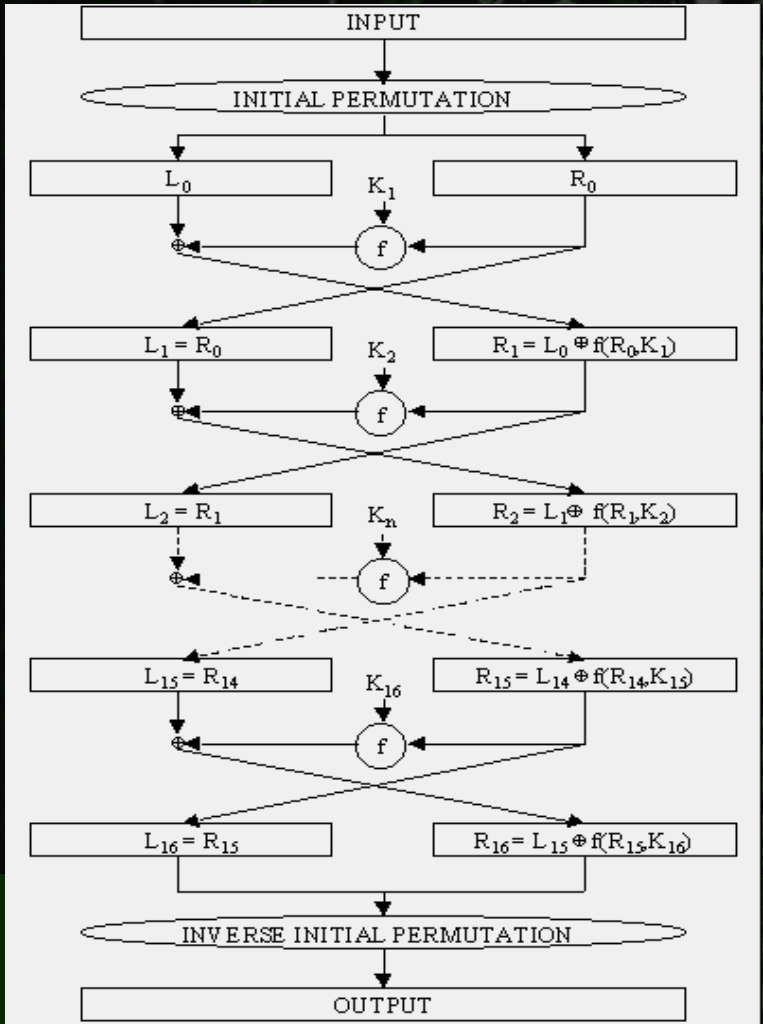
TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LE CHIFFREMENT PAR BLOCS

Schéma général du DES
(Data Encryption Standard)
qui fut le chiffrement par blocs
le plus utilisé de 1977 à 1999.
(clés de 56 bits)

Remplacé ensuite par le triple DES.

Le standard DES a été remplacé
en 2001 par l'AES : un algorithme
nommé Rijndael,
conçu par des cryptologues belges,
Vincent Rijmen et Joan Daemen
(Advanced Encryption Standard).
(clés de 128 bits)



Famille des réseaux de Feistel

un bloc de texte en clair est découpé en deux ; la transformation de ronde est appliquée à une des deux moitiés, et le résultat est combiné avec l'autre moitié par ou exclusif. Les deux moitiés sont alors inversées pour l'application de la ronde suivante.

TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LE CHIFFREMENT PAR BLOCS

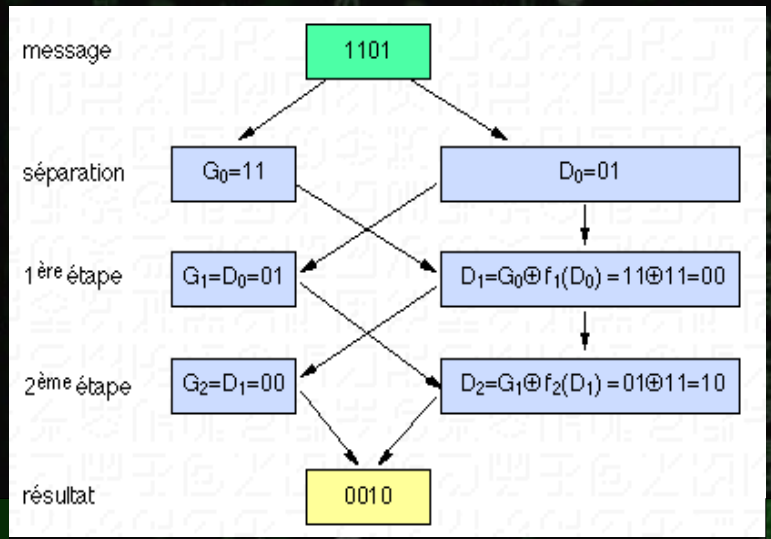
À titre d'exemple, nous allons chiffrer par un réseau de Feistel à deux rondes un message constitué de quatre bits (16 possibilités de messages), ce qui revient à construire une bijection de quatre bits vers quatre bits à partir de deux fonctions f1 et f2 de deux bits vers deux bits. Nous considérerons que pour une certaine clef entrée, ces fonctions sont les suivantes :

entrée f1	*sortie*
00	01
01	11
10	10
11	01

entrée f2	*sortie*
00	11
01	00
10	00
11	01

On peut "additionner" deux bits à l'aide de la fonction XOR (symbolisée par un + entouré d'un cercle) donnée par le tableau ci-dessous. Chiffrons le message 1101. G désigne la moitié gauche du message à chiffrer, D la moitié droite.

XOR	0	1
0	0	1
1	1	0



CRYPTER
QUELQUES MESSAGES

PARMI LES 16 POSSIBLES.

TROISIEME STRATEGIE : CRYPTER

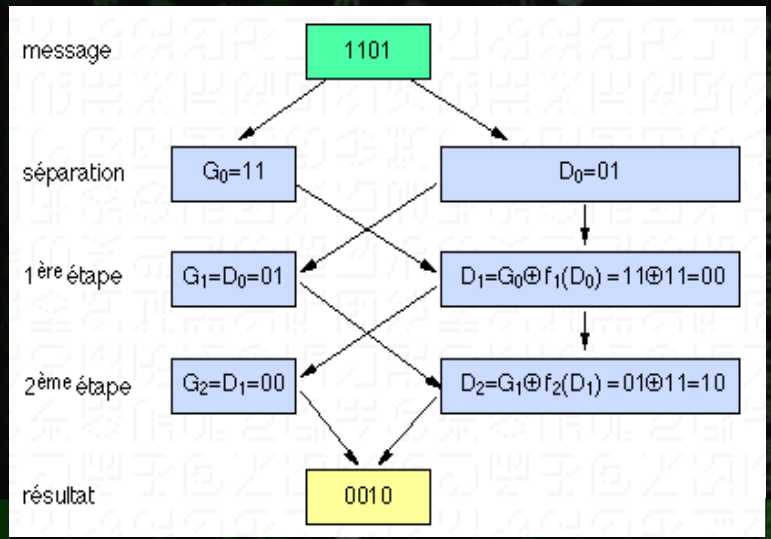
LA CRYPTOGRAPHIE MODERNE : LE CHIFFREMENT PAR BLOCS

À titre d'exemple, nous allons chiffrer par un réseau de Feistel à deux rondes un message constitué de quatre bits (16 possibilités de messages), ce qui revient à construire une bijection de quatre bits vers quatre bits à partir de deux fonctions f1 et f2 de deux bits vers deux bits. Nous considérerons que pour une certaine clef entrée, ces fonctions sont les suivantes :

entrée f1	*sortie*
00	01
01	11
10	10
11	01
entrée f2	*sortie*
00	11
01	00
10	00
11	01

On peut "additionner" deux bits à l'aide de la fonction XOR (symbolisée par un + entouré d'un cercle) donnée par le tableau ci-dessous. Chiffrons le message 1101. G désigne la moitié gauche du message à chiffrer, D la moitié droite.

XOR	0	1
0	0	1
1	1	0



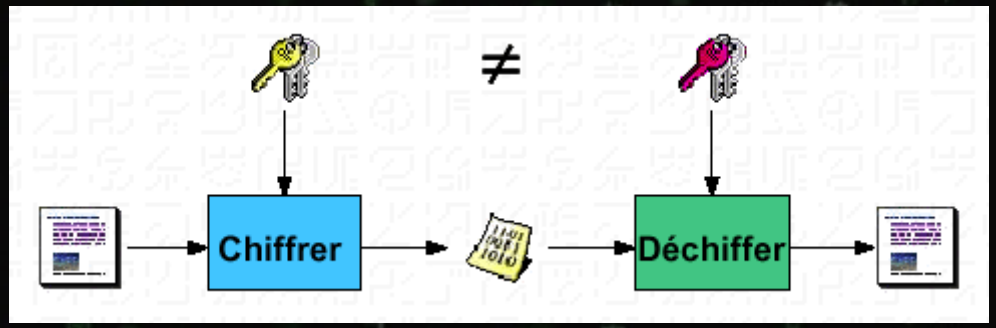
message	résultat
0000	0100
0001	1100
0010	1010
0011	0111
0100	0011
0101	1001
0110	1111
0111	0000
1000	1101
1001	0101
1010	0001
1011	1110
1100	1000
1101	0010
1110	0110
1111	1011

TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LES SYSTEMES À CLEFS PUBLIQUES

Depuis les origines de la cryptographie, et jusqu'à récemment, tous les procédés étaient basés sur une même notion fondamentale : chaque correspondant était en possession d'une **clef secrète**, qu'il utilisait pour chiffrer et déchiffrer. Cela a un inconvénient majeur : comment communiquer la clef au correspondant ? Il faut pour cela utiliser un canal sûr (par exemple une valise diplomatique). Il faut donc un contact préalable avec la personne qui devra (dé)chiffrer nos messages.

Le milieu des années 1970 a vu l'avènement d'une nouvelle méthode de cryptage : le système à clefs publiques. L'idée de ce système a été proposée en 1976 par Diffie et Hellman, qui ont proposé une méthode totalement nouvelle : une clef pour chiffrer et une autre pour déchiffrer.

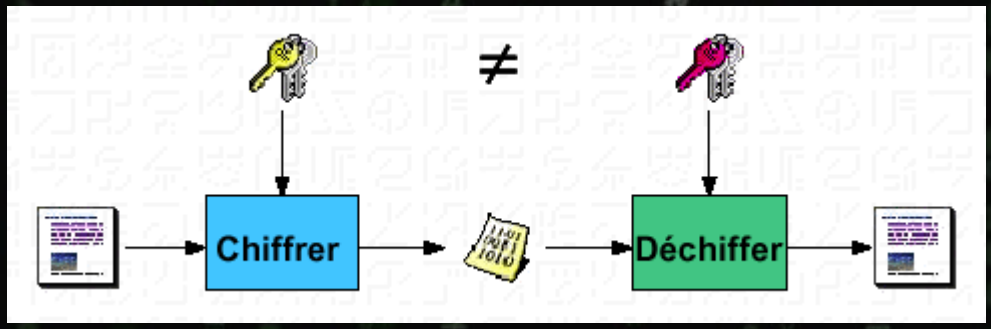


TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LES SYSTEMES À CLEFS PUBLIQUES

Il existe un lien mathématique entre ces deux clefs, mais ce lien est constitué par une **«fonction trappe à sens unique»**. Cette fonction permet de calculer aisément la clef de chiffrement en connaissant la clef de déchiffrement. En revanche, l'opération inverse est pratiquement impossible.

L'intérêt de ce système est considérable. En effet, toute personne ou toute entreprise disposant de moyens informatiques peut élaborer sa clef de déchiffrement - qu'elle garde secrète pour son usage exclusif - puis en déduire la clef de chiffrement correspondante. Tous les utilisateurs de ce système agissant de même, les clefs de chiffrement peuvent ensuite être groupées dans une sorte d'annuaire mis à la disposition du public. Ainsi deux correspondants peuvent-ils communiquer secrètement sans aucun contact préalable. Les systèmes à clefs publiques les plus connus sont RSA et PGP.



TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE : LES SYSTEMES À CLEFS PUBLIQUES : RSA

1978 (Rivest, Shamir et Adleman). On appelle Alice la personne qui désire recevoir un message chiffré, et Bob celle qui envoie le message.

1. Choix de la clef RSA : Alice choisit deux grands entiers naturels premiers p et q (d'environ 100 chiffres ou plus) et fait leur produit n = p·q. Puis elle choisit un entier e premier avec (p-1)·(q-1). Enfin, elle publie dans un annuaire, par exemple sur le web, sa clef publique : (RSA, n, e).

2. Chiffrement texte : Bob veut donc envoyer un message à Alice. Il cherche dans l'annuaire la clef de chiffrement qu'elle a publiée. Il sait maintenant qu'il doit utiliser le système RSA avec les deux entiers n et e. Il transforme en nombres son message en remplaçant chaque lettre par son rang dans l'alphabet. Puis il découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que n. Cette opération est essentielle, car si on ne faisait pas des blocs assez longs, on retomberait sur un simple chiffre de substitution que l'on pourrait attaquer par l'analyse des fréquences. Un bloc B est chiffré par la formule $C = B^e \bmod n$, où C est un bloc du message chiffré que Bob enverra à Alice.

3. Déchiffrement code : Alice calcule à partir de p et q, qu'elle a gardés secrets, la clef d de déchiffrage (c'est sa clef privée). Celle-ci doit satisfaire l'équation $e \cdot d \bmod ((p-1).(q-1)) = 1$. Chacun des blocs C du message chiffré sera déchiffré par la formule $B = C^d \bmod n$.

TROISIEME STRATEGIE : CRYPTER

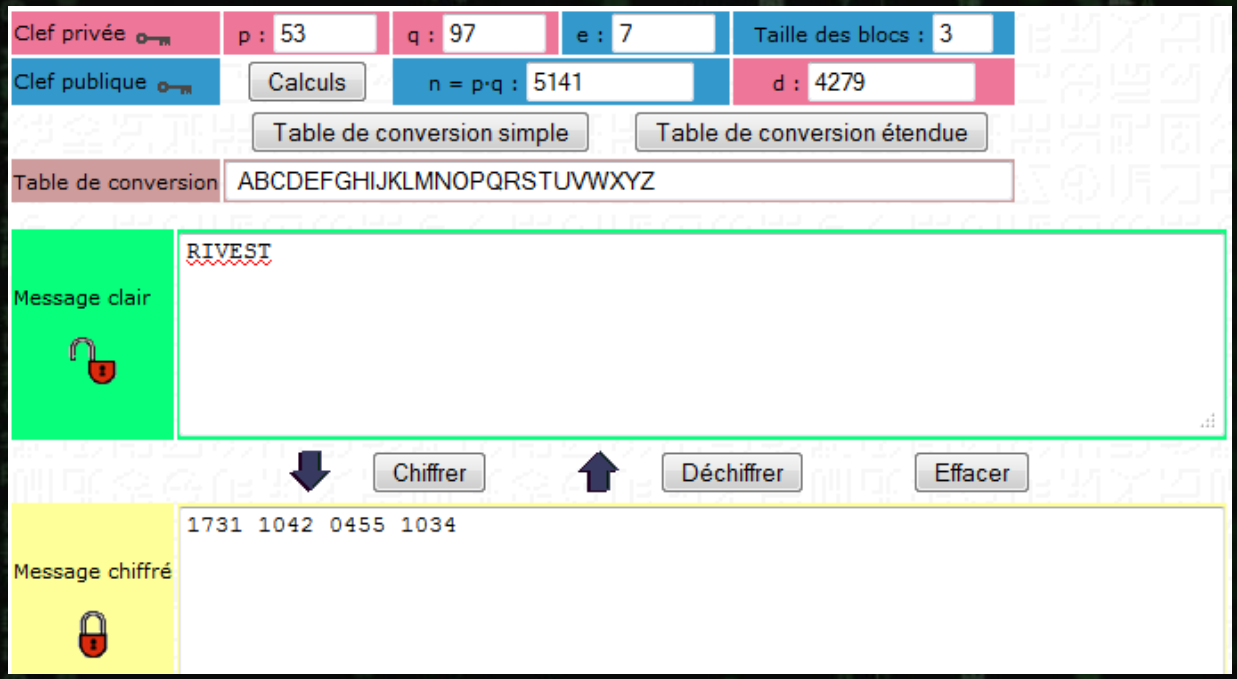
LA CRYPTOGRAPHIE MODERNE : LES SYSTEMES À CLEFS PUBLIQUES : RSA

Tout l'intérêt du système RSA repose sur le fait qu'à l'heure actuelle il est pratiquement impossible de retrouver dans un temps raisonnable p et q à partir de n si celui-ci est très grand (ou alors, si c'est possible, les cryptanalystes qui ont trouvé la méthode la gardent secrète). Alice est donc la seule à pouvoir calculer d dans un temps court. De plus, elle n'a jamais à transmettre les entiers p et q, ce qui empêche leur piratage.

Clé publique d' Alice :
(RSA, 5141, 7)

Bob calcule :

$180^{7} \bmod 5141 = 1731$
$922^{7} \bmod 5141 = 1042$
$051^{7} \bmod 5141 = 0455$
$920^{7} \bmod 5141 = 1034$



Message à crypter
R I V E S T
18 09 22 05 19 20
Blocs de 3 chiffres
180 922 051 920

Alice calcule :

$1731^{4279} \bmod 5141 = 180$
$1042^{4279} \bmod 5141 = 922$
$0455^{4279} \bmod 5141 = 051$
$1034^{4279} \bmod 5141 = 920$

TROISIEME STRATEGIE : CRYPTER

LA CRYPTOGRAPHIE MODERNE ET SON EVOLUTION FUTURE

RECAPITULATIF

CACHER : LA STEGANOGRAPHIE → encres sympathiques ; ave maria Trithème ; grille de Cardan ; alphabet bilitère de Bacon ; semagrammes et genres littéraires (Musset et Sand)

CODER : LES SYSTEMES → Mary Stuart ; Popham (marine) ; Morse ; ASCII ; Navajo

CRYPTER : LA TRANSPOSITION → Scytale ; rail fence ; grille tournante ; trans. rectangulaire ; double transposition

LA SUBSTITUTION →
- **MONOALPHABETIQUES** → Carré de Polybe ; alphabets désordonnés ; chiffre de César ; hébreux ; pig pen ; templiers ; homophoniques
- **POLYALPHABETIQUES** → Chiffre de Porta ; Vigenère ; masque jetable ; Cylindre de Jefferson ; machine Enigma
- **TOMOGRAMMIQUES** → Collon ; Delastelle ; digraphide ; ADFGVX
- **POLYGRAMMIQUES** → Playfair ; slidefair ; à 2 ou 3 carrés ; Hill

MODERNE (INFORMAT.) →
- **PAR BLOCS** → DES ; AES ; Rijndael
- **PAR CLES PUBLIQUES** → RSA