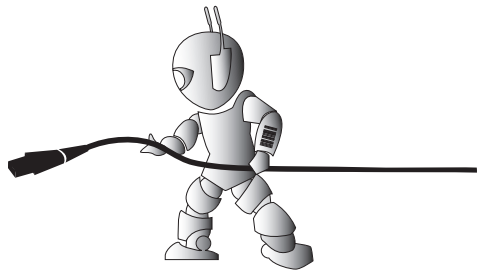
Chiffrement et authentification

Introduction

Tuyêt Trâm DANG NGOC
<dntt@u-cergy.fr>

Université de Cergy-Pontoise

2012–2013



DÉPARTEMENT
Sciences Informatiques

Plan

DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Historique des messages secrets

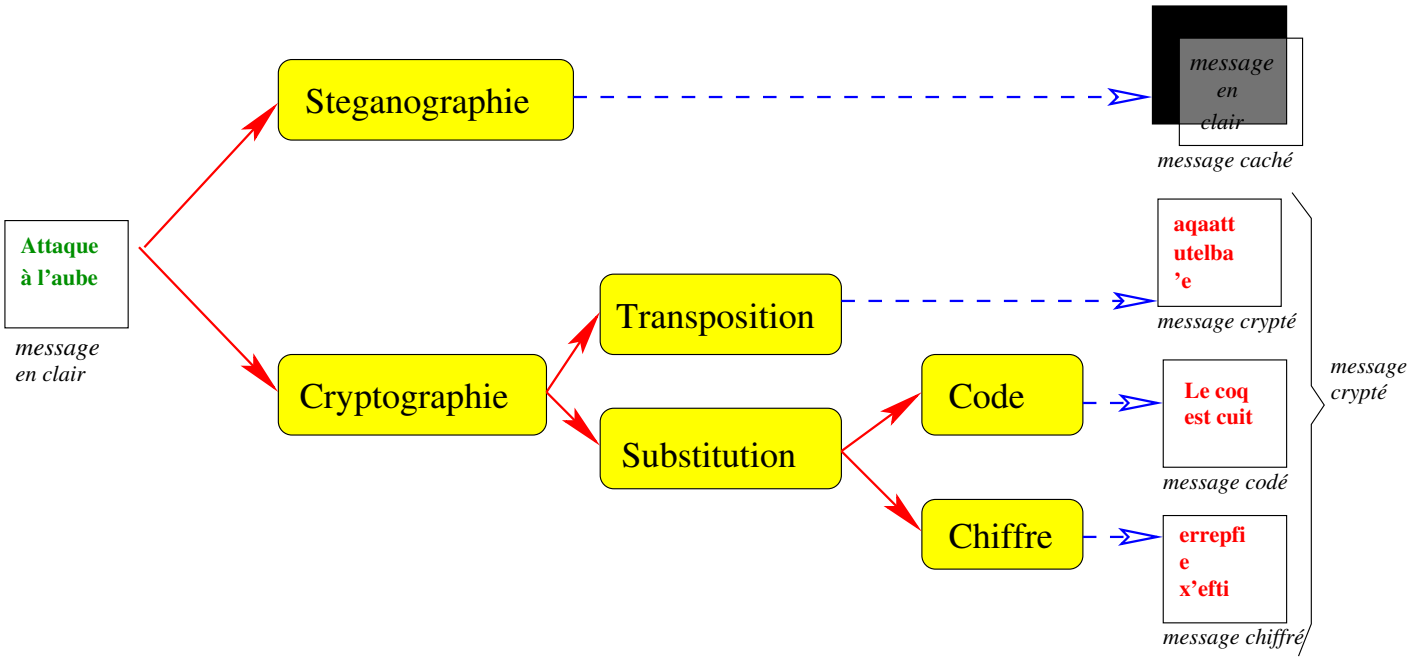
Apparu presque en même temps que l'écriture dans le domaine militaire.

- Protéger ses écrits des indiscrets.
- Être lisible par le destinataire de l'écrit.

Les besoins

- Confidentialité : s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé
- Intégrité : l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle
- Signature :
  - Authentification : procédure qui consiste à vérifier l'identité d'une entité (personne, ordinateur...)
  - Non-répudiation : assure que le message ne peut être remis en cause par l'un des partis.
  - Horodatage : certifier des heures et des dates de signature électronique et renforcer la fonction de non répudiation

Classification des méthodes



DÉPARTEMENT
Sciences Informatiques

Stéganographie

On cache le message

- Dans la doublure des vêtements, un double fond, etc.
- Sur le crane rasé du messager (et on attend que ça repousse)
- À travers la coquille d'un oeuf
- Sur une plaquette qu'on recouvre ensuite de cire
- À l'encre "invisible" (jus de citron, lait, etc.)
- Avec des piqûres d'épingle sur certaines lettres d'un texte banal
- En micropoint
- Dans les commentaires d'une page web, en blanc sur blanc, etc.
- Dans une image informatique
- ...

DÉPARTEMENT Sciences Informatiques

Stéganographie

Le message est en clair mais caché physiquement ou logiquement au sein d'un autre support.
⇒ Si l'ennemi intercepte le support et trouve le message (en cherchant consciencieusement ou parce qu'il connait la "cachette"), il n'aura aucun problème pour lire le message.
⇒ On couple en général la stéganographie avec du cryptage (i.e. on crypte un minimum le message avant de le cacher).

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Expéditeur : Message en clair

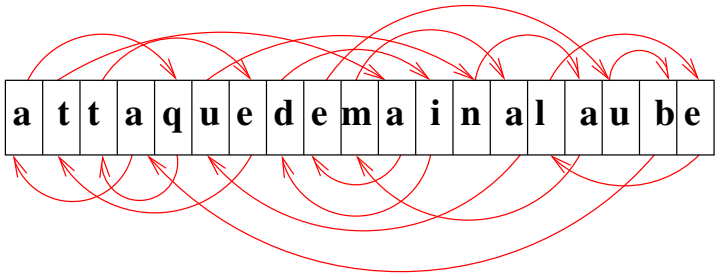
a	t	t	a	q	u	e	d	e	m	a	i	n	a	l	a	u	b	e

DÉPARTEMENT
Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Expéditeur : Chiffrement

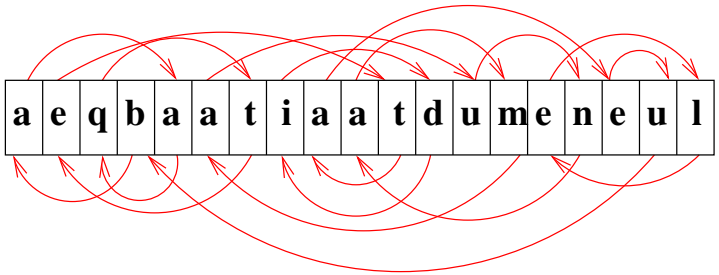


DÉPARTEMENT Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Expéditeur : Chiffrement



DÉPARTEMENT
Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Message chiffré à transmettre

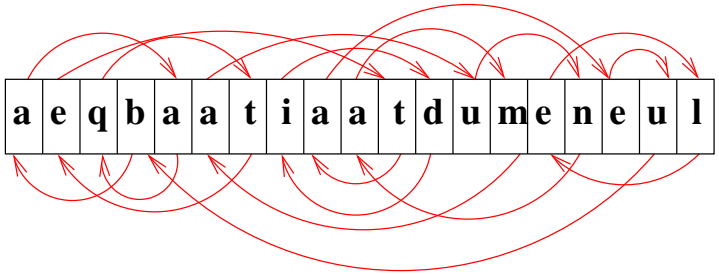
a	e	q	b	a	a	t	i	a	a	t	d	u	m	e	n	e	u	l

DÉPARTEMENT
Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Destinataire : Déchiffrement

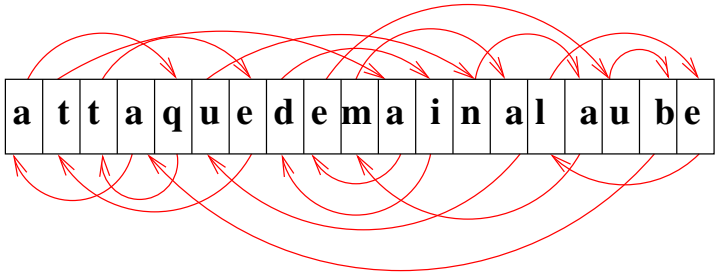


DÉPARTEMENT
Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

Destinataire : Déchiffrement



DÉPARTEMENT Sciences Informatiques

Transposition

Chaque lettre garde son identité mais pas sa position (anagramme).
Ex : code : CODE, COED, CDOE, CDEO, CEOD, CEOD, OCDE, OCED, ODCE, ODEC, OECD, OECD, DOCE, DOEC, DCOE, DCEO, DEOC, DEOC, EODC, EOCD, EDOC, EDCO, ECOD, ECOD

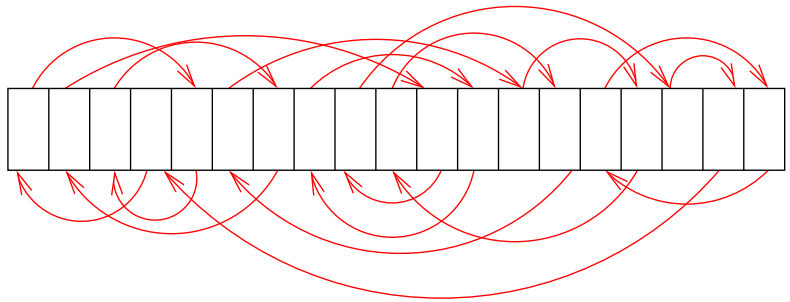
Destinataire : Message en clair

a	t	t	a	q	u	e	d	e	m	a	i	n	a	l		a	u	b	e

DÉPARTEMENT
Sciences Informatiques

Transposition

Pour un message de n caractères : $n!$ combinaisons possibles. (pour n=40, 8×10^{47} combinaisons possibles)
Impossible à l'espion de décrypter le message.
MAIS pour que le destinataire puisse aussi le déchiffrer, il faut un algorithme rigoureux et réversible...
Dans l'exemple précédent, comment transmettre la méthode de transposition :

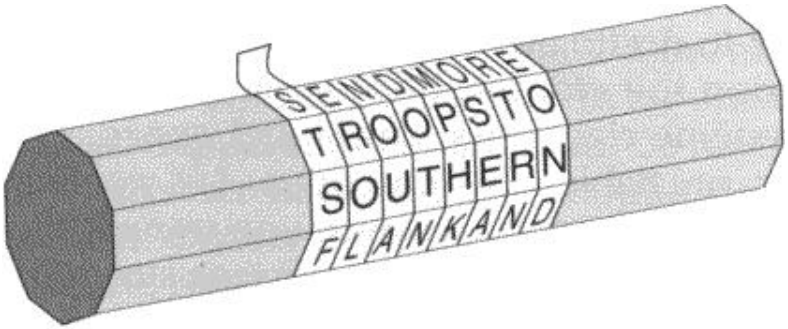


et surtout, comment la rendre généralisable pour n'importe quelle longueur de texte.

DÉPARTEMENT Sciences Informatiques

Transposition

- Scytale spartiate (V siècle avant JC) : bâton de diamètre d



`attaquedemainalaube` ⇒ AUAATEIUTDNBAEAEQML

a	t	t	a	q
u	e	d	e	m
a	i	n	a	l
a	u	b	e	

d=4 (lire toutes les 4 lettres)

- En dent de scie (écoliers) : d = 2.

`attaquedemainalaube` ⇒ AATITNAAQLUAEUDBEEM

a	t	t	a	q	u	e	d	e	m
a	i	n	a	l	a	u	b	e	

d=2

DÉPARTEMENT Sciences Informatiques

Transposition : synthèse

- Suffisamment de combinaisons : Pour un message de n caractères : $n!$ combinaisons possibles.
- Schéma de transposition difficilement généralisable.
- Schéma de transposition difficilement mémorisable.
- Schéma de transposition difficilement transmissible.

Ce qui entraine

- Utilisation de schéma de transposition automatisable basé sur le principe de la scytale.

$\Rightarrow$ cassable facilement par essai exhaustif du diamètre de la scytale.

DÉPARTEMENT Sciences Informatiques

Substitution

Substitution d'un mot, d'une phrase ou d'un caractère par un autre.

- Codage
- Chiffrement par substitutions monoalphabétique
- Chiffrement par substitutions polyalphabétique
- Chiffrement par substitutions polygrammiques
- Chiffrement par substitutions tomogrammiques

Codage

Substitution d'un mot ou d'une phrase par un autre.

on attaque	LES CAROTTES SONT CUITES
à l'aube	AVEC LE COQ
ennemis en vue	PINGOUINS SUR LA BANQUISE
avion	ABEILLE
demandons renfort	ELEPHANT EN SURSIS

`ennemis en vue : avions. Demandons renfort, on attaque à l'aube.` $\Rightarrow$ PINGOUINS SUR LA BANQUISE : ABEILLES. ELEPHANT EN SURSIS, LES CAROTTES SONT CUITES AVEC LE COQ.

DÉPARTEMENT Sciences Informatiques

Codage

on attaque	α
à l'aube	β
ennemis en vue	γ
avion	δ
demandons renfort	ϵ

ennemis en vue : avions. Demandons renfort, on attaque à l'aube. $\Rightarrow$

$\gamma : \delta.\epsilon, \alpha\beta$

on attaque	lalala
à l'aube	il fait beau
ennemis en vue	oh la belle fleur !
avion	bonjour oiseau.
demandons renfort	allons nous promener dans les champs

ennemis en vue : avions. Demandons renfort, on attaque à l'aube. $\Rightarrow$

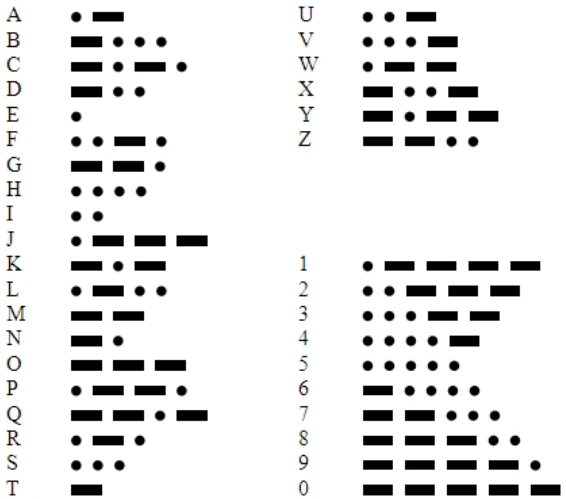
Oh la belle fleur ! Bonjour oiseau. Allons nous promener dans les champs, lalala, il fait beau.

DÉPARTEMENT Sciences Informatiques

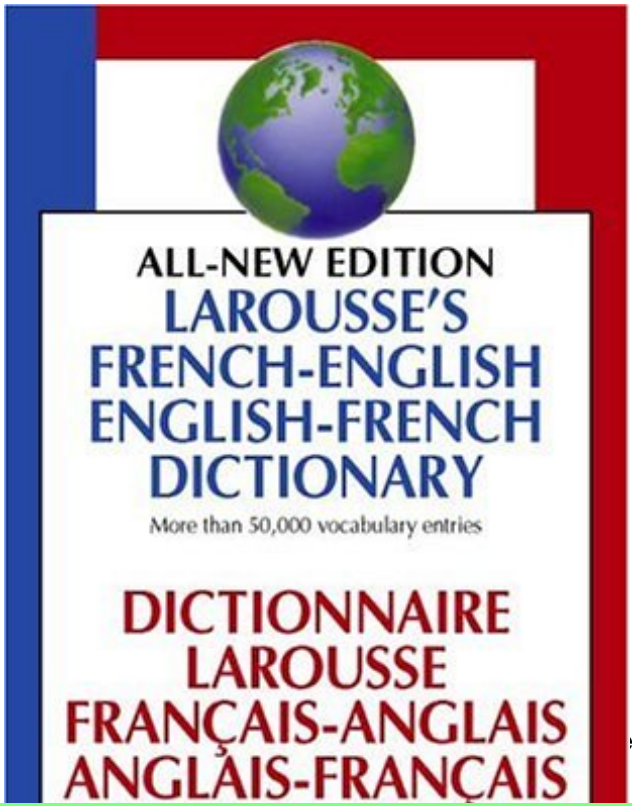
Exemple de codage

Le codage n'est pas forcément utilisé pour cacher le message :

- Code Morse : pour transmettre un message lorsque l'on a pas de support pour transporter du son, des écrits ou des images
- Code ASCII : pour "coder" les caractères en nombre (et donc en binaire)
- Langue étrangère : pour communiquer dans un autre pays



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL



Exemple de codage

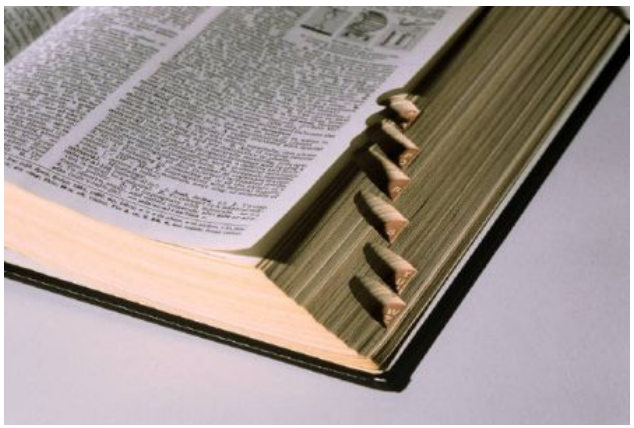
Exemple d'utilisation d'un "code" pour cacher le message

- Langue Navajo : : Pendant la Seconde Guerre mondiale, des indiens Navajos servant dans les services de transmissions américains avaient mis sur pied un code basé sur leur langue afin d'assurer la confidentialité des messages radio (cf. film Windtalkers (2002)).

DÉPARTEMENT Sciences Informatiques

Codage : synthèse

- Dictionnaire très volumineux pour le codage et le décodage (difficilement transmissible et mémorisable).
- Comment généraliser à des nouveaux mots n'existant pas dans le dictionnaire ?



DÉPARTEMENT Sciences Informatiques

Substitution par alphabet mono-alphabétique

(qu'on appelle aussi monoalphabétiques), chaque lettre est remplacée par une autre lettre ou un autre symbole.

- Le Mlecchita-Vikalpà : (45ème art du Kama-Sùtra : IVème siècle avant JC)
- Le carré de Polybe : (150 ans avant JC)
- Le chiffre de César : (60 ans avant JC)
- le chiffre Pig Pen : (18ème siècle)
- L'alphabet désordonné :
- le chiffre Atbash :
- le chiffre affine :
- Chiffre de Beale :

DÉPARTEMENT Sciences Informatiques

Alphabet de substitution

- Substitution par appariement (avec le même alphabet ou non)
- si la "technique" (l'algorithme) est dévoilée, il suffit de changer le tableau de déchiffrement
- Rélativement sûr : 26! = 29146112660563558400000 clefs possibles.
- Nécessite de retenir et de transmettre le tableau de déchiffrement (la clef). ⇒ très très difficile

a	b	c	d	e	f	g	h	i	j	k	l	m
U	K	F	R	W	B	Z	D	O	I	H	N	T

n	o	p	q	r	s	t	u	v	w	x	y	z
C	V	X	J	Q	Y	E	A	P	L	G	M	S

ou encore

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
♈	♉	♊	♋	☊	♐	◐	♑	♒	♓	♓	♏	♇

DÉPARTEMENT Sciences Informatiques

Mlecchita-Vikalpà

Substitution par appariement symétrique.

Appariements simples :

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	b	c	d	e	f	g	h	i	j	k	l	m
z	y	x	w	v	u	t	s	r	q	p	o	n

Appariements complexes :

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

$13! = 6227020000$ clefs possibles.

$\Rightarrow$ si la "technique" (l'algorithme) est dévoilée, il suffit de changer le tableau de déchiffrement.

$\Rightarrow$ relativement sûr. Mais le tableau de déchiffrement est complexe à retenir (et à transmettre).

DÉPARTEMENT Sciences Informatiques

Substitution simple par les écoliers

On remplace la lettre par sa position dans l'alphabet : A=1, B=2, C=3, ..., Z=26.

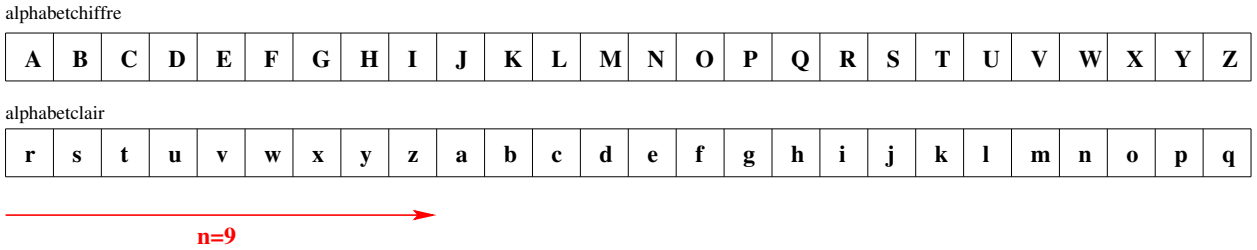
`vivelacryptographie` $\Rightarrow$ 22 9 22 5 12 1 3 18 25 16 20 15 7 18 1 16 8 9 5

$\Rightarrow$ trop simple !

DÉPARTEMENT Sciences Informatiques

Chiffre de César

Chaque lettre du texte en clair est remplacée par une autre lettre à distance fixe dans l'alphabet.

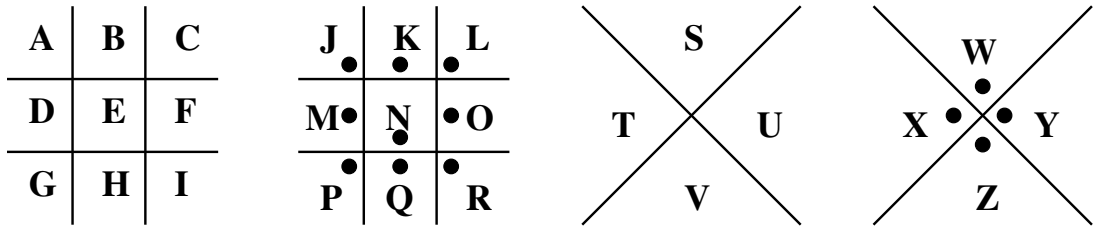


$\Rightarrow$ 26 combinaisons possibles (dont une sans intérêt).
$E_n(x) = (x + n) mod 26$ $D_n(x) = (x - n) mod 26$
$\Rightarrow$ trop simple !
(algorithme d'encryptage ROT13, avec n=13, utilisé pour raconter la chute d'une blague ou la solution d'une devinette)

DÉPARTEMENT Sciences Informatiques

Le chiffre Pig-Pen

Substitution simple de lettre par symbole. Utilisé par les templiers.



vive la cryptographie ⇒ 

⇒ si la "technique" (l'algorithme) est dévoilée, on ne peut plus utiliser cette technique.

DÉPARTEMENT Sciences Informatiques

Carré de Polybe

Utilisé par les nihilistes russes enfermés dans les prisons des tsars.

- chaque lettre de l'alphabet est remplacée par les coordonnées de sa position dans un carré.

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

`attaquedemainalaube` $\Rightarrow$ 11 44 44 11 41 45 15 14 15 32 11 24 34 11 31 11 45 12 15

$\Rightarrow$ si la "technique" (l'algorithme) est dévoilée, on ne peut plus utiliser cette technique.

DÉPARTEMENT Sciences Informatiques

L'alphabet désordonné avec mot clef

- Substitution par appariement non-symétrique.
- Pour retenir et transmettre facilement le tableau de déchiffrement, il suffit d'utiliser un mot-clef et de compléter avec le reste de l'alphabet.
- si la "technique" (l'algorithme) est dévoilée, il suffit de changer la clef

DÉPARTEMENT
Sciences Informatiques

L'alphabet désordonné avec mot clef

ce sont de droles de types qui traversent la brume avec des pas d oiseaux sous l aile des chansons leur ame est en carafe sous les ponts de la seine leurs sous dans les bouquins qu'ils n'ont jamais vendus

avec l'alphabet :

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

BLQJI RULUP JGLQU LRXKL QMSCR PZTLP QLIRG ZEPSH LZTLB ULQKZ QUJCQ LZSWQ JSQGZ CGLUL QBAZI QJIQG LSPZH LLQRL IBZPZ OLQJS QGLQK JIRQU LGZQL CILGL SPQQJ SQUZI QGLQE JSMSC IQMSC GQIJI RDZHZ CQTLI USQ

DÉPARTEMENT Sciences Informatiques

L'alphabet désordonné avec mot clef

ce sont de droles de types qui traversent la brume avec des pas d oiseaux sous l aile des chansons leur ame est en carafe sous les ponts de la seine leurs sous dans les bouquins qu'ils n'ont jamais vendus

avec l'alphabet :

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

BLQJI RULUP JGLQU LRXKL QMSCR PZTLP QLIRG ZEPSH LZTLB ULQKZ QUJCQ LZSWQ JSQGZ CGLUL QBAZI QJIQG LSPZH LLQRL IBZPZ OLQJS QGLQK JIRQU LGZQL CILGL SPQQJ SQUZI QGLQE JSMSC IQMSC GQIJI RDZHZ CQTLI USQ

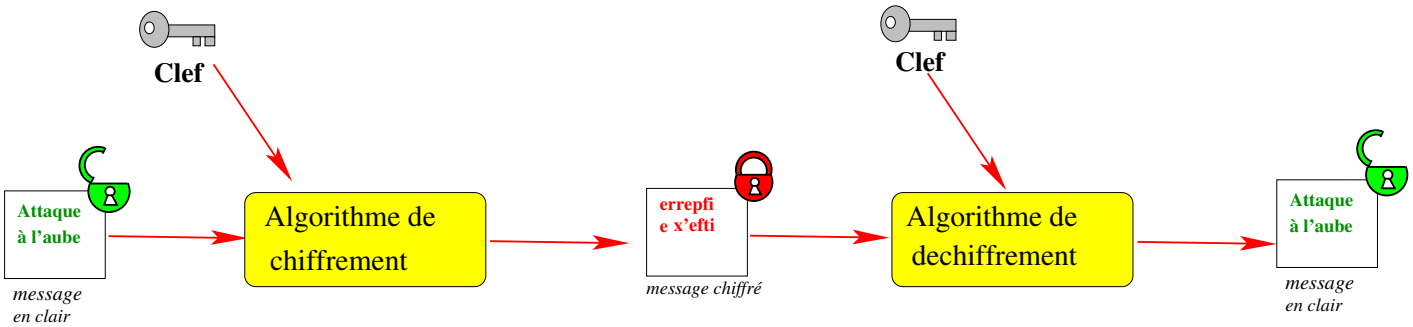
Avec le mot clef : ZEBULON

DÉPARTEMENT Sciences Informatiques

Substitution mono-alphabétique

- $26! = 291461126605635584000000$ clefs possibles.
- si on excepte les algorithmes simples (césar, polybe, pig pen, etc.), la substitution est difficile à décrypter sans avoir les correspondances entre les alphabets
- en utilisant un mot-clef, il est simple de transmettre, mémoriser la correspondance entre les alphabets.
- la substitution mono-alphabétique a été $\Rightarrow$ efficace durant près de 1000 ans.

Clef



DÉPARTEMENT Sciences Informatiques

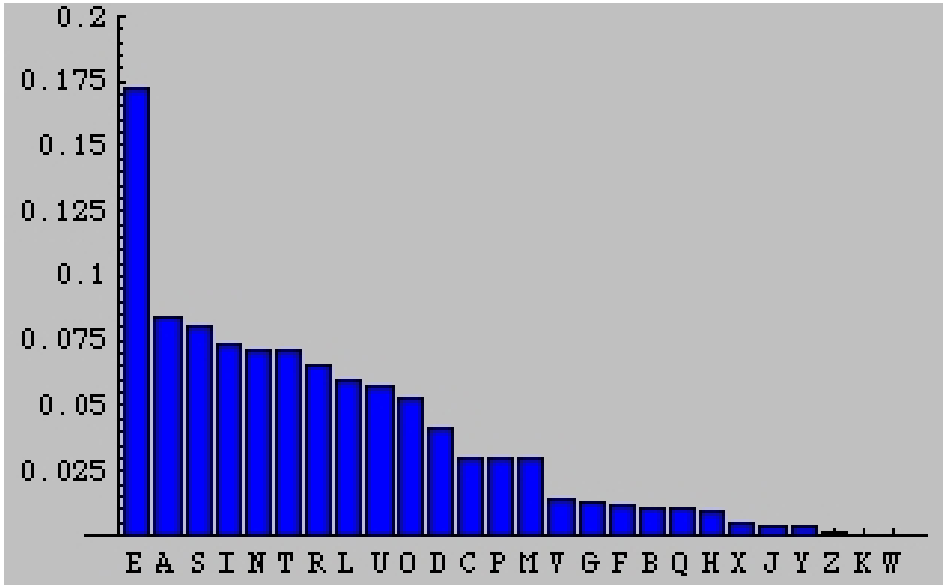
Principe de Kerchoffs

Principe de Kerchoffs

La sécurité d'un système de cryptement ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef.

Cryptanalyse

- Al-Kindi découvre une méthode de cassage de la substitution mono-alphabétique, et les savants arabes (8ème siècle) inventent la cryptanalyse.
- Méthode basée sur l'analyse statistique des fréquences



DÉPARTEMENT Sciences Informatiques

Cryptanalyse

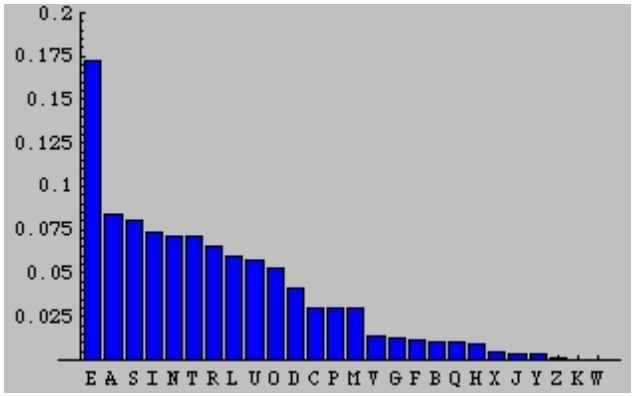
Exemple de décryptage d'un texte chiffré avec un alphabet mono-alphabétique

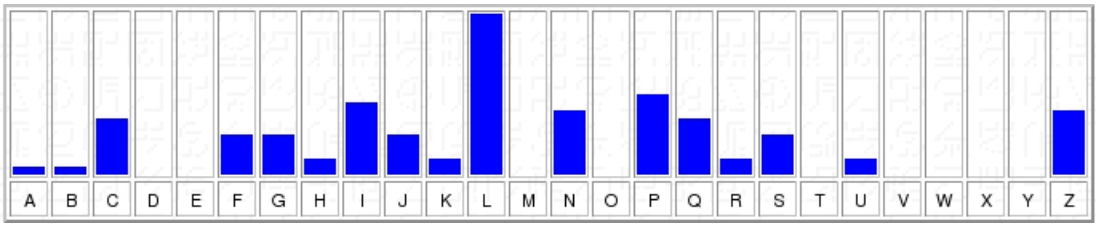
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN JSKLP LPRZF

ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ CQCLR JIQJS NILNZ FZOZP LLIIL

HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS

ILUSP LLGLG LQNLP PLFZI RLLGL KSCPF ZUJNL Q





On associe les lettres par fréquence et on commence à compléter l'alphabet.

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

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
KSCPF ZUJNL Q
----- ----- -
```

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
chiffre																										

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

Grâce aux calculs de fréquences, on déduit la correspondance du 'e'

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
----- ---e- -e-e- e---e --e-- e---- -e-e- ----- ---e- -e--- ----e -e---
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---e- e---- --e-- ----- ----e ----e --e-- e---- --e-- ----- ----- --e--
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
---e- ----- --e-- ----- ee--e --e-- --e-- -e--- --e-- e---e --e-- -----
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-e--e --e-- ----- ----- -e-e- ----- e---- -e--- ee-e- e--e- -e--- -ee-e
KSCPF ZUJNL Q
----- ----e -
```

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
chiffre																										
chiffre					L																					

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.
Les digrammes PP du début ainsi que les mots cherchés (assassinat, général, ennemis, etc. (cribs) permettent de déduire les lettres du mot assassiner.

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner -e-e- e---e --e-- e---- -e-e- ----- ---e- -e--- ----e -e---
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---e- e---- --e-- ----- ----e ----e --e-- e---- --e-- ----- ----- --e--
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
---e- ----- --e-- ----- ee--e --e-- --e-- -e--- --e-- e---e --e-- -----
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-e--e --e-- ----- ----- -e-e- ----- e---- -e--- ee-e- e--e- -e--- -ee-e
KSCPF ZUJNL Q
----- ----e -
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.
Les digrammes PP du début ainsi que les mots cherchés (assassinat, général, ennemis, etc. (cribs) permettent de déduire les lettres du mot assassiner.

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner -e-en era-e nne-i ens-i -e-es -ir-- i--e- re-a- -i-ie -es-r
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-a- a-er- n--a- a-a-e n-r-e -se-i en-r- n-en- -si-i -n-a- -re--
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
i-ie- -n--- rnera -a-as eenne -ie-a r-es- -en-i n-es- e-rre sser- n--is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse s-esi -na-- a--a- -eser a--nn e-ar- ne--s ee-e- e-res se-an -ee-e
KSCPF ZUJNL Q
--is- a--re -
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On distingue le mot 'ennemi'

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner -e-en era-e nnemi ens-i -e-es -ir-- i--e- re-am -i-ie -es-r
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-a- a-er- n--a- a-a-e n-r-e -se-i en-r- n-en- -si-i -n-a- -rem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
i-ie- -n--- rnera -a-as eenne mie-a r-es- -en-i n-es- e-rre sser- n--is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse s-esi -na-- a--a- -eser a--nn e-ar- ne--s ee-e- e-res se-an -ee-e
KSCPF ZUJNL Q
--is- a--re -
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P							

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On recherche le crib 'general' pas loin du mot assassiner

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner -egen erale nnemi ens-i -e-es -ir-- i--e- re-am -i-ie -es-r
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-a- a-er- n--a- a-a-e n-r-e -se-i en-r- n-en- -si-i -n-a- -rem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
i-ie- -n--- rnera -a-as eenne mie-a r-es- -en-i n-es- e-rre sser- n--is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse s-esi -na-- a--a- -eser a--nn e-ar- ne--s ee-e- e-res se-an -ee-e
KSCPF ZUJNL Q
--is- a--re -
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P	Q						

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On recherche le crib 'general' pas loin du mot assassiner

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ens-i -e-es -ir-- i--e- relam -i-ie -es-r
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-al a-er- n-la- a-a-e n-r-e -se-i en-r- n-en- -si-i -nla- -rem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
i-ie- -n--- rnera la-as eenne mie-a rles- -en-i n-esl e-rre sser- n--is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse slesi gnal- a--a- -eser a--nn e-ar- ne--s ee-e- e-res selan -ee-e
KSCPF ZUJNL Q
--isl a--re -
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P	Q						
chiffre	Z				L		B		C			F	H	I			M	N	P	Q	S					

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.
Parmi les lettres très fréquentes restantes, il reste le Q (chiffré) et le t (clair). On tente la correspondance

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ens-i te-es -ir-- it-e- relam -itie -estr
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-al a-er- ntla- a-a-e n-r-e tseti en-r- nten- -siti -nla- trem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
itie- -nt-- rnera la-as eenne mie-a rles- -en-i n-esl e-rre sser- nt-is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse slesi gnal- atta- -eser a--nn e-ar- ne--s ee-e- etres selan -ee-e
KSCPF ZUJNL Q
--isl a--re t
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P	Q						
chiffre	Z				L		B		C			F	H	I			M	N	P	Q	S					
chiffre	Z				L		B		C			F	H	I	J		M	N	P	Q	S					

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.
Parmi les lettres très fréquentes restantes, il reste le Q (chiffré) et le t (clair). On tente la correspondance

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ens-i te-es -ir-- it-e- relam -itie -estr
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
---es es-al a-er- ntla- a-a-e n-r-e tseti en-r- nten- -siti -nla- trem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
itie- -nt-- rnera la-as eenne mie-a rles- -en-i n-esl e-rre sser- nt-is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse slesi gnal- attaq ueser a--nn e-ar- ne--s ee-e- etres selan -ee-e
KSCPF ZUJNL Q
--isl a--re t
```

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
chiffre																										
chiffre					L																					
chiffre	Z				L				C					I				N	P							
chiffre	Z				L				C				H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P							
chiffre	Z				L		B		C			F	H	I				N	P	Q						
chiffre	Z				L		B		C			F	H	I			M	N	P	Q	S					
chiffre	Z				L		B		C			F	H	I	J		M	N	P	Q	S					
chiffre	Z	O	R	G	L	U	B	A	C			F	H	I	J	K	M	N	P	Q	S					

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On distingue le mot 'attaque'

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ensui te-es -ir-u it-eu relam -itie -estr
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
-u-es es-al a-er- ntla- a-a-e n-r-e tseti en-r- nten- -siti -nlau trem-
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
itie- -nt-u rnera la-as eenne mie-a rlesu -en-i n-esl eurre sser- nt-is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse slesi gnal- attaq ueser a--nn e-aru ne-us ee-e- etres selan -ee-e
KSCPF ZUJNL Q
-uisl a--re t
```

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

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On distingue le mot 'tourne'

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ensui te-es oir-u it-eu relam oitie -estr
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
ou-es es-al a-ero ntla- a-a-e nor-e tseti en-ro nten- ositi onlau tremo
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
itie- ontou rnera la-as eenne mie-a rlesu -en-i n-esl eurre ssero nt-is
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
-erse slesi gnal- attaq ueser a-onn e-aru ne-us ee-e- etres selan -ee-e
KSCPF ZUJNL Q
-uisl a-ore t
```

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

DÉPARTEMENT Sciences Informatiques

Contexte : on intercepte le message ce message de l'ennemi en temps de guerre. Des rumeurs font état d'une tentative d'assassinat d'un général et d'une attaque imminente.

On termine

```
ZPPZP PCILN FLBLI LNZFL IILHC LIPSC QLRLP JCNAS CQALS NLFZH JCQCL GLPQN
assas siner legen erale nnemi ensui teces oirhu itheu relam oitie destr
JSKLP LPRZF ZGLNJ IQFZU ZRZGL IJNGL QPLQC LIGNJ IQLIK JPCQC JIFZS QNLHJ
oupes escal adero ntlaf acade norde tseti endro ntenp ositi onlau tremo
CQCLR JIQJS NILNZ FZOZP LLIIL HCLKZ NFLPS GLIUC IGLPF LSNNL PPLNJ IQGCP
itiec ontou rnera labas eenne miepa rlesu denfi ndesl eurre ssero ntdis
KLNPL PFLPC BIZFG ZQQZM SLPLN ZGJII LKZNS ILUSP LLGLG LQNLP PLFZI RLLGL
perse slesi gnald attaq ueser adonn eparu nefus eeded etres selan ceede
KSCPF ZUJNL Q
puisl afore t
```

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

DÉPARTEMENT Sciences Informatiques

Parade : Substitution mono-alphabétique homophonique

Chaque lettre est codée par divers substituts, le nombre de substituts possibles étant proportionnel à la fréquence de la 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
09 12 33 47 48 53 67 78 92	81	13 41 62	01 03 45	06 10 14 16 23 24 44 46 54 55 57 74 79 82 87	31	25	39	32 50 56 70 73 83 88 93	15	04	26 37 51 65 84	22 27 68	18 58 59 66 71 91 99	00 05 07 54 72	38 90 95	94	29 35 40 42 77 80	11 19 21 36 76 86 97 96	17 20 30 43 49 69 75	02 08 61 63 85 90	34 52	60	28	24	01

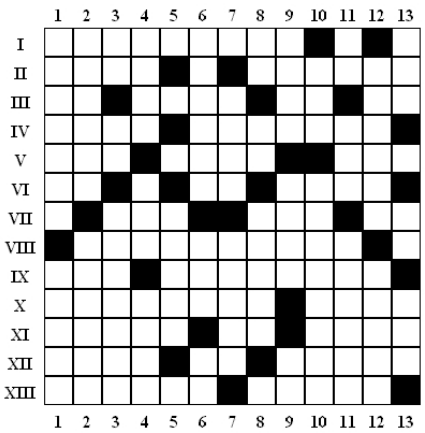
On peut rajouter aussi des symboles nuls (ne codant rien).

- Plus complexe à décrypter
- Mais faisable quand même avec une bonne connaissance de la langue
  - fréquence de digramme (nn, mm, rr, etc.)
  - occurences 'q' suivi en général d'un 'u'
  - grammaire : 's' souvent terminal
  - ...

DÉPARTEMENT Sciences Informatiques

Casseurs de code (et toutes ses variantes)

Pour la deuxième guerre mondiale, des casseurs de codes étaient engagés par le gouvernement parmi les lecteurs du daily telegraph qui avaient réussi à résoudre les grilles de mots croisés publiés dans le journal.



Horizontal

I. Sentiment que notre grand-mère nous apporte la plupart du temps. **II.** Elle l'est souvent aussi. C'est celle de notre grand-père. **III.** Célèbre actrice dont la cause est la protection des animaux. Plus belle fête de l'année. Article étranger. Période du calendrier. **IV.** Indispensable au bébé. Nos grand-mères nous en font. **V.** Mesure internationale. Se dit parfois quand on est content au lieu de "chouette". Personnage d'un déluge. **VI.** Terminaison. Spécialisé en. Suffixe anglais qui concerne les 13-19 ans. **VII.** Lorsqu'il contient des roses, c'est qu'un secret a été soulevé. OK à la française. Appris. **VIII.** Patriarche en latin. **IX.** Fais ce qu'il te plait ! Relatifs à une orbite. **X.** Poste d'émission (de radio ou de télévision). Rode dans le désordre. **XI.** Elles sont fêtées plus tard dans l'année. Pronom personnel. Langue du serpent. **XII.** Ardeur impétueuse. Note. Triste perte. **XIII.** On en change au mois de mars. On en fait beaucoup à nos mamies.

Vertical

1. Il est de plus en plus rare qu'elles en portent un. Surnom qu'elles apprécient de moins en moins. (pl). **2.** Partie d'une pièce servant d'appui, de support à une autre pièce. Femme de Bobby dans "Dallas". **3.** Conjonction négative. Presque Rio. Récompenserai. **4.** Quenotte. Indispensables après le biberon. Nets dans le désordre. **5.** Allures du cheval. **6.** Palais épiscopal. Vieille colère. Route Nationale. **7.** Petits poèmes du Moyen Age. Utilise avec excès. **8.** Pronom personnel. Sorte d'avion. Direction Régionale de l'Industrie de la Recherche et de l'Environnement. **9.** Démarche inutile si son coup est porté dans l'eau. Doigté. Dessin industriel. **10.** Forfait proposé par France télécom. Petits éclats de bois qui entrent dans la chair. **11.** Précède approuvé. Gros titre. Courage. **12.** De Saxe. Vin d'Espagne. **13.** Ecole bouddhiste originaire de Chine et répandue au Japon depuis la fin du XIIe s. Unique. Operational Data Store.

DÉPARTEMENT Sciences Informatiques

Chiffre de Beale

On remplace la lettre en le numéro d'un mot d'un livre qui a cette lettre pour première lettre.
La clef est le livre.

- difficilement transmissible
- difficilement mémorisable
- très long à chiffrer et déchiffrer.

ATTAQUE $\Rightarrow$ 15 - 27 - 30 - 32 - 14 - 9 - 5

Les 3 messages de Beale indiquant l'emplacement de son trésor. Seul le deuxième a été déchiffré (clef : la déclaration d'indépendance). Les 2 autres indiquant où se trouve exactement le trésor sont à ce jour encore non-déchiffrés.

DÉPARTEMENT Sciences Informatiques

Chiffre de Beale

[1]On [2]remplace [3]la [4]lettre [5]en [6]le [7]numéro [8]d'[9]un [10]mot [11]d'[12]un [13]livre [14]qui [15]a [16]cette [17]lettre [18]pour [19]première [20]lettre.
[21]La [22]clef [23]est [24]le [25]livre.

- [26]difficilement [27]transmissible
- [28]difficilement [29]mémorisable
- [30]très [31]long [32]à [33]chiffrer [34]et [35]déchiffrer.

ATTAQUE $\Rightarrow$ 15 - 27 - 30 - 32 - 14 - 9 - 5

Les 3 messages de Beale indiquant l'emplacement de son trésor. Seul le deuxième a été déchiffré (clef : la déclaration d'indépendance). Les 2 autres indiquant où se trouve exactement le trésor sont à ce jour encore non-déchiffrés.

DÉPARTEMENT Sciences Informatiques

Substitution polyalphabétique

(aussi appelées à double clef ou à alphabets multiples), utilisent plusieurs "alphabets", ce qui signifie qu'une même lettre peut être remplacée par plusieurs symboles.

- Chiffre de Bellaso, chiffre de Porta
- Carré de Trithème / Carré de Vigenère
  - variante : le chiffre de Beaufort
  - variante : le chiffre de Gronsfeld
- le cylindre de Jefferson
- la machine Enigma.

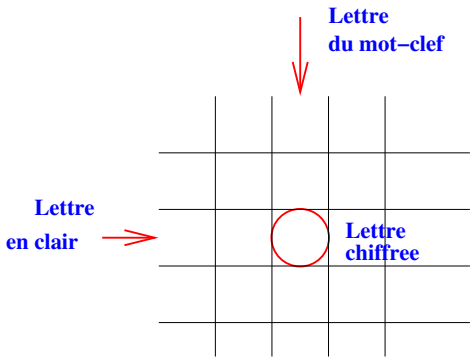
DÉPARTEMENT Sciences Informatiques

Carré de Trithème/Carré de Vigenère

	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

Mot clef : ZUT

Z	U	T	Z	U	T	Z
b	o	n	j	o	u	r
A	I	G	I	I	N	Q



DÉPARTEMENT
Sciences Informatiques

Alphabet poly-alphabétique

- Assez complexe à utiliser ⇒ automatisation
- Assez robuste

Principe du cassage de ce chiffre : **Test de Friedman** : Pour chaque sous-chaînes obtenues en prenant les lettres à intervalle donné,calculer l'indice de coïncidence (probabilité que deux lettres choisies aléatoirement dans un texte soient identiques) et la comparer à l'IC de la langue (Francais : IC=0.074).
Une fois la longueur du mot-clef trouvé, utiliser l'analyse des fréquences sur chaque sous-chaine et se ramener au problème de la substitution mono-alphabétique.

DÉPARTEMENT Sciences Informatiques

Substitution Polygrammique

(aussi appelées polygraphiques), les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement).

- Le chiffre bigrammatique (Giovanni Porta)
- Le chiffre Playfair
- Les chiffrements à deux carrés
- Les chiffrements à trois carrés
- Les chiffrements à quatre carrés
- Le chiffre de Hill.
- Le RSA.

DÉPARTEMENT Sciences Informatiques

Substitution tomogrammiques

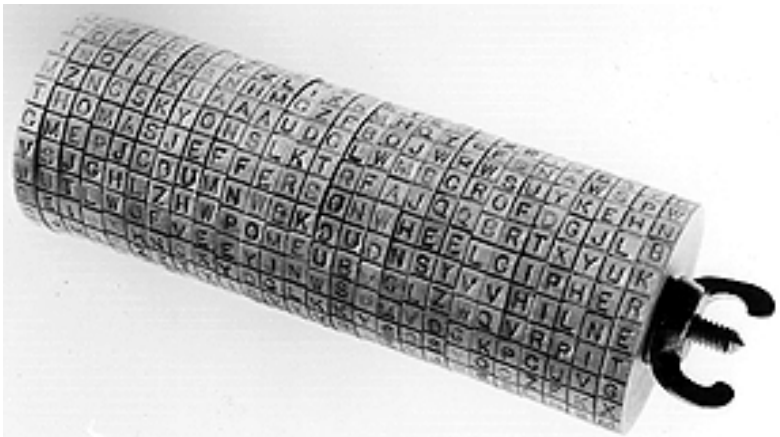
(aussi appelées par fractions de lettres) dans lesquelles chaque lettre est tout d'abord représentée par des groupes de deux ou plusieurs symboles, qui sont ensuite chiffrés séparément par substitution ou transposition

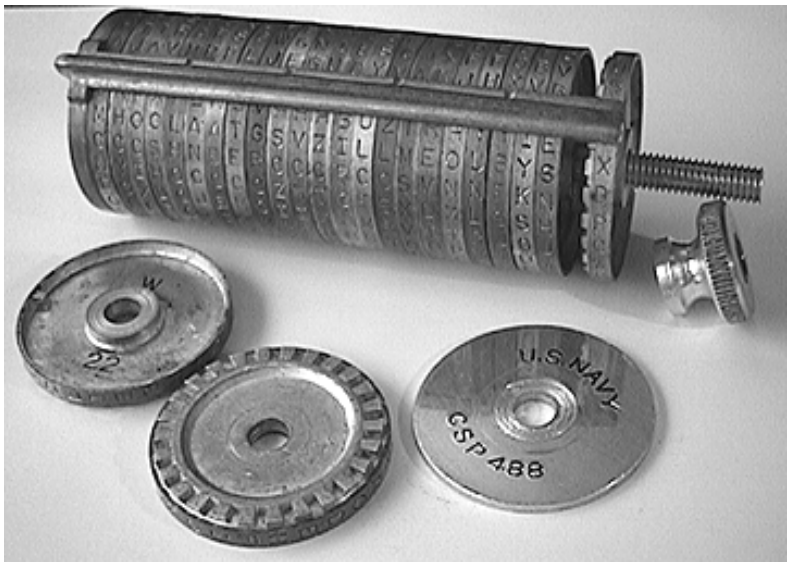
- Le chiffre Pollux
- Le chiffre de Collon
- Le chiffre de Delastelle
- Le chiffre ADFGVX
- Le chiffre digrafide.

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Cylindre de Jefferson



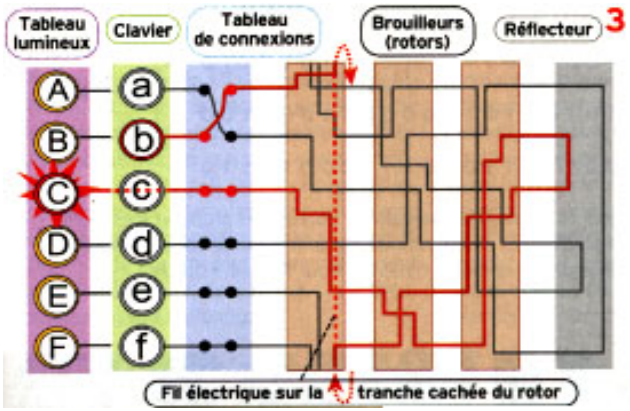


- 26 roues sur un axe
- Les 26 lettres de l'alphabet inscrites sur la tranche de chaque roue dans un ordre aléatoire
- Former le message en tournant ces roues
- Le correspondant a le même cylindre
- la clef est l'ordre dans lequel mettre les cylindres.

$\Rightarrow$ Substitution polyalphabétique

DÉPARTEMENT Sciences Informatiques

Enigma



- les rotors produisent un nouvel alphabet de substitution à chaque pression de touche
- pas de "clef" unique comme dans le chiffrement polyalphabétique
- trois rotors, donc 26 x 26 x 26 = 17 576 alphabets de substitution pour toute combinaison de trois rotors.
- aucune répétition de l'alphabet de substitution
- "clé" : numéro de rotors, position de l'anneau et position de départ

DÉPARTEMENT Sciences Informatiques

Enigma

Utilisé durant la seconde guerre mondiale par les allemands

- les alliés ont eu beaucoup de mal à la déchiffrer
- utilisation de cribs (les rapports militaires commencent toujours par les informations sur le terrain)
- une machine enigma avait été récupéré...

les travaux de déchiffrement de Bletchley Park classifiés jusqu'en 1974.
Algorithme de chiffrement d'Enigma développé par un étudiant (commande UNIX : crypt) en

- Utilisé par des laboratoires civils et militaires pour protéger leurs communications

$\Rightarrow$ espionnage industriel.

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Cryptanalyse

La cryptanalyse s'oppose à la cryptographie. Déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière.
Même si on décrit les cryptanalystes comme des « briseurs de codes », un algorithme est considéré comme cassé lorsqu'une attaque permet de retrouver la clé en effectuant moins d'opérations que via une attaque par force brute.

Techniques classiques de cryptanalyse

- Analyse de fréquence : : Regarder la répartition des fréquences de chacune des lettres : si la même que dans la langue supposé $\Rightarrow$ substitution mono-alphabétique
- Test de Friedman : Pour chaque sous-chaînes obtenues en prenant les lettres à intervalle donné,calculer l'indice de coïncidence (probabilité que deux lettres choisies aléatoirement dans un texte soient identiques) et la comparer à l'IC de la langue (Francais : IC=0.074).
  - Permet de déterminer si le chiffrement est mono-alphabétique ou poly-alphabétique
  - Permet de déterminer la longueur de la clef dans un carré de Vigénère.
- Technique du mot probable (Cribbing) : supposer qu'une séquence de lettres du cryptogramme correspond à un mot que l'on devine (crib)
- Méthode de Babbage/Kasinski : repérer des séquences de lettres qui se répètent dans le cryptogramme.
- L'attaque par force brute : : tester toutes les solutions possibles de mots de passe ou de clés.

DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Crédits I

- Histoire des codes secrets - Simon Singh - ed. Le livre de poche
- Les codes secrets décryptés - Didier Müller - ed. City
- http ://www.apprendre-en-ligne.net/crypto/ de Didier Müller.

DÉPARTEMENT
Sciences Informatiques