Cryptographie Classique

January 18, 2010

Plan

- Les plus anciennes écritures secrètes connues sont celles rapportées par Hérodote lors des conflits entre la Grèce et la Perse au V^e siècle avant JC.
- Lors de la construction de Persepolis, Athène et Sparte refuse d'envoyer de l'aide à la Perse.

Xerxes Roi-Dieu de Perse

Nous étendrons l'empire de la Perse jusqu'à ce ses frontières se confondent avec le ciel de dieu afin que le soleil n'éclaire aucune autre terre que la notre

Pendant les 5 années qui suivirent Xerxes les consacra à rassembler la plus grande armée jamais connue et en 480 il s'estima prêt à lancer une attaque surprise.

- L'armement de la Perse fut dévoilé par un grec Demaratus vivant en Perse.
- Il gratta de la cire sur une paire de tablette de bois pliante, inscrivit le projets de Xerxes sur le bois, et recouvrit d'une seconde couche de cire.

- Personne n'en découvrit le contenu du message jusqu'à ce que Cléomène épouse de Léonidas (Roi de Sparte) proposa d'enlever la cire afin d'en découvrir le message.
- Les Spartes et les Grecs purent se préparer à contrer l'attaque de Xerxes.

Stéganographie

- La ruse de Demaratus est le premier procédé de stéganographie connu.
- Stéganographie = Ecriture (graphie), couverte (stégano).
- D'autres types de stéganographie furent utilisés dans l'histoire.
  - message caché sous la chevelure d'un messager,
  - jus de citron qui apparaît sous la flamme d'une bougie,
  - oeuf.
- Ces exemples montrent que la dissimulation d'un message peut en assurer le secret.
- Mais si l'ennemi met tout ses pouvoirs à rechercher un message il peut le trouver et en connaître son contenu.
- C'est ce qui a motivé le développement des "codes secrets" ou cryptographie.

Plan

Chiffrement par permutation

On considère le message

ton secret est ton prisonnier; s'il fuit tu deviendras son prisonnier.

On le réécrit sur deux lignes

$$\begin{array}{ccccccccccc} T & & N & & E & & R & & T & \ldots \\ & O & & S & & C & & E & & \ldots \end{array}$$

On le lit ligne à ligne, et on obtient le message chiffré.

$$TNERTSTNRSNIRFITDVEADSNRSNIROSCEET \ldots$$

Autrement dit on a réécrit les lettres du message dans un ordre différent.

La Scytale

- En 404 avant J.C., Lysandre de Sparte vit un messager venant de Perse.
- Celui-ci lui tendit sa ceinture qui était entièrement écrite, mais incompréhensible.

- Lysandre prit alors sa scytale, rond de bois calibré autour duquel il entoura la ceinture.
- Le message se recomposa, en clair, suivant la génératrice du cylindre.

Chiffrement par permutation général

Pour message dont les lettres sont numérotées de 1 à n

$$M = (l_1, l_2, l_3, \cdots, l_n)$$

Et une permutation (bijection)

$$P : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

A la place i on met la lettre d'indice $P(i)$. Le message chiffré est alors

$$C = (l_{P(1)}, l_{P(2)}, l_{P(3)}, \ldots, l_{P(n)})$$

Le déchiffrement de $C = (c_1, \ldots, c_n)$ se fait en

$$M = (c_{P^{-1}(1)}, c_{P^{-1}(2)}, \ldots, c_{P^{-1}(n)})$$

.

Plan

Le Kama Sutra

- Texte écrit par le brahmane Vatsyayana au IVeme siècle AJC.
- C'est un texte qui expose des règles pour avoir une vie de couple épanouie (ce n'est pas qu'un traité érotique!!).
- Il recommande, page 26, que les femmes apprennent 64 arts. Entre autre
  - cuisiner,
  - s'habiller,
  - masser,
  - élaborer des parfums,

  Mais aussi
  - les échecs,
  - la prestidigitation,
  - les écritures secrètes.
- L'une des écritures secrètes enseignées consiste à apparier au hasard les lettres de l'alphabet.

Chiffrement par substitution, un exemple

On apparie à chaque lettre de l'alphabet une seconde

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	D	I	T	W	M	C	O	F	K	R	P	G

Pour crypter un message on substitue la lettre de l'alphabet avec celle à quoi on l'a appariée.

j	a	i	c	a	c	h	e	...

Chiffrement par substitution, un exemple

On apparie à chaque lettre de l'alphabet une seconde

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	D	I	T	W	M	C	O	F	K	R	P	G

Pour crypter un message on substitue la lettre de l'alphabet avec celle à quoi on l'a appariée.

j	a	i	c	a	c	h	e	...
E								

Chiffrement par substitution, un exemple

On apparie à chaque lettre de l'alphabet une seconde

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	D	I	T	W	M	C	O	F	K	R	P	G

Pour crypter un message on substitue la lettre de l'alphabet avec celle à quoi on l'a appariée.

j	a	i	c	a	c	h	e	...
E	B							

Chiffrement par substitution, un exemple

On apparie à chaque lettre de l'alphabet une seconde

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	D	I	T	W	M	C	O	F	K	R	P	G

Pour crypter un message on substitue la lettre de l'alphabet avec celle à quoi on l'a appariée.

j	a	i	c	a	c	h	e	...
E	B	Y						

Chiffrement par substitution, un exemple

On apparie à chaque lettre de l'alphabet une seconde

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
B	N	S	U	H	Z	J	R	Y	E	A	Q	V

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
X	D	I	T	W	M	C	O	F	K	R	P	G

Pour crypter un message on substitue la lettre de l'alphabet avec celle à quoi on l'a appariée.

j	a	i	c	a	c	h	e	...
E	B	Y	S	B	S	R	H	

Autre formulation

On se donne une une fonction bijective S

$$S \ : \ \{a, b, \ldots, z\} \rightarrow \{A, B, \ldots, Z\}$$

- Chiffrement : on substitue chaque lettre λ du message clair par $S(\lambda)$.
- Déchiffrement : on substitue chaque lettre Λ du message chiffré par $S^{-1}(\lambda)$.

Chiffrement par décalage ou de César

- C'est un exemple simple de chiffrement par substitution.
- Décalage de k rangs : chaque lettre est substituée par la lettre se trouvant k rang après elle.
- Par exemple pour $k = 4$

a	b	c	d	e	f	g	h	i	j	k	l	m
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
E	F	G	H	I	J	K	L	M	N	O	P	Q

n	o	p	q	r	s	t	u	v	w	x	y	z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
R	S	T	U	V	W	X	Y	Z	A	B	C	D

- C'est une des méthodes de chiffrement utilisée par César.

Le schéma général d'un envoie de message

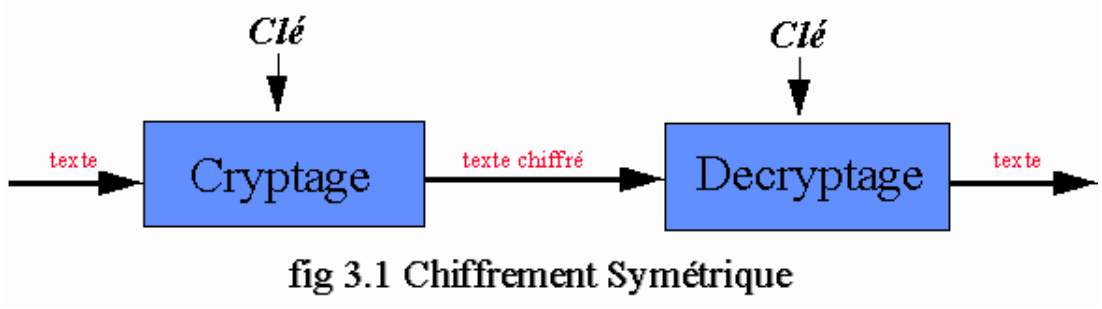


fig 3.1 Chiffrement Symétrique

Si l'ennemi intercepte le message et qu'il connaît la méthode de chiffrement

- Si c'est un décalage : il pourra essayer les 25 décalages possibles.
- Si c'est une substitution plus générale il y devra essayer

  $26! \cong 400000000000000000000000000$ substitutions possibles

  Ce qui est impossible même avec les ordinateurs d'aujourd'hui.

Utilisation de mot/phrase clef

Problème pratique :

- Si l'alphabet substitué est aléatoire, il est difficile de le mémoriser. Par exemple

$$BNSUHZJRYEAQVXDITWMCOFKRPG$$

- On serait tenter de le griffonner quelque part ce qui est risqué.
- Un moyen pratique couramment utilisé, est d'utiliser une **phrase clef**.

Exemple d'utilisation de phrase clef

- Par exemple : *TOUT CADENASSER*
- Pour fabriquer l'alphabet substitué on enlève les doublons

TOUCADENSR

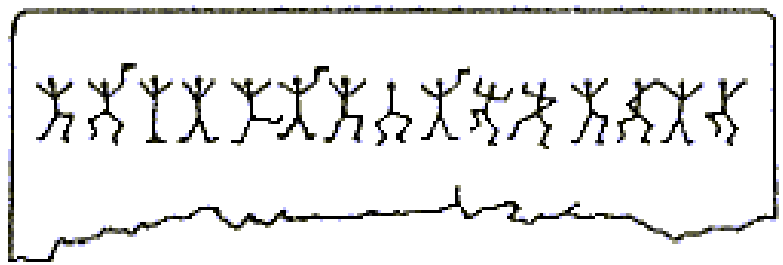
- Et on complète par les lettres de l'alphabet manquantes (s'il y en a) à la fin

TOUCADENSRBFGHIJKLMPQVWXYZ

- On peut aisément retenir la phrase clef et reconstituer l'alphabet désordonné correspondant.

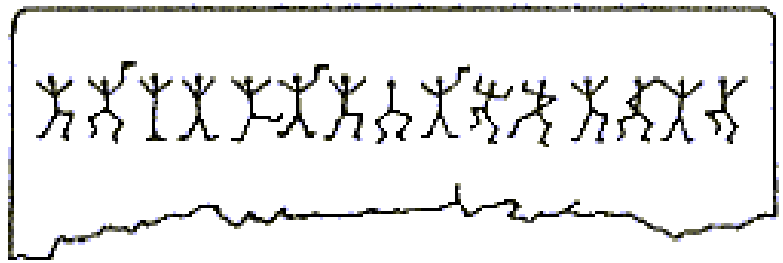
Substitution par des symboles quelconques

- Consiste à substituer les lettres de l'alphabet par un symbole autre qu'alphabétique.
- Par exemple **les hommes dansant** dans le roman éponyme de Conan Doyle, on trouve

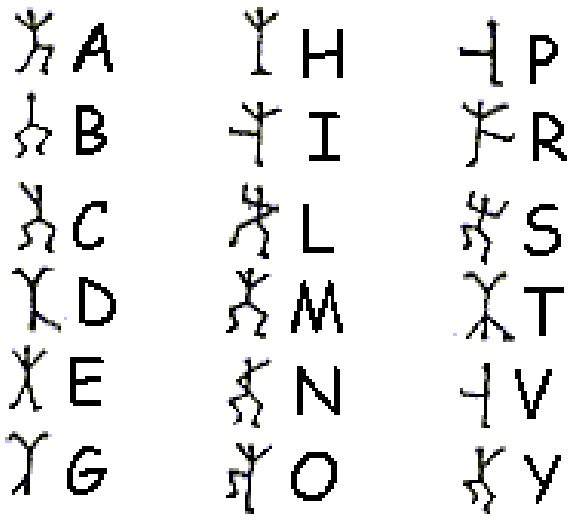


Substitution par des symboles quelconques

- Consiste à substituer les lettres de l'alphabet par un symbole autre qu'alphabétique.
- Par exemple **les hommes dansant** dans le roman éponyme de Conan Doyle, on trouve



- La correspondance lettre $\leftrightarrow$ symbole obtenu par Sherlock Holmes.



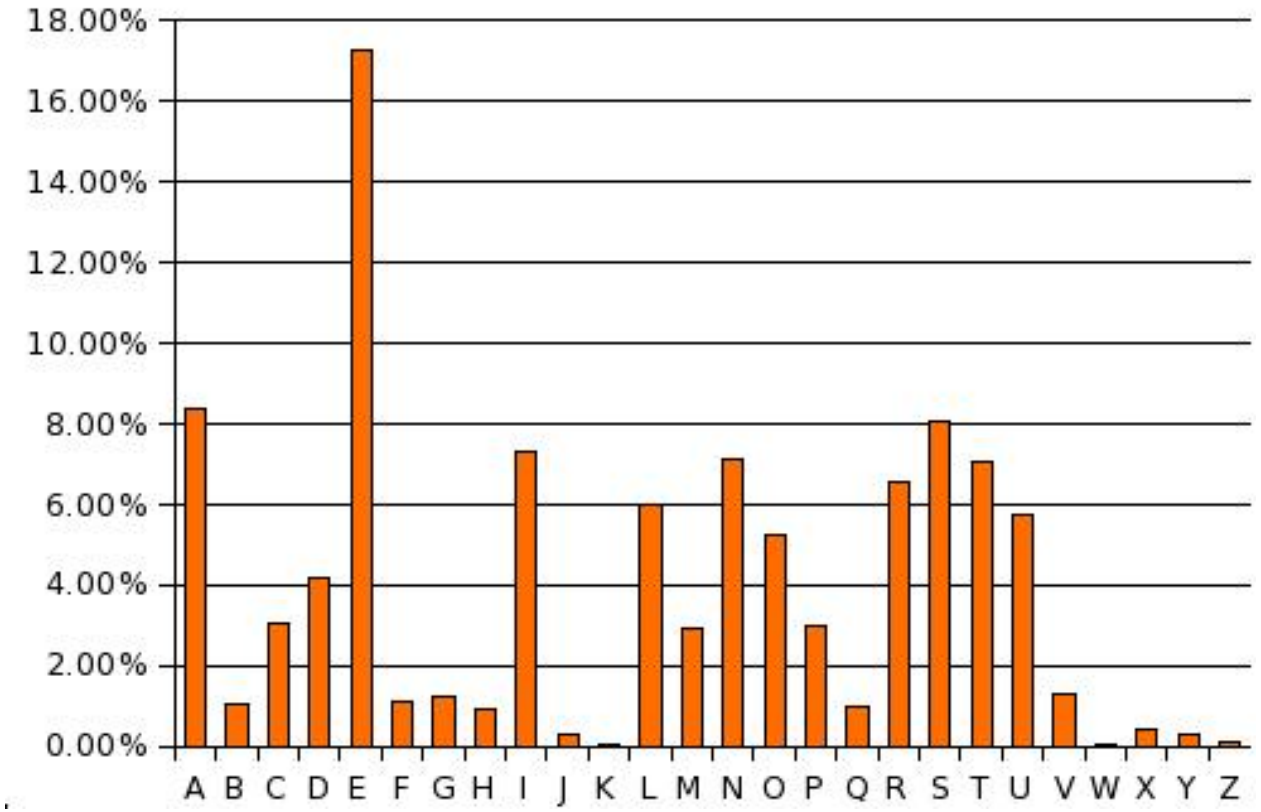
Plan

Génèse

- Les théologiens de Basra, de Kufa et de Bagdad essayaient de reconstituer la chronologie des révélations de Mahomet telles qu'elles apparaissent dans le Coran.
- Ils étudiaient la fréquence des mots employés : certains apparaissaient, d'autres disparaissaient.
- Pour le Hadith, journal attribué à Mahomet, ils recherchaient ce qui était à attribuer à Mahomet
  - ils étudiaient la forme linguistique, le style,
  - le choix des mots employés
  - **la fréquence d'apparition des lettres.**
- Ce fût une découverte essentielle, due à Abû Yusuf Al Kindi, pour la cryptonymie qui sera employée jusque vers 1920.

Analyse de fréquence dans la langue française

Dans la langue française chaque lettre n'apparaît pas avec la même fréquence.



Analyse de fréquence dans la langue française

On peut classifier les lettres en différents groupes

$$
\begin{array}{lcl}
17\% & \longrightarrow & e \\
6\% - 8\% & \longrightarrow & a, i, l, n, r, s, t, u, o \\
3\% - 4\% & \longrightarrow & c, d, m, p \\
0\% - 1\% & \longrightarrow & b, f, g, h, j, k, q, v, w, x, y, z
\end{array}
$$

Analyse de fréquence dans la langue française

Dans un message chiffré par substitution,

une lettre λ apparaîtra dans le message clair avec la même fréquence que $S(\lambda)$ dans le message chiffré.

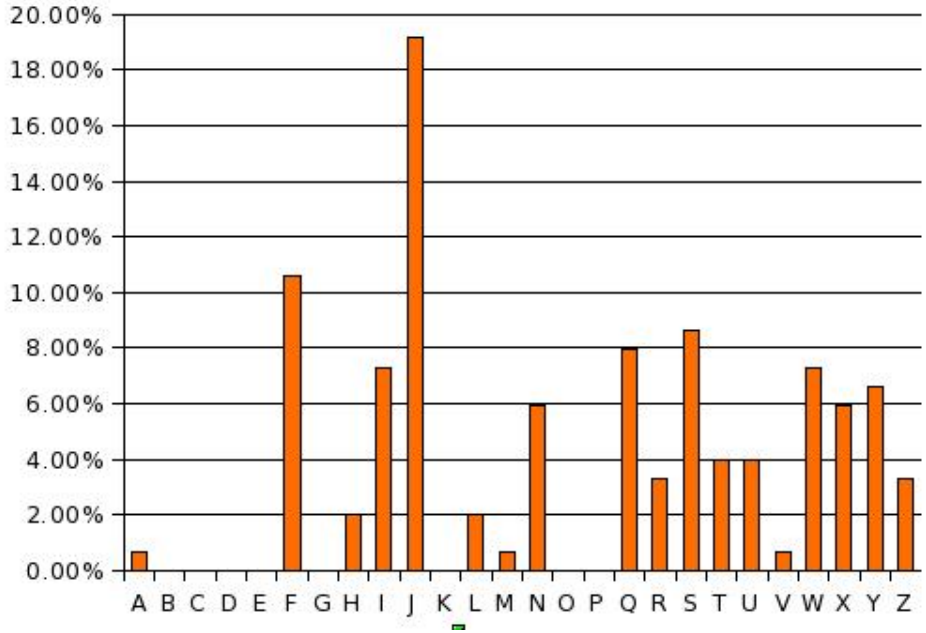
En étudiant la fréquence d'apparition des lettre d'un message chiffré, on peut les ranger dans l'un des groupe ci-dessous.

$$\begin{array}{lcl} 17\% & \longrightarrow & e \\ 6\% - 8\% & \longrightarrow & a, i, l, n, r, s, t, u, o \\ 3\% - 4\% & \longrightarrow & c, d, m, p \\ 0\% - 1\% & \longrightarrow & b, f, g, h, j, k, q, v, w, x, y, z \end{array}$$

Ensuite en étudiant les fréquences d'apparition des paires de lettre on peut affiner l'étude et découvrir la clef de chiffrement.

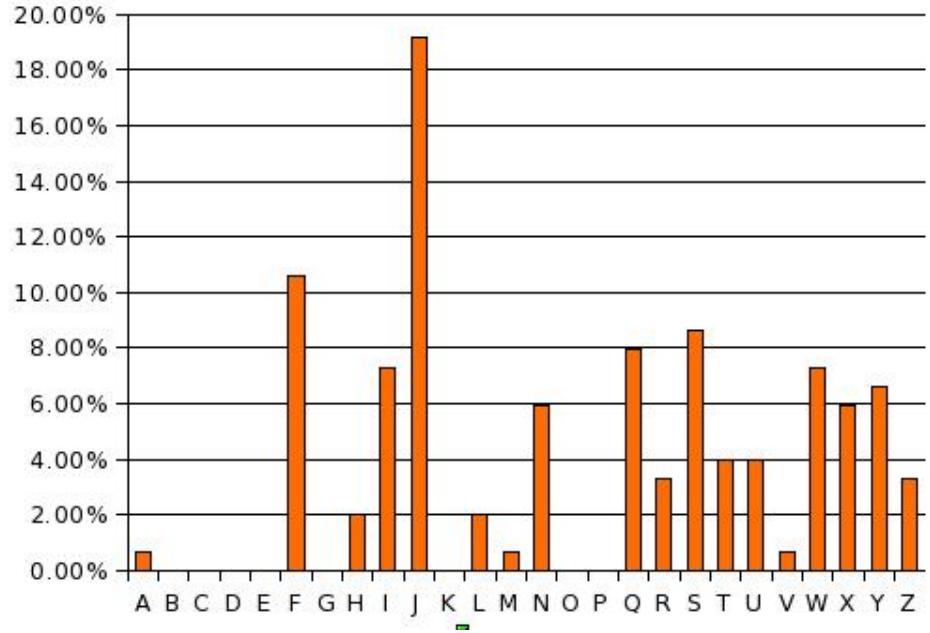
Soit un message chiffré par décalage

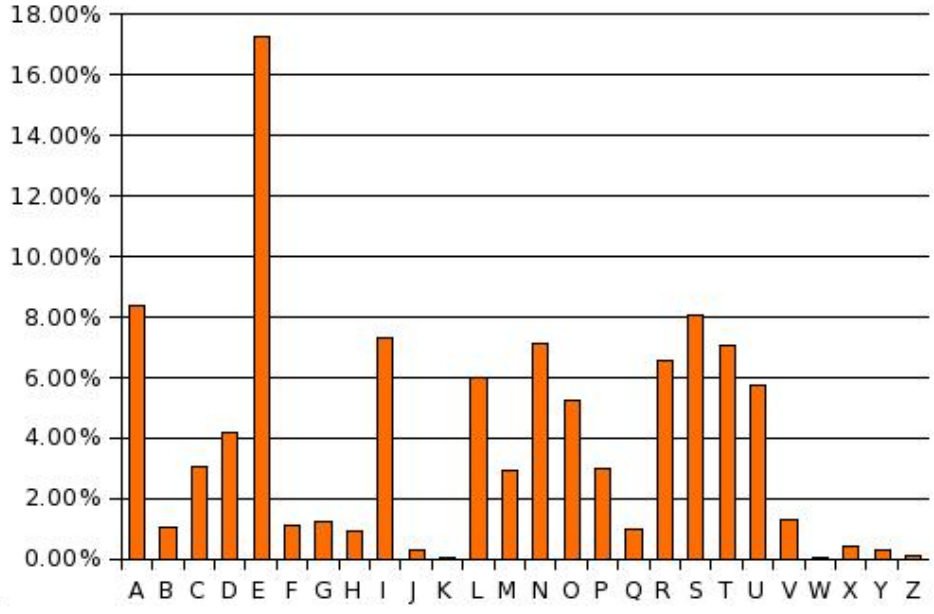
IJAFS YQFQT NXJIW JXXJQ
JLFWI NJSIJ QFUTW YJZSM
TRRJI JQFHF RUFLS JXJUW
JXJSY JJYIJ RFSIJ FJSYW JWIFS
XQFQT NRFNX QJLFW INJSI
NYVZJ UTZWQ NSXYF SYNQS
JUJZY UFXQZ NFHHT WIJWQ
JSYWJ J



Soit un message chiffré par décalage

IJAFS YQFQT NXJIW JXXJQ
JLFWI NJSIJ QFUTW YJZSM
TRRJI JQFHF RUFLS JXJUW
JXJSY JJYIJ RFSIJ FJSYW JWIFS
XQFQT NRFNX QJLFW INJSI
NYVZJ UTZWQ NSXYF SYNQS
JUJZY UFXQZ NFHHT WIJWQ
JSYWJ J

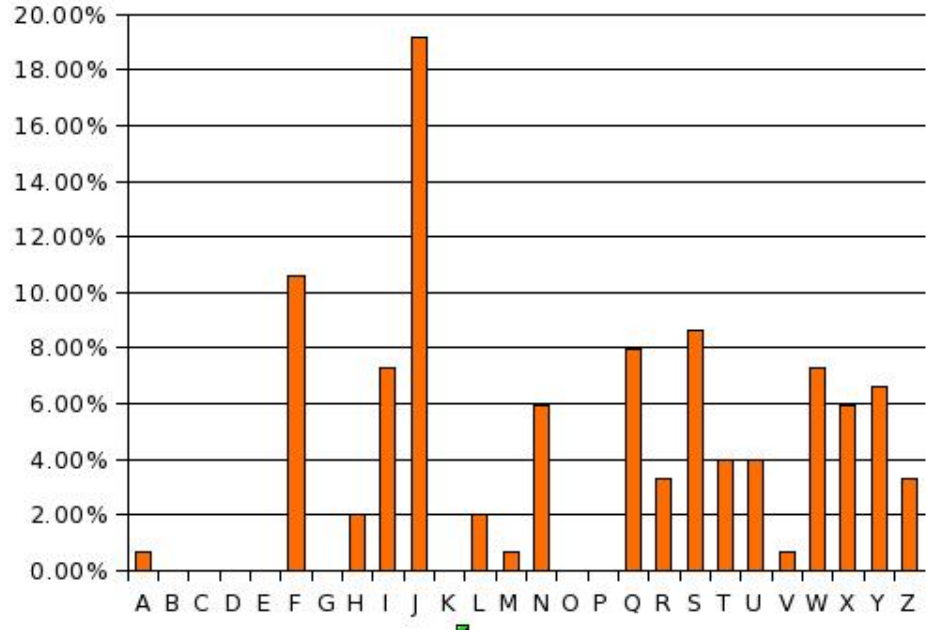


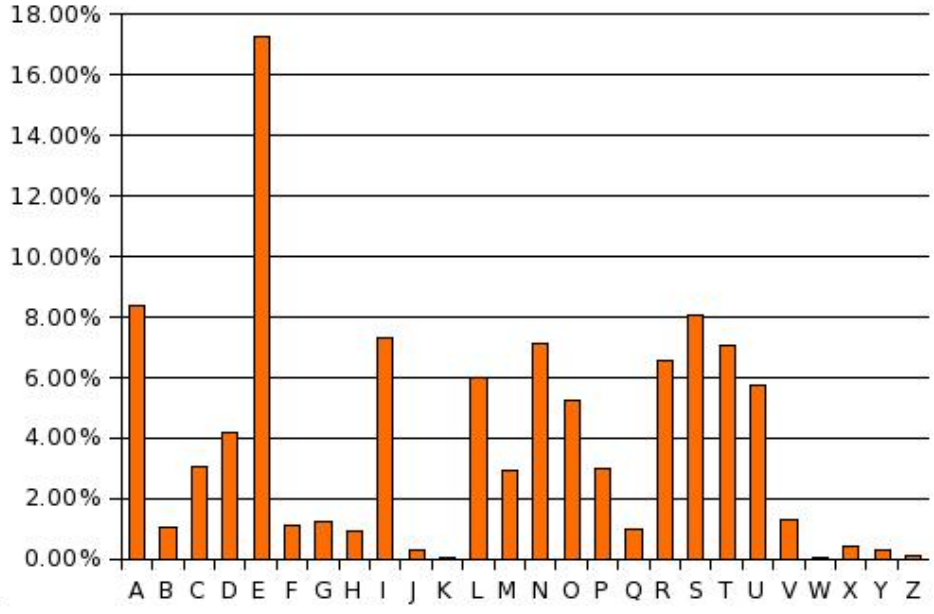


Soit un message chiffré par décalage

IJAFS YQFQT NXJIW JXXJQ JLFWI NJSIJ QFUTW YJZSM TRRJI JQFHF RUFLS JXJUW JXJSY JJYIJ RFSIJ FJSYW JWIFS XQFQT NRFNX QJLFW INJSI NYVZJ UTZWQ NSXYF SYNQS JUJZY UFXQZ NFHHT WIJWQ JSYWJ J

DEVANT LA LOI SE DRESSE LE GARDIEN DE LA PORTE. UN HOMME DE LA CAMPAGNE SE PRESENTE ET DEMANDE A ENTRER DANS LA LOI. MAIS LE GARDIEN DIT QUE POUR L INSTANT IL NE PEUT PAS LUI ACCORDER L ENTREE.





Exemple détaillé

On a le message suivant chiffré par substitution

XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

...

Étude des Fréquences des lettres

$$f_X = 17,8 \leftrightarrow f_e = 17,26$$

$f_R = 8.0$	$f_a = 8.40$
$f_V = 7.7$	$f_s = 8.08$
$f_Y = 7.7$	$f_i = 7.34$
$f_M = 7.5$	$f_n = 7.13$
$f_B = 7.2$	$f_t = 7.07$
$f_J = 6.9$	$f_r = 6.55$
$f_G = 6.5$	$f_l = 6.01$

Étude des Bigrammes

$$\{R, V, , Y, M, B, J, G\} \leftrightarrow \{a, s, i, n, t, r, l\}$$

Chiffré		Francais	
XR	49	*ES*	3318
GX	37	*DE*	2409
XY	34	*LE*	2366
VX	32	*EN*	2121
XJ	29	*RE*	1885
NX	26	*NT*	1694
XV	25	*ON*	1646
VC	23	*ER*	1514
CY	23	*TE*	1484
RX	21	*EL*	1382
UV	21	*AN*	1378
YJ	21	*SE*	1377
XG	17	*ET*	1307

Étude des Bigrammes

$$\{R, V, , Y, M, B, J, G\} \leftrightarrow \{a, s, i, n, t, r, l\}$$

Chiffré		Francais	
XR	49	ES	3318
GX	37	DE	2409
XY	34	LE	2366
VX	32	EN	2121
XJ	29	RE	1885
NX	26	NT	1694
XV	25	ON	1646
VC	23	ER	1514
CY	23	TE	1484
RX	21	EL	1382
UV	21	AN	1378
YJ	21	SE	1377
XG	17	ET	1307

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 es	ES 3318
GX 37	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32 *le*	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32 *le*	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32 *le*, *re*	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34	LE 2366
VX 32 *le*, *re*	EN 2121
XJ 29	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	*ES* 3318
GX 37 *le*, *re*	*DE* 2409
XY 34	*LE* 2366
VX 32 *le*, *re*, *te*	*EN* 2121
XJ 29	*RE* 1885
NX 26	*NT* 1694
XV 25	*ON* 1646
VC 23	*ER* 1514
CY 23	*TE* 1484
RX 21	*EL* 1382
UV 21	*AN* 1378
YJ 21	*SE* 1377
XG 17	*ET* 1307
BJ 16	*LA* 1270
LX 16	*AI* 1255
BX 16	*IT* 1243
BY 15	*ME* 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	*ES* 3318
GX 37 *le*, *re*	*DE* 2409
XY 34 *en*, *et*	*LE* 2366
VX 32 *le*, *re*, *te*	*EN* 2121
XJ 29	*RE* 1885
NX 26	*NT* 1694
XV 25	*ON* 1646
VC 23	*ER* 1514
CY 23	*TE* 1484
RX 21	*EL* 1382
UV 21	*AN* 1378
YJ 21	*SE* 1377
XG 17	*ET* 1307
BJ 16	*LA* 1270
LX 16	*AI* 1255
BX 16	*IT* 1243
BY 15	*ME* 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	*ES* 3318
GX 37 *le*, *re*	*DE* 2409
XY 34 *en*, *et*	*LE* 2366
VX 32 *le*, *re*, *te*	*EN* 2121
XJ 29	*RE* 1885
NX 26	*NT* 1694
XV 25	*ON* 1646
VC 23	*ER* 1514
CY 23	*TE* 1484
RX 21	*EL* 1382
UV 21	*AN* 1378
YJ 21	*SE* 1377
XG 17	*ET* 1307
BJ 16	*LA* 1270
LX 16	*AI* 1255
BX 16	*IT* 1243
BY 15	*ME* 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	*ES* 3318
GX 37 *le*, *re*	*DE* 2409
XY 34 *en*, *et*	*LE* 2366
VX 32 *le*, *re*, *te*	*EN* 2121
XJ 29 *en*, *et*	*RE* 1885
NX 26	*NT* 1694
XV 25	*ON* 1646
VC 23	*ER* 1514
CY 23	*TE* 1484
RX 21	*EL* 1382
UV 21	*AN* 1378
YJ 21	*SE* 1377
XG 17	*ET* 1307
BJ 16	*LA* 1270
LX 16	*AI* 1255
BX 16	*IT* 1243
BY 15	*ME* 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34 *en*	LE 2366
VX 32 *le*, *re*	EN 2121
XJ 29 *et*	RE 1885
NX 26	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

G, Y, V, J, N

Chiffré	Francais
XR 49 *es*	ES 3318
GX 37 *le*, *re*	DE 2409
XY 34 *en*	LE 2366
VX 32 *le*, *re*	EN 2121
XJ 29 *et*	RE 1885
NX 26 *de*	NT 1694
XV 25	ON 1646
VC 23	ER 1514
CY 23	TE 1484
RX 21	EL 1382
UV 21	AN 1378
YJ 21	SE 1377
XG 17	ET 1307
BJ 16	LA 1270
LX 16	AI 1255
BX 16	IT 1243
BY 15	ME 1099

Pour l'instant

$$R \leftrightarrow s$$
$$V \leftrightarrow l, r$$
$$Y \leftrightarrow n$$
$$J \leftrightarrow t$$
$$G \leftrightarrow l, r$$

Pour l'instant

$$R \leftrightarrow s$$
$$V \leftrightarrow l, r$$
$$Y \leftrightarrow n$$
$$J \leftrightarrow t$$
$$G \leftrightarrow l, r$$

Texte	*Francais*
$f_R = 8.0$	$f_a = 8.40$
$f_V = 7.7$	$f_s = 8.08$
$f_Y = 7.7$	$f_i = 7.34$
$f_M = 7.5$	$f_n = 7.13$
$f_B = 7.2$	$f_t = 7.07$
$f_J = 6.9$	$f_r = 6.55$
$f_G = 6.5$	$f_l = 6.01$

en*et*nst*nt****r*rentles****ts**ne***n*****eet*ls
XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

e*r***renten***e****n*el**res*rle*l*tre****r****l*
XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

*sr***ller****t*ette**rt*e*e***n***e*r****t*l*rsle
BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

en*et*nst*nt****r*rentles****ts**ne***n*****eet*ls

XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

e*r***renten***e****n*el**res*rle*l*tre****r****l*

XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

*sr***ller****t*ette**rt*e*e***n***e*r****t*l*rsle

BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

$M \leftrightarrow a$

en*et*nstanta**ar*rentles****ts**ne*a*n*****eet*ls
XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

e*r***renten*a*e***an*ela*res*rle*latre****r***ala
XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

*sr**aller****t*ette*art*e*e*a*n***e*r**a*tal*rsle
BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

en*et*nstanta**ar*rentles****ts**ne*a*n*****eet*ls

XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

e*r***renten*a*e***an*ela*res*rle*latre****r***ala

XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

*sr**aller****t*ette*art*e*e*a*n***e*r**a*tal*rsle

BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

$$B \leftrightarrow I$$

Et ainsi de suite...

encetinstantapparurentlesdoigtsdunemaindhommeetils

XYAXJBYRJMYJMQQMVUVXYJGXRNCBWJRNUYXLMBYNPCLLX

ecrivirentenfaceducandelabresurleplatredumurdupala

XAVBDBVXYJXYIMAXNUAMYNXGMFVXRUVGXQGMJVXNULUVN

isroyalleroivitcettepartiedemainquiecrivaitalorsle

BRVCEMGGXVCBDBJAXJJXQMVJBXNXLMBYKUBXAVBDMBJMG

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
c	i	o	v	y	b	l	$*$	f	t	q	m	a	d	$*$	h	p	s	j

Plan

Conséquence de l'analyse de fréquence

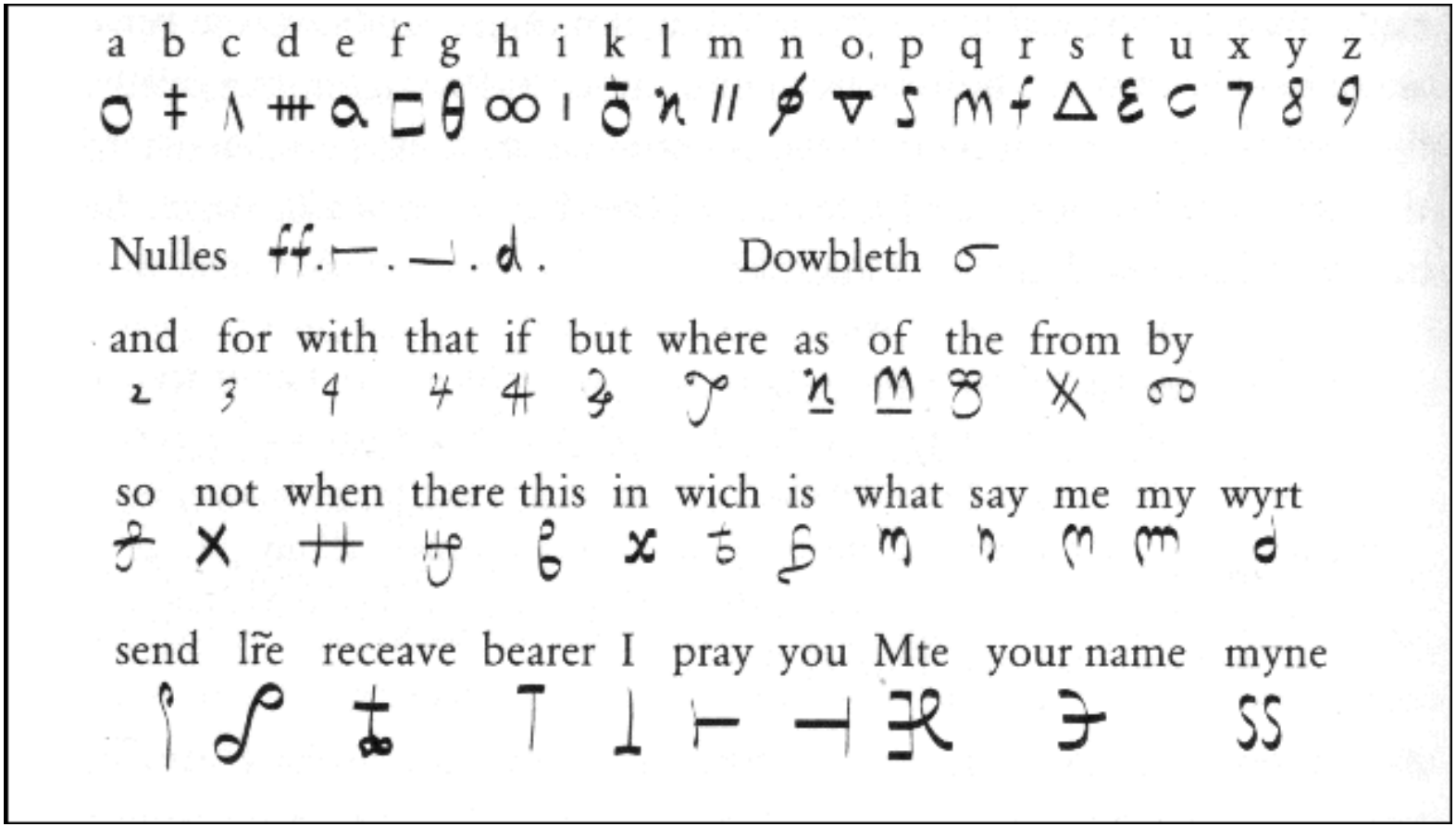
Le code substitutions "simple" n'était plus sur.
Plusieurs méthodes ont été introduites pour "modifier" les fréquences des lettres

- Ajout de symbole muet.
- Substitution de syllabe et de mot entiers par de nouveaux symboles.
- Substitution par symboles multiples.

  E$\longrightarrow$ 17 symboles
  A$\longrightarrow$ 8 symboles
  etc...

  Chaque symbole apparaît alors avec la même fréquence!!

Exemple : le code Marie Stuart.



L'exécution de Marie Stuart

- Cela se déroule durant les heures noires de la guerre des religions entre catholique et protestant.
- Marie Stuart fut pendant une période Reine d'Ecosse avant de perdre le trône au profit de son fils.
- Elle pouvait prétendre aussi légitimement au trône d'Angleterre, pour cette raison elle fut emprisonnée par la reine d'Angleterre.
- Un groupe d'écossais catholique, partisan de Marie Stuart, projetaient de monter un coup d'état.
- La faiblesse du code de Marie provoqua l'arrestation de celle-ci et son exécution sanglante.

Plan

L'ébauche du Code de Vigenère

- Comme le montre cruellement la fin tragique de Marie Stuart,
- les amélioration faite au chiffrement par substitution n'était pas toujours suffisante.
- Au XVe siècle Alberti proposa d'utiliser deux (ou plusieurs) substitutions alternativement.
- Il remarqua que cela permettait d'équilibrer les fréquences des lettres.

$$\begin{array}{rcccccccc} M = & l_1 & & l_2 & & l_3 & & l_4 & \cdots \\ & \downarrow S_1 & & \downarrow S_2 & & \downarrow S_1 & & \downarrow S_2 & \\ C = & L_1 & & L_2 & & L_3 & & L_4 & \cdots \end{array}$$

où S_1 et S_2 sont deux substitutions distinctes.

Exemple

Si

$S_1 =$ décalage d'une lettre vers la droite.

$S_2 =$ décalage d'une lettre vers la gauche.

$M =$	D	E	S	E	S	P	E	R	E	E
	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$
$C =$	E	D	T	D	T	O	F	Q	F	D

On remarque

- $5e- > 3D, 2F$
- $2s- > 2T$

Exemple

Si

S_1 = décalage d'une lettre vers la droite.

S_2 = décalage d'une lettre vers la gauche.

$M =$	D	E	S	E	S	P	E	R	E	E
	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$
$C =$	E	D	T	D	T	O	F	Q	F	D

On remarque

- $5e- > 3D, 2F$
- $2s- > 2T$

Exemple

Si

S_1 = décalage d'une lettre vers la droite.

S_2 = décalage d'une lettre vers la gauche.

$M =$	D	E	S	E	S	P	E	R	E	E
	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$	$\downarrow S_1$	$\downarrow S_2$
$C =$	E	D	T	D	T	O	F	Q	F	D

On remarque

- $5e- > 3D, 2F$
- $2s- > 2T$

Le code de Vigenère

- Blaise de Vigenère, diplomate français publia en 1586 une version simplifiée de l'idée d'Alberti.
- Il proposait simplement de n'utiliser que des substitutions par décalage.
- Cela avait le mérite de simplifier la méthode d'Alberti (les clefs sont plus simples).

Le code de Vigenère

1. On met le message clair et la clef

$$M = (l_1, \ldots, l_n) \qquad K = (k_1, \ldots, k_m)$$

sous forme numérique avec la correspondance.
$(a \to 0, b \to 1, c \to 2, \ldots, z \to 25)$.

2. On ajoute la clef lettre à lettre modulo 26 de façon répétitive.

$$\begin{array}{cccccccccc} & m_1 & m_2 & \cdots & m_\ell & m_{\ell+1} & \cdots & m_{2\ell} & m_{2\ell+1} & \cdots \\ + & k_1 & k_2 & \cdots & k_\ell & k_1 & \cdots & k_\ell & k_1 & \cdots \\ \hline & c_1 & c_2 & \cdots & c_\ell & c_{\ell+1} & \cdots & c_{2\ell} & c_{2\ell+1} & \cdots \end{array}$$

Exemple, chiffrement de Vigenère

Message = coucou

Clef = la

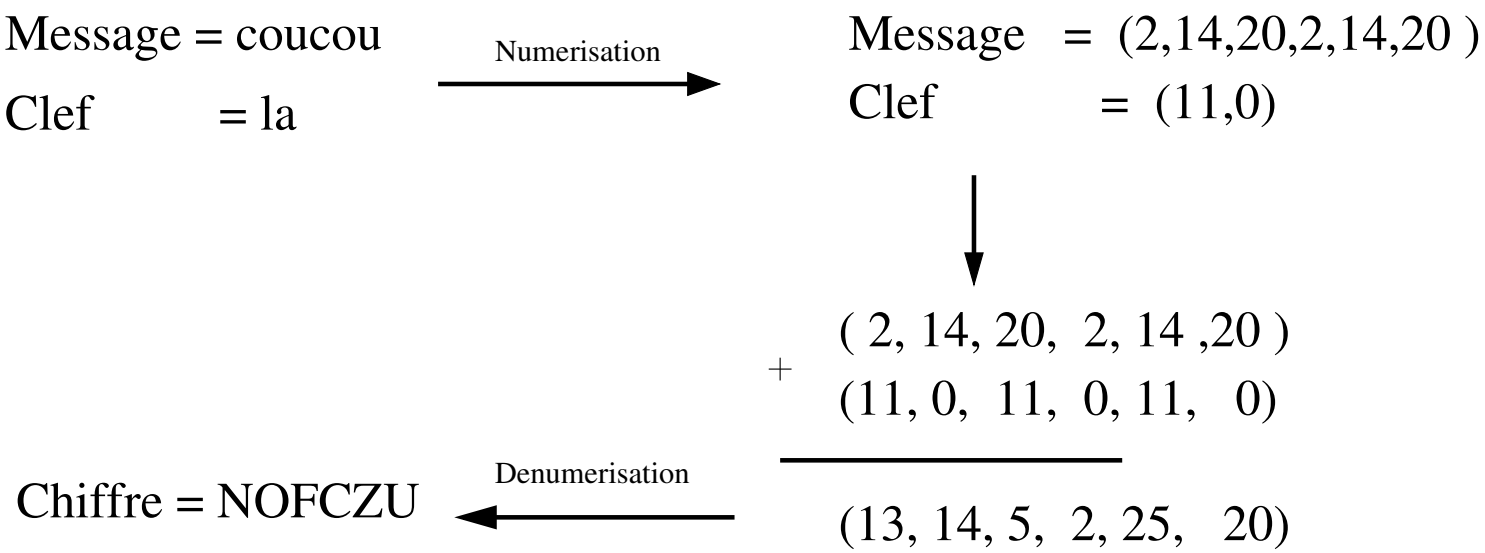
Exemple, chiffrement de Vigenère

Message = coucou
Clef = la

Numerisation →

Message = (2,14,20,2,14,20)
Clef = (11,0)

Exemple, chiffrement de Vigenère



Exemple, déchiffrement de Vigenère

Au lieu d'additionner la clef, on la soustrait modulo 26

Chiffre = PMTLTE

Clef = la

Exemple, déchiffrement de Vigenère

Au lieu d'additionner la clef, on la soustrait modulo 26

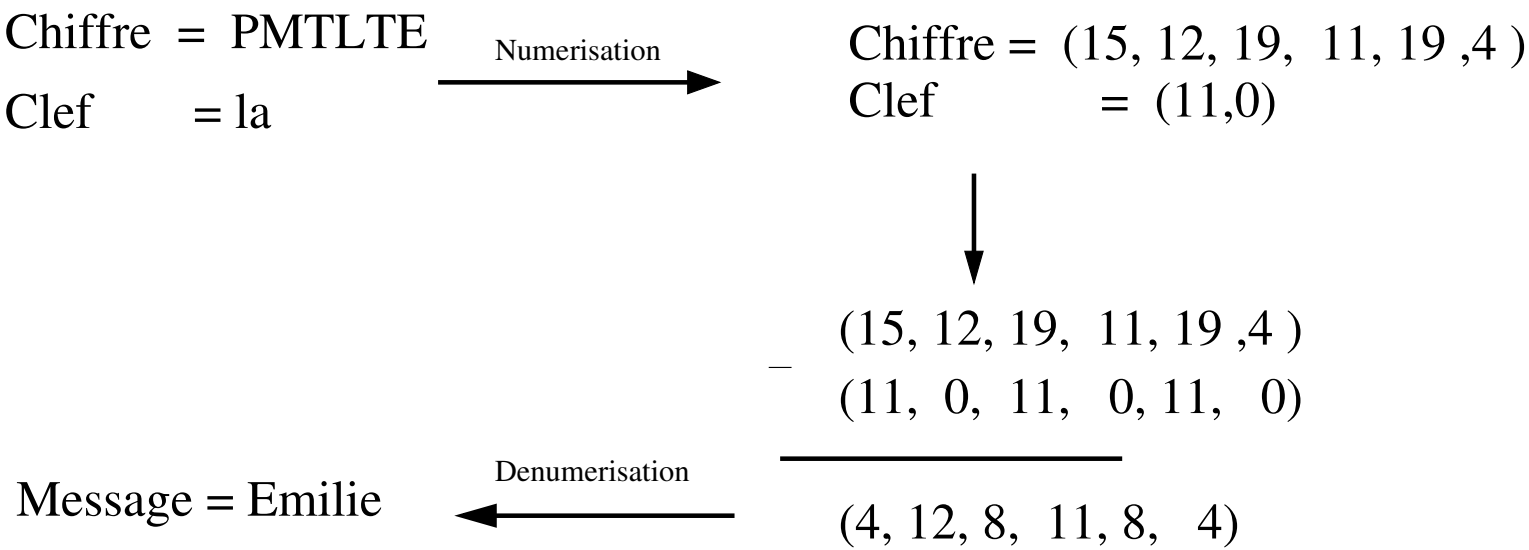
Chiffre = PMTLTE
Clef = la

Numerisation →

Chiffre = (15, 12, 19, 11, 19 ,4)
Clef = (11,0)

Exemple, déchiffrement de Vigenère

Au lieu d'additionner la clef, on la soustrait modulo 26



- Le code de Vigenère fut ignoré pendant 200 ans jusqu'en 1786.
- Ensuite il acquis rapidement la réputation d'un code indéchiffrable.
- Il fut "cassé" au milieu du 19eme siècle par Babage.

Fréquence de lettre dans Vigenère

Proposition

Soit $K = (k_1, \ldots, k_26)$ *une clef de chiffrement de Vigenère. On suppose que pour tout* $i \neq j$ *on a* $k_i \neq k_j$ *Un message chiffré* C *vérifie alors pour toute lettre* $\lambda \in \{A, \ldots, Z\}$

$$f_C(\lambda) \cong 1/26$$

Proof.

Soit λ un lettre, on a après découpage du message M en 26 message $M_1, \ldots, M_{26}$

$$f_C(\lambda) = \left(\sum_{i=1,\ldots,26} f_{M_i}(lambda - k_i) \right) /26$$

Mais comme $k_i \neq k_j$ pour tout $i \neq j$, $f_{M_i}(lambda - k_i)$ décrit toutes les valeurs du tableau lorsque i parcours $1, \ldots, 26$.

Idée de l'attaque de Babage

- Soit ℓ la longueur de la clef.
- Si l'on connaît la longueur de la clef alors on peut découper le message en ℓ morceaux.

$$\begin{aligned} C_1 &= (c_1, c_{1+\ell}, c_{1+2\ell}, \ldots) \\ C_2 &= (c_2, c_{2+\ell}, c_{2+2\ell}, \ldots) \\ &\vdots \\ C_\ell &= (c_\ell, c_{2\ell}, c3\ell, \cdots) \end{aligned}$$

- Chacun des morceaux est un chiffré par décalage, la taille du décalage peut être retrouver par une analyse de fréquence.

C_1 chiffré par décalage de k_1
C_2 chiffré par décalage de k_2
$\vdots$
C_ℓ chiffré par décalage de k_ℓ

TOUTE LA DIFFICULTE EST DANS LA DETERMINATION DE LA LONGUEUR DE LA CLEF.

Indice de Coincidence

Definition

Soient deux textes M et M' de longueur respective n et n'. Soient f_λ (resp. f'_λ) le nombre d'apparition de la lettre λ dans le texte M (resp. dans le texte M'). L'indice de coïncidence de M et M' par

$$I_c(M, M') = \frac{1}{nn'} \sum_{\lambda=a,b,\ldots,z} f_\lambda f'_\lambda$$

Pour simplifier si $M = M'$ on notera simplement $I_c(M)$.

Exemple

Considérons le texte suivant de longueur 61

M="Le brachyta borni est un capricorne très paisible de l'ordre des coléoptères"

Le décompte de chaque lettre nous donne le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
4	3	4	3	8	0	0	1	4	0	0	4	0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	5	3	0	8	5	4	1	0	0	0	1	0

On obtient alors que l'indice de coïncidence de M vaut
$I_c(M) = \frac{1}{61^2}(3\times 1^2+4\times 3^2+5\times 4^2+2\times 5^2+2\times 8^2) = \frac{293}{61^2} \cong 0,078$

Soit M un texte

- Si chaque lettre de l'alphabet apparaît avec la même fréquence alors

$$I_c(M) \cong 1/26 = \times(\sum_{\lambda=a}^{z} \left(\frac{1}{26}\right)^2 \cong 0,4$$

- Si M est un texte français on a

$$I_c(M) \cong \sum_{\lambda=a}^{z} p_\lambda^2 \equiv 0,076$$

,

- Le tableau ci-dessous donne l'indice de coïncidence de certaines langues européennes.

anglais	français	allemand	portugais	espagnol
0,066	0,076	0,076	0,079	0,078

L'indice de coïncidence d'un texte est invariant par chiffrement par décalage.

Proposition

Soit M un texte et $k \in \{0, \ldots, 25\}$. Soit C le chiffré par décalage de k rangs de M. Nous avons

$$I_c(C) = I_c(M) \quad (= 0,076 \textit{ en français})$$

Par contre au vu de la Proposition 1, si C est un chiffré de Vigenère (de longueur de clef ¿=2) la fréquence des lettres se rapproche de $1/26$ et donc

$$I_c(C) \cong 0.4$$

Méthode pour le calcul de la longueur de la clef.

Pour calculer la longueur de la clef on va procéder comme suit

1. On choisit ℓ susceptible d'être la longueur de la clef.
2. On découpe le message chiffré C en ℓ sous messages $C_1, \ldots, C_\ell$

$$\begin{aligned} C_1 &= (c_1, c_{1+\ell}, c_{1+2\ell}, \ldots) \\ C_2 &= (c_2, c_{2+\ell}, c_{2+2\ell}, \ldots) \\ &\vdots \\ C_\ell &= (c_\ell, c_{2\ell}, c3\ell, \cdots) \end{aligned}$$

3. On calcule ensuite pour tout $j = 1, \ldots, \ell$ l'indice $I_c(C_j)$ et si chacun des $I_c(C_j) \cong 0,076$ alors ℓ devrait être la bonne longueur (ou en fait un multiple). Sinon on choisit un autre candidat pour ℓ et on retourne à l'étape 1.

Exemple détaillé

On considère le texte suivant chiffré avec une méthode de Vigenère.

owdoapfntvulxcfxvldrykycoboobcoepcjrscpcpcopzbblwblcncoccydg
kmlxbdywwscxoclwxczqzcnpxdywxycccenfhrycnndntvnekrecdcvnoybf
xmzcjfcbtndcadfxnnkalzjnoneowcoupfjyddyznfvjeocpsugscmyvmokc
ewnvxtcxyxnakaooblblpkdizufcatqroobdywllmzwnycdcvnskdendbenw
vjnydgoaeeapzapdnlqutcbpbczeclpjtdwpdnykrezufczfkypswpcndxxx
lapebpcyldcpculwnydjmvnxoweqapvndzjcmxxzjckrdywlfnnvjnyaaeup
xlpadtvjgkrezjckrwvnfbbrbxfsuwkrpxcoobpcypbnxowecxfcbpchpeg

Exemple, Longueur de la clef

Les indices de coïncidence du texte sont

Longueur ℓ				
1	$0,053968$			
2	$0,060726$	$0,053560$		
3	0.082551	$0,086633$	$0,082755$	
4	$0,053061$	$0,063220$	$0,061950$	$0,062857$

Exemple, Longueur de la clef

Les indices de coïncidence du texte sont

Longueur ℓ				
1	0,053968			
2	0,060726	0,053560		
3	0.082551	0,086633	0,082755	
4	0,053061	0,063220	0,061950	0,062857

Découpons le texte en trois sous-messages

$$C_1 = oofvxxdkooocscobwcoyk...$$
$$C_2 = wanucvrybbejcppbbncdm...$$
$$C_3 = dptlflycocprpczllccg...$$

sous-texte							
C_1	a	b	c	d	e	f	g
	0.071	0.100	0.085	0.085	0.007	0.000	0.007
	h	i	j	k	l	m	
	0.007	0.000	0.092	0.007	0.014	0.021	
	n	o	p	q	r	s	t
	0.171	0.000	0.014	0.007	0.064	0.000	0.000
	u	v	w	x	y	z	
	0.064	0.014	0.071	0.057	0.028	0.007	

sous-texte							
C_2	a	b	c	d	e	f	g
	0.021	0.007	0.107	0.042	0.071	0.085	0.028
	h	i	j	k	l	m	
	0.000	0.007	0.000	0.000	0.100	0.021	
	n	o	p	q	r	s	t
	0.050	0.035	0.171	0.000	0.014	0.007	0.057
	u	v	w	x	y	z	
	0.000	0.000	0.028	0.035	0.071	0.035	
C_3	a	b	c	d	e	f	g
	0.014	0.043	0.151	0.057	0.057	0.021	0.000
	h	i	j	k	l	m	
	0.007	0.000	0.000	0.093	0.014	0.007	
	n	o	p	q	r	s	t
	0.014	0.129	0.007	0.021	0.000	0.043	0.000
	u	v	w	x	y	z	
	0.000	0.086	0.035	0.071	0.057	0.064	

sous-texte	lettre de plus haute fréquence	décalage
$c(3,1)$	p	11
$c(3,2)$	c	24
$c(3,3)$	n	9

ensereveillantunmatinapresdesrevesagitesgregor
samsaseretrouvadanssonlitmetamorphoseenun
monstrueuxinsecte

Plan

Période de faiblesse cryptographique

Entre 1870 et 1920 on assiste à une nouvelle période de faiblesse cryptographique.

- L'entrée en guerre des Etats Unis.
  - En juin 1917 le ministère des affaires étrangère allemand envoie un message à son ambassadeur au Mexique.
  - Il souhaite encourager le Mexique à entrer en guerre contre les USA.
  - Le message fut intercepté et décrypté par les anglais, qui le transmettent au président américain.
  - C'est ce qui décidera les américains à entrer en guerre contre les allemands.
- L'offensive allemande de juin 1918.
  - C'est le code de Vigenère mais avec *en plus* les symboles numériques.
  - Mis au point avant l'offensive de juin 1918.
  - Un message fut intercepté indiquant que les allemands préparaient une offensive.
  - Il fut décrypté, et l'armée Française pu contrer l'offensive.

Naissance d'Enigma

- Après la guerre :
  - l'importance grandissante des communications électriques,
  - la faiblesse des schémas de chiffrement

  poussèrent deux allemands **Scherbius et Ritter** à inventer une machine à chiffrer électrique et automatique **Enigma**.
- L'invention jugée d'abord curieuse, fut ensuite reconnue comme ayant une efficacité redoutable.
- Malgré son prix très élevé, plusieurs pays ou grandes compagnies s'en équipèrent.
- L'Allemagne y vint tardivement (1930), elle en commanda 30 000 pour son armée.
- Enigma devint alors le fer de lance du renseignement allemand.

Enigma

Description d'Enigma

La faiblesse de Vigenère était lié à l'aspect cyclique du processus. Enigma est une variante de Vigenère mais supprime cette cyclicité.

Elle comporte

- 3 disques ou rotors, sur chacun desquels un alphabet était gravé.
- Un reflecteur (B).
- Un panneau de connecteurs.

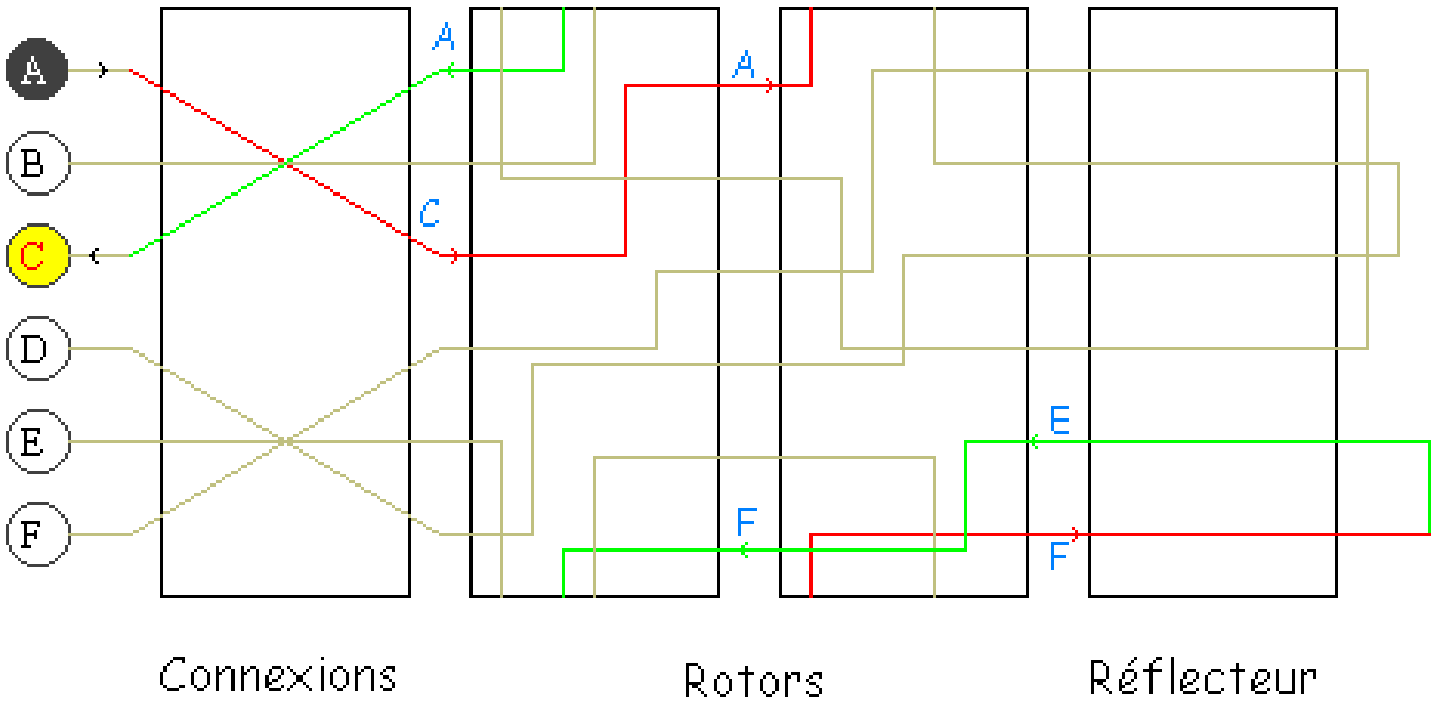
Description d'Enigma

La faiblesse de Vigenère était lié à l'aspect cyclique du processus. Enigma est une variante de Vigenère mais supprime cette cyclicité.

Elle comporte

- 3 disques ou rotors, sur chacun desquels un alphabet était gravé.
- Un reflecteur (B).
- Un panneau de connecteurs.

Fonctionnement d'Enigma



Fonctionnement d'Enigma

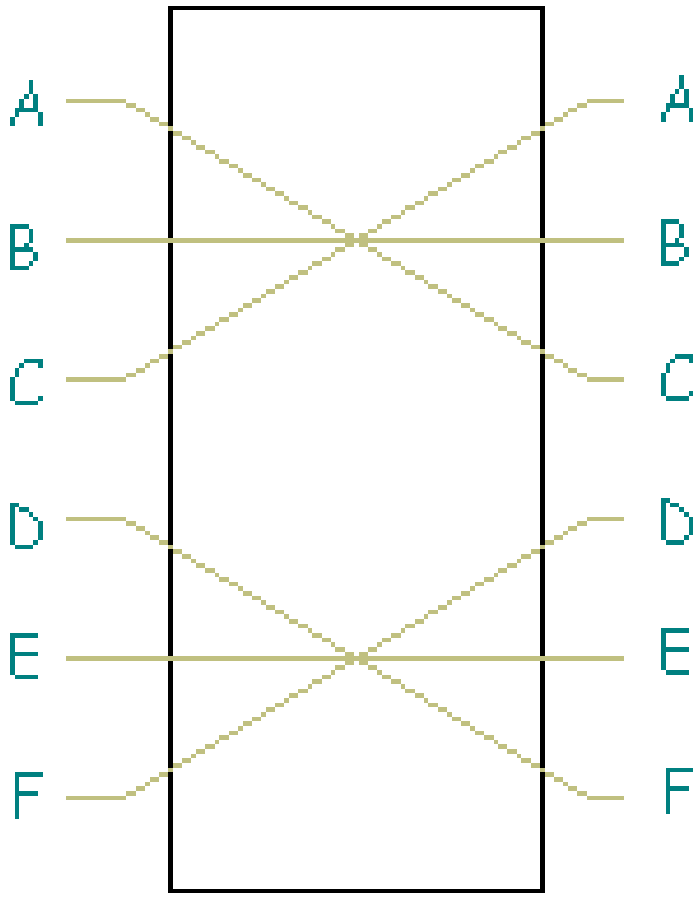
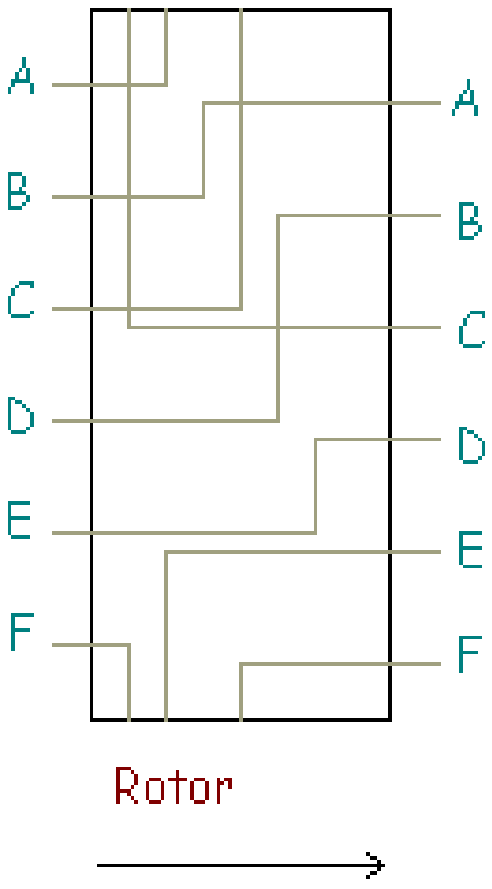


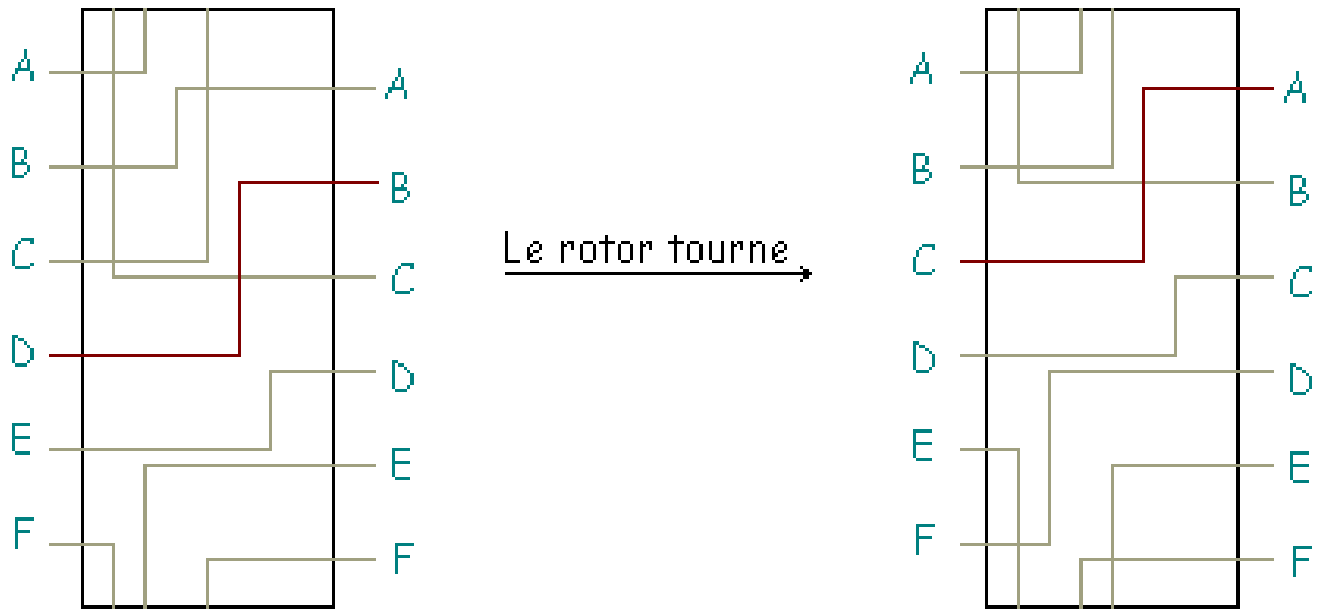
Tableau de connexions

Fonctionnement d'Enigma

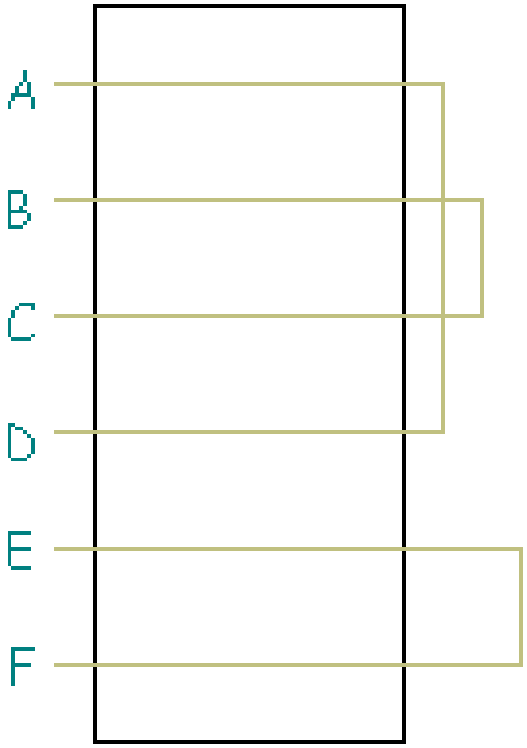


Entrée	Sortie
A	E
B	A
C	F
D	B
E	D
F	F

Fonctionnement d'Enigma



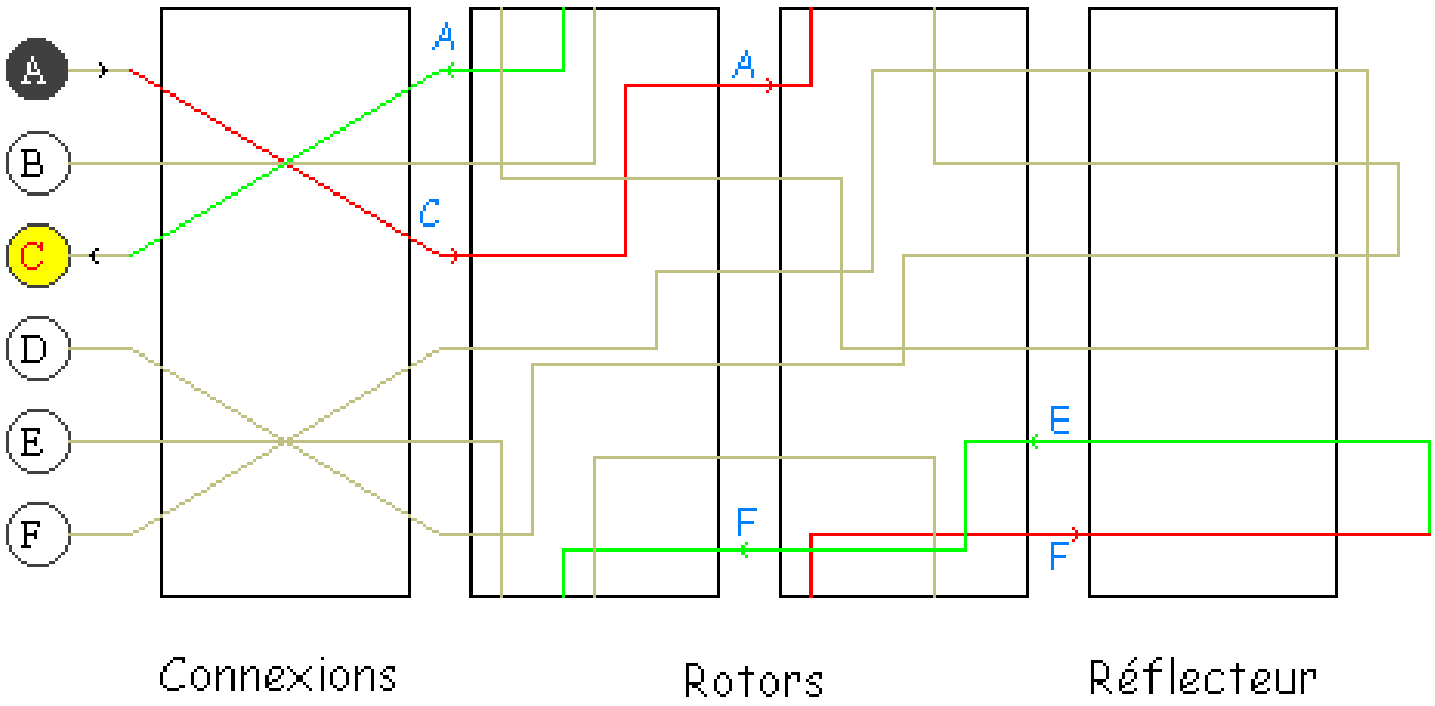
Fonctionnement d'Enigma



A est permuté avec D, B est permuté avec C, et E avec F.

Le réflecteur

Fonctionnement d'Enigma



Nombre de clefs

Il y a trois éléments à connaitre pour pouvoir coder un message avec la machine Enigma.

1. la position des 6 fiches du tableau de connexion

   $$100391791500 \text{ possibilités.}$$

2. l'ordre des rotors : il y a autant d'ordre que de façons d'ordonner 3 éléments : $3! = 6$.
3. la position initiale des rotors : chaque rotor ayant 26 éléments, il y a $26 * 26 * 26 = 17576$ choix possible.

On multiplie tout cela, et on obtient plus de $1782061951644000 \cong 10^{16}$ possibilités.

Principe de Kerckhoffs

Un des principes de la cryptographie moderne, principe de Kerckhoffs (19eme siècle)

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

Enigma était l'une des première à satisfaire le principe de Kerckhoffs.

Attaque d'Enigma

- Le chiffrement d'Enigma fut attaqué pendant la guerre 1940-1945 par les Polonais jusqu'en 1940 puis par les anglais.
- La faiblesse d'Enigma = seul les rotors ont un rôle cryptographique important.
- Le nombre de positions de rotor est de 17576.
- Les rotors utilisés et leur position pouvaient être déterminés par une attaque exhaustive grâce à une automatisation de l'attaque.

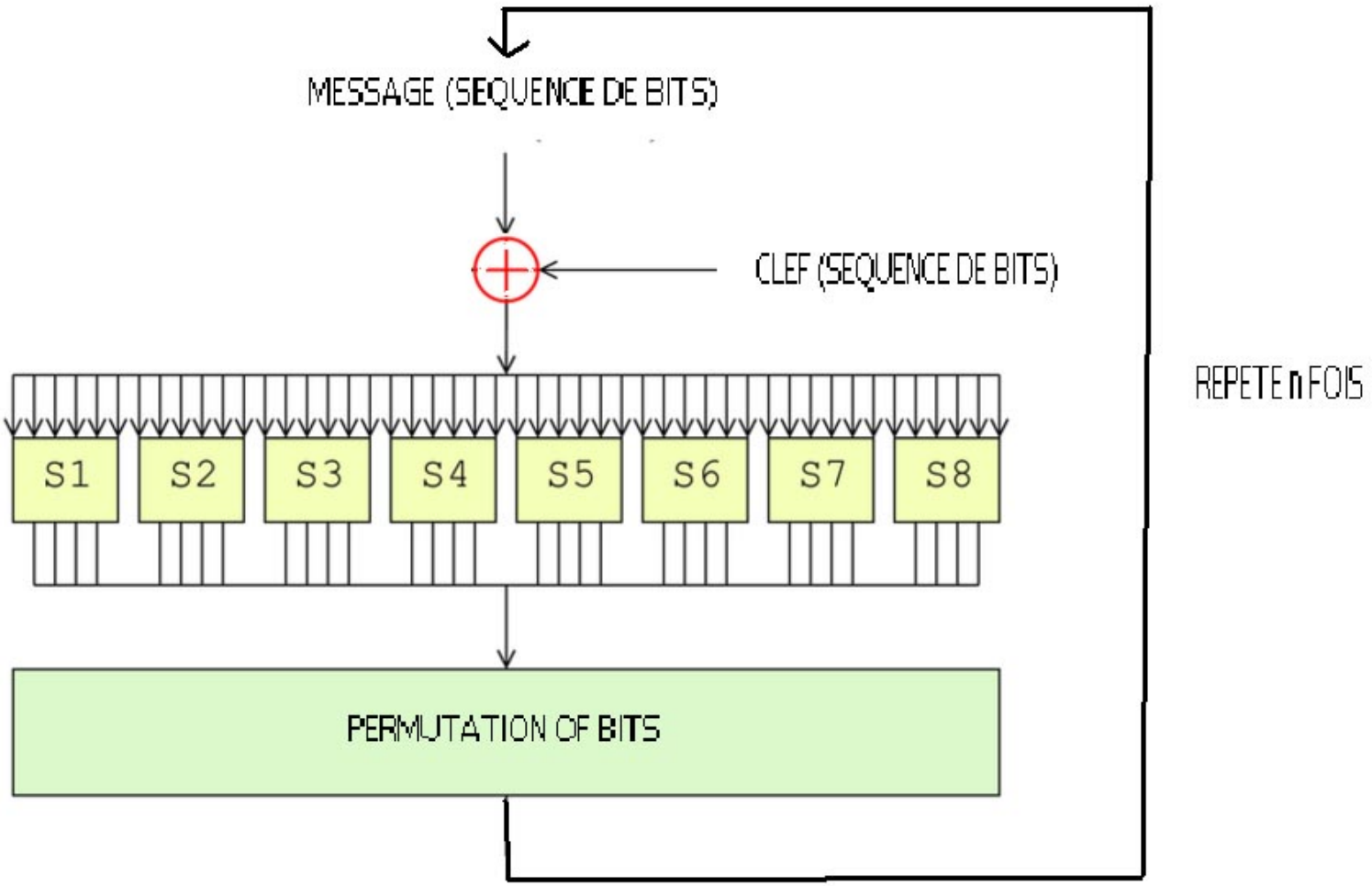
Plan

Utilisation actuelle de la cryptographie

Avec les moyens de communications actuel, la cryptographie est devenu d'usage courant pour tout un chacun

- Carte à puce.
- Téléphone portable.
- Courrier électronique, connection.
- Commerce électronique.
- etc.

Le chiffrement à clef secrète moderne

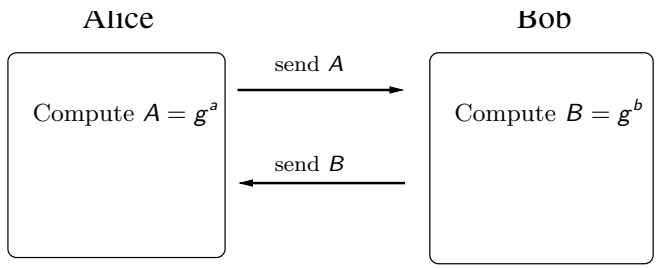


Le problème de l'échange de clef

- Dans les années 60-70, le besoin de communication sécurisé est de plus en plus important.
- Les modes de chiffrement à clef secrètes, nécessite que deux personne distante aient une clef commune.
- Des sociétés se sont donc spécialisées dans l'échange de clef.

L'échange de clef de Diffie-Hellman

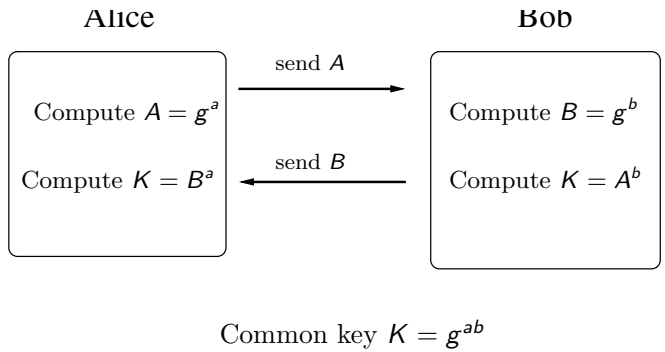
Soit p un entier premier grand ($\sim 2^{1000}$) et $2 \leq g \leq p$.



Si p, a, b sont grand alors c'est *impossible* de *calculer* $g^{ab} \mod p$ *à partir de* $g, g^a \mod p, g^b \mod p$.

L'échange de clef de Diffie-Hellman

Soit p un entier premier grand ($\sim 2^{1000}$) et $2 \leq g \leq p$.



Si p, a, b sont grand alors c'est *impossible* de *calculer* $g^{ab} \mod p$ *à partir de* $g, g^a \mod p, g^b \mod p$.

La cryptographie à clef publique

- L'idée de Diffie-Hellman étaient révolutionnaire.
- Elle a ouvert la voie d'une nouvelle cryptographie ne necessitant plus l'échange de clef préalable.
- Aujourd'hui la cryptograhie cours toujours apres son graal

  Un système de chiffrement RAPIDE et PROUVE SUR

Références

- Histoire des codes Secrets. Simon Singh. Livre de poche.
- Cryptographie - Théorie et Pratique - 2ème édition - Douglas Stinson - Vuibert.
- `http://www.apprendre-en-ligne.net/crypto/menu/index.html`
- `http://www.bibmath.net/crypto/`