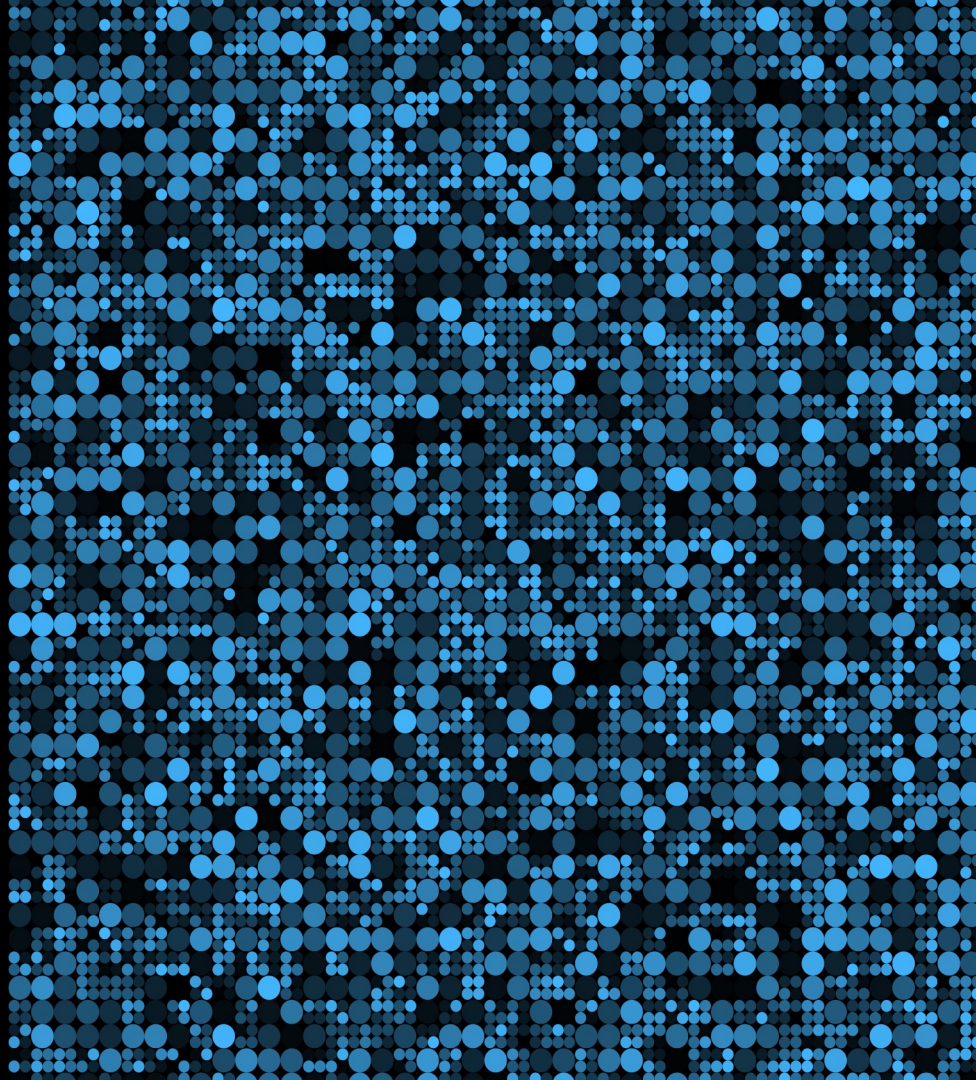
Cryptologie

Bastien Vialla

bastien.vialla@orange.com

Année 2023-2024



Qu’est ce que la cryptologie ?

- **Cryptologie :**
  - Cryptographie :
    - Crypto = caché, graphie = écriture
    - L’art de « caché » une message, de le rendre illisible

Qu’est ce que la cryptologie ?

- **Cryptologie :**
  - Cryptographie :
    - Crypto = caché, graphie = écriture
    - L’art de « caché » une message, de le rendre illisible
    - ATTENTION : On cache le contenu du message pas le fait qu’on écrit une message.
      - Stéganographie

Exemples de Stéganographie

- **Encres invisibles : 1er siècle av. J.C. Pline l'Ancien**

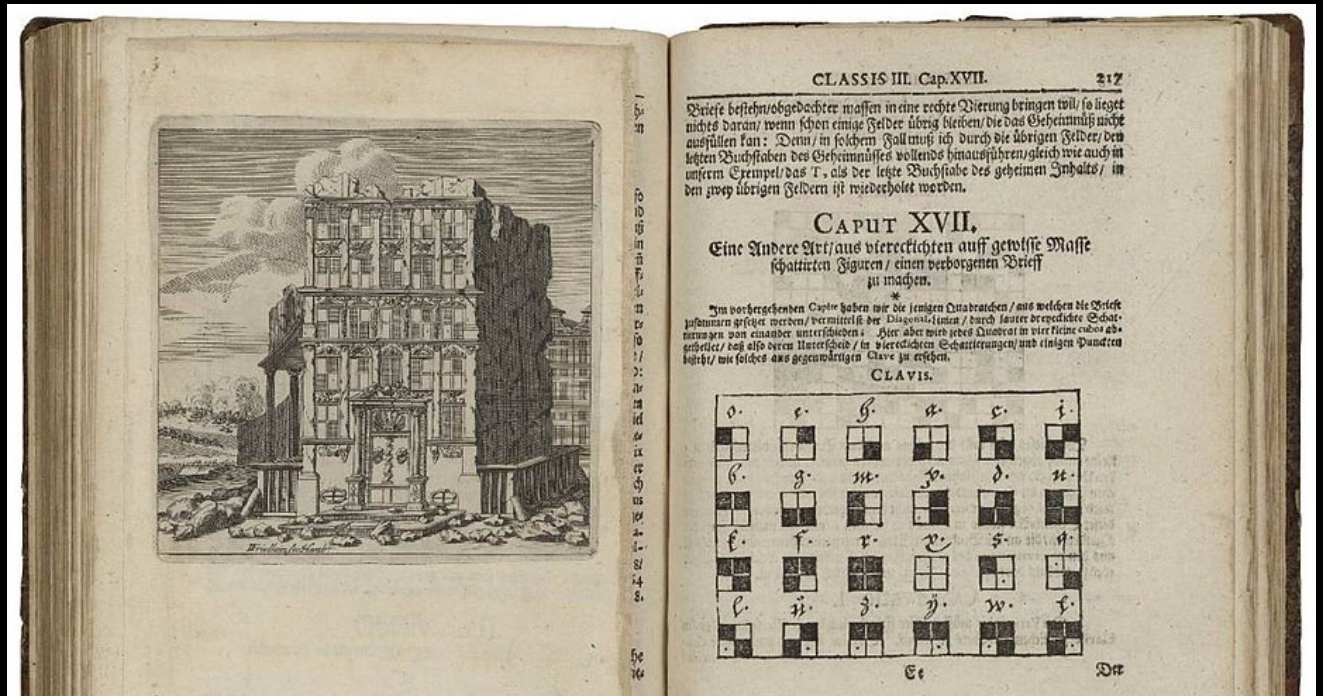
Exemples de Stéganographie

- **Encres invisibles : 1er siècle av. J.C. Pline l'Ancien**

- **Dessins : Johannes Balthasar Friderici, *Cryptographia oder Geheime Schrifft-münd- und Würkliche Correspondendentz (1684)***

Exemples de Stéganographie

- **Encres invisibles : 1er siècle av. J.C. Pline l'Ancien**
- **Dessins : Johannes Balthasar Friderici, *Cryptographia oder Geheime Schrifft-münd- und Würkliche Correspondendentz (1684)***



CLASSIS III. Cap. XVII. 217

Briefe bestehn/obgedachter massen in eine rechte Vierung bringen will/ so lieget nichts daran/ wenn schon einige Felder übrig bleiben/ die das Geheimniß nicht ausfüllen kan: Denn/ in solchem Fall muß ich durch die übrigen Felder/ den letzten Buchstaben des Geheimnüsses vollends hinausführen/ gleich wie auch in unserm Exempel/ das T. als der letzte Buchstabe des geheimen Inhalts/ in den zwey übrigen Feldern ist wiederholet worden.

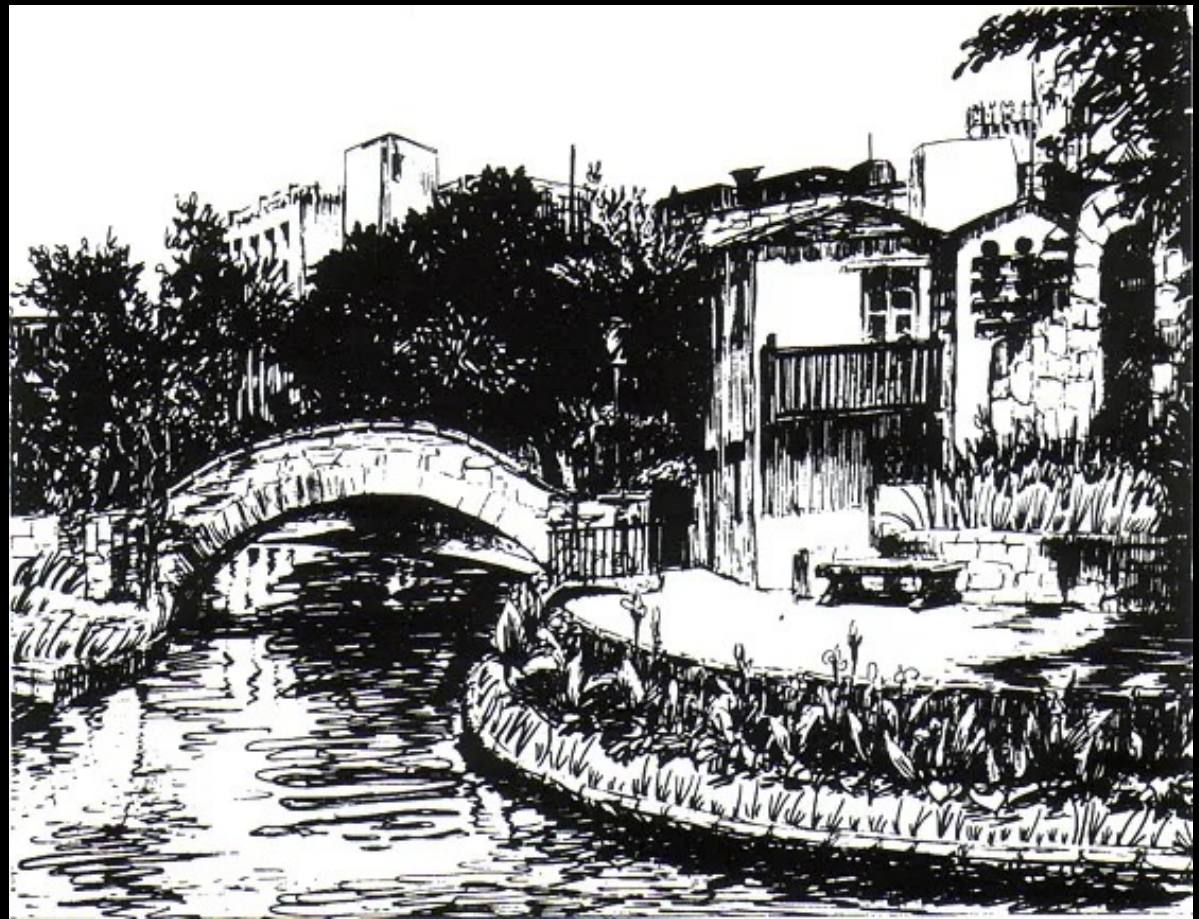
CAPUT XVII.

Eine Andere Art/ aus viereckichten auff gewisse Masse schattirten Figuren/ einen verborgenen Brieff zu machen.

Im vorhergehenden Capite haben wir die jenigen Quadratchen/ aus welchen die Briefe zusammen gesetzet werden/ vermittelst der Diagonal-linien/ durch lauter dreyeckichte Schattierungen von einander unterschieden. Hier aber wird jedes Quadrat in vier kleine cubos abgetheilet/ daß also deren Unterscheid/ in viereckichten Schattierungen/ und einigen Punckten bestehet/ wie solches aus gegenwärtigen Clave zu ersehen.

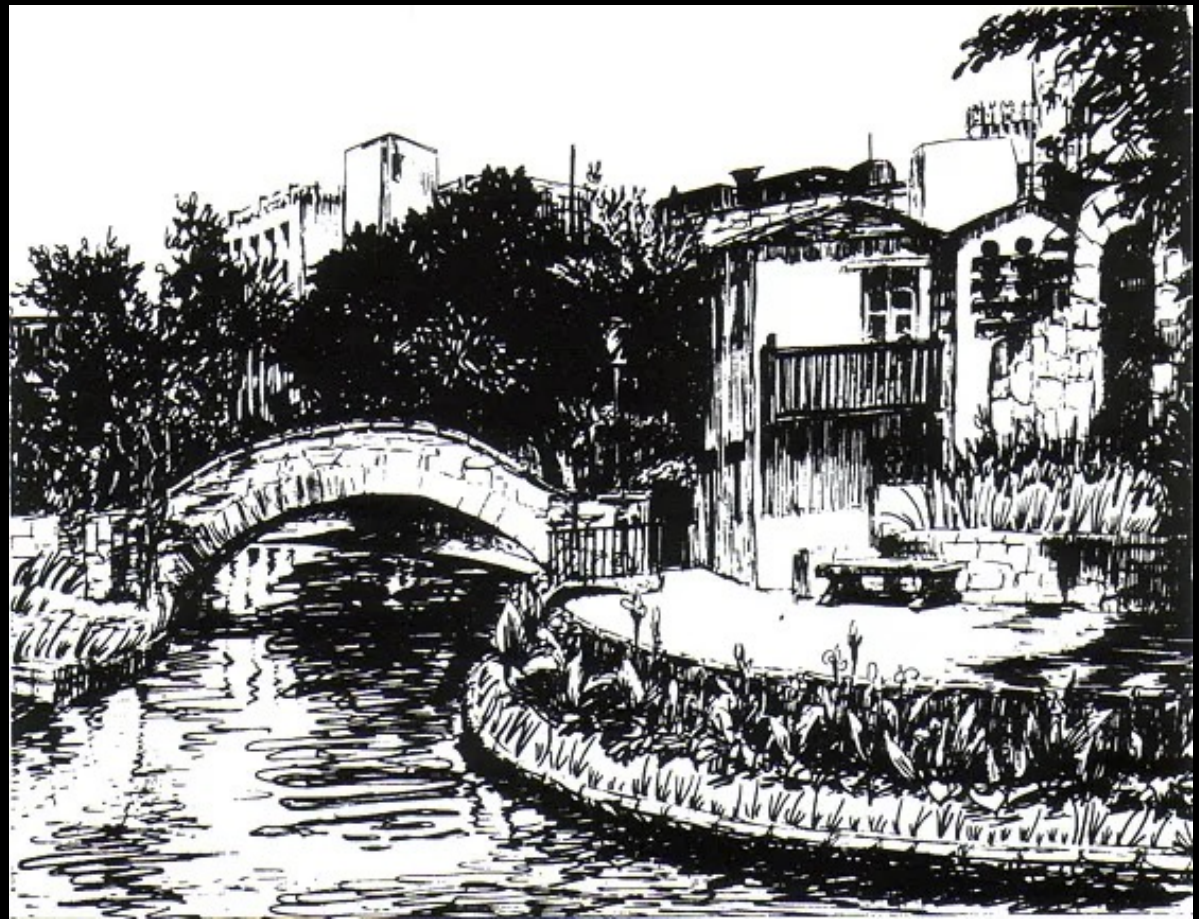
CLAVIS.

Exemples de Stéganographie



Exemples de Stéganographie

- Les brins d'herbe le long de la rivière et sur le mur du jardin
- La longueur des brins d'herbe représentent les points et traits de l'alphabet Morse



Exemples de Stéganographie

- **Encres invisibles : 1er siècle av. J.C. Pline l'Ancien**
- **Dessins : Johannes Balthasar Friderici, *Cryptographia oder Geheime Schrifft-münd- und Würkliche Correspondendentz (1684)***
- **Méthodes modernes**
  - Images : utilisation des bits de poids faibles des pixels pour cacher le message
  - Audio : utilisation des sons inaudible par l'humain (ultrasons) pour cacher le message

Qu’est ce que la cryptologie ?

- **Cryptologie :**
  - Cryptographie :
    - Crypto = caché, graphie = écriture
    - L’art de « caché » une message, de le rendre illisible
    - ATTENTION : On cache le contenu du message pas le fait qu’on écrit une message.
      - Stéganographie
      - Utiliser pour cacher les paramètres de config par certains malwares
      - Watermarks invisibles

Qu’est ce que la cryptologie ?

- **Cryptologie :**
  - Cryptographie :
    - Crypto = caché, graphie = écriture
    - L’art de « caché » une message, de le rendre illisible

- **Cryptanalyse :**
  - Crypto = caché, analyse = analyse
  - L’analyse des messages chiffrés
  - L’attaque des systèmes de cryptographie

Exemples d’applications

- Sur les sites internet httpS
- Cartes à puces : cartes bancaires, carte vitale, …

Exemples d’applications

- Sur les sites internet httpS
- Cartes à puces : cartes bancaires, carte vitale, …
- Dans les puces RFID (Radio Frequency IDentification)
- Plateformes de streaming (Netflix, PrimeVideo, …)

Exemples d’applications

- Sur les sites internet httpS
- Cartes à puces : cartes bancaires, carte vitale, …
- Dans les puces RFID (Radio Frequency IDentification)
- Plateformes de streaming (Netflix, PrimeVideo, …)
- Télécommunications : WIFI, 4G / 5G, …
- Smartphones

Vocabulaire utile

- Le clair (plaintext) : le message que l'on souhaite envoyer
- Le chiffré (ciphertext) : le message après avoir été « caché »

Vocabulaire utile

- Le clair (plaintext) : le message que l'on souhaite envoyer
- Le chiffré (ciphertext) : le message après avoir été « caché »
- Chiffrer (encrypt) : l'opération qui transforme le clair en chiffré à partir d'une autre information (la clé de chiffrement)
- Déchiffrer (decrypt) : L'opération qui révèle le clair à partir du chiffré, grâce à une information (la clé de déchiffrement)

Vocabulaire utile

- Le clair (plaintext) : le message que l'on souhaite envoyer
- Le chiffré (ciphertext) : le message après avoir été « caché »
- Chiffrer (encrypt) : l'opération qui transforme le clair en chiffré à partir d'une autre information (la clé de chiffrement)
- Déchiffrer (decrypt) : L'opération qui révèle le clair à partir du chiffré, grâce à une information (la clé de déchiffrement)
- Décrypter : retrouver le clair à partir du chiffré sans connaître la clé
- Attention ! « Crypter » n'est pas un mot français.

Cryptomonnaies ≠ Cryptologie

- **Attention ! Les « cryptos » ne sont pas à confondre avec cryptologie / cryptographie.**

- **Définition par l'autorité des marchés financiers (AMF):**

« Une cryptomonnaie ou un cryptoactif désigne des actifs numériques virtuels qui reposent sur la technologie de la blockchain (chaine de bloc) à travers un registre décentralisé et un protocole crypté. »

Les garanties de la cryptographie

- **Confidentialité :** le message ne pourra être lu que par son destinataire légitime
- **Intégrité** : le destinataire peut s’assurer que le message n’a pas été modifié

Les garanties de la cryptographie

- **Confidentialité :** le message ne pourra être lu que par son destinataire légitime
- **Intégrité** : le destinataire peut s'assurer que le message n'a pas été modifié
- **Authenticité** : le destinataire peut s'assurer de l'origine du message (que l'expéditeur est bien celui qu'il prétend être)
- **Non répudiation** : l'expéditeur ne peut nier être à l'origine du message

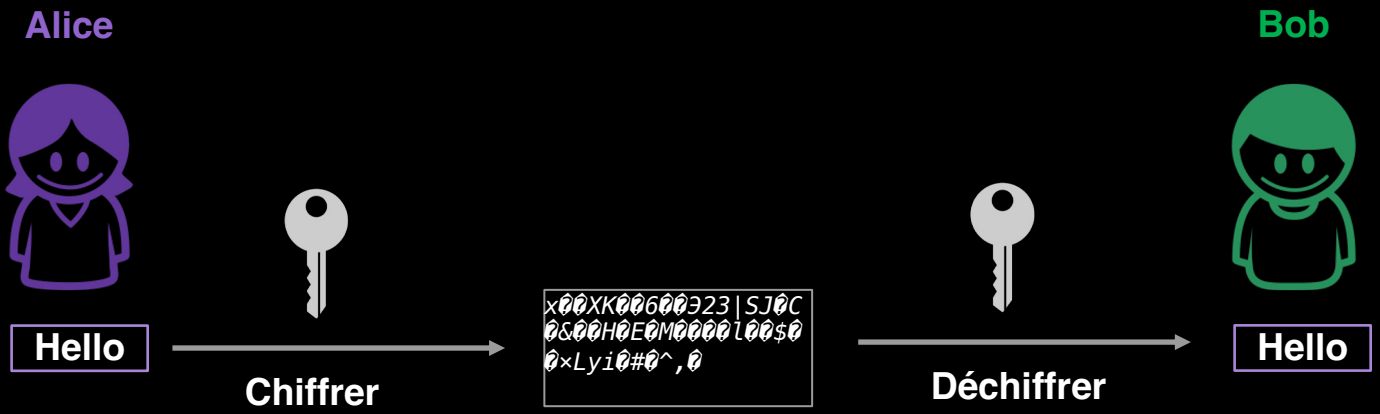
Principe(s) à retenir

- **Principe de Kerckhoffs : pour garantir la sécurité d'un schéma de chiffrement, la méthode doit être publique (elle finira par l'être un jour de toute façon). Seule une petite partie de la méthode (appelée clé) restera secrète et sera facilement modifiable.**

- **Loi de Moore : le nombre de transistors d'un cpu doubles tous les deux ans.**
  - N'est plus vraiment valable en 2023
  - La sécurité d'un protocole cryptographique se mesure en partie par la complexité algorithmique de casser un chiffré

Cryptographie Symétrique

Cryptographie symétrique, ou à clé secrète



Chiffrements antiques : la Scytale

- Message écrit le long du cylindre, une lettre par morceau de ruban.

- Message chiffré correspond à la lecture du ruban déroulé

Chiffrements antiques : la Scytale

- Message écrit le long du cylindre, une lettre par morceau de ruban.
- Message chiffré correspond à la lecture du ruban déroulé
- Pour déchiffrer : connaître nombre N de lettres par tour de ruban ou L nombre de tour du ruban ($L \times N$ nombre de lettres du message)
- Enrouler le message autour du cylindre et le message clair apparait.

Chiffrements antiques : la Scytale

- Message écrit le long du cylindre, une lettre par morceau de ruban.
- Message chiffré correspond à la lecture du ruban déroulé
- Pour déchiffrer : connaître nombre N de lettres par tour de ruban ou L nombre de tour du ruban ($L \times N$ nombre de lettres du message)
- Enrouler le message autour du cylindre et le message clair apparait.
- C’est un chiffrement par permutation

Chiffrements antiques : le chiffrement de César

- On décale chaque lettre de 3 rangs

a	b	c	d	e	f	g	h	i	…	v	w	x	y	z
d	e	f	g	h	i	j	k	l	…	y	z	a	b	c

Chiffrements antiques : le chiffrement de César

- On décale chaque lettre de 3 rangs

a	b	c	d	e	f	g	h	i	…	v	w	x	y	z
d	e	f	g	h	i	j	k	l	…	y	z	a	b	c

Exemple:

m	e	s	s	a	g	e
12	4	18	18	0	6	4
15	7	21	21	3	9	7
p	h	v	v	d	j	h

Chiffrements antiques : le chiffrement de César

- On décale chaque lettre de 3 rangs

a	b	c	d	e	f	g	h	i	…	v	w	x	y	z
d	e	f	g	h	i	j	k	l	…	y	z	a	b	c

Exemple:

m	e	s	s	a	g	e
12	4	18	18	0	6	4
15	7	21	21	3	9	7
p	h	v	v	d	j	h

- C’est une substitution monoalphabétique

Chiffrements antiques : ROT 13

- On décale chaque lettre de 13 rangs

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

Exemple:

m	e	s	s	a	g	e
12	4	18	18	0	6	4
25	17	5	5	13	19	17
z	r	f	f	n	t	r

Chiffrements antiques : ROT 13

- On décale chaque lettre de 13 rangs

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

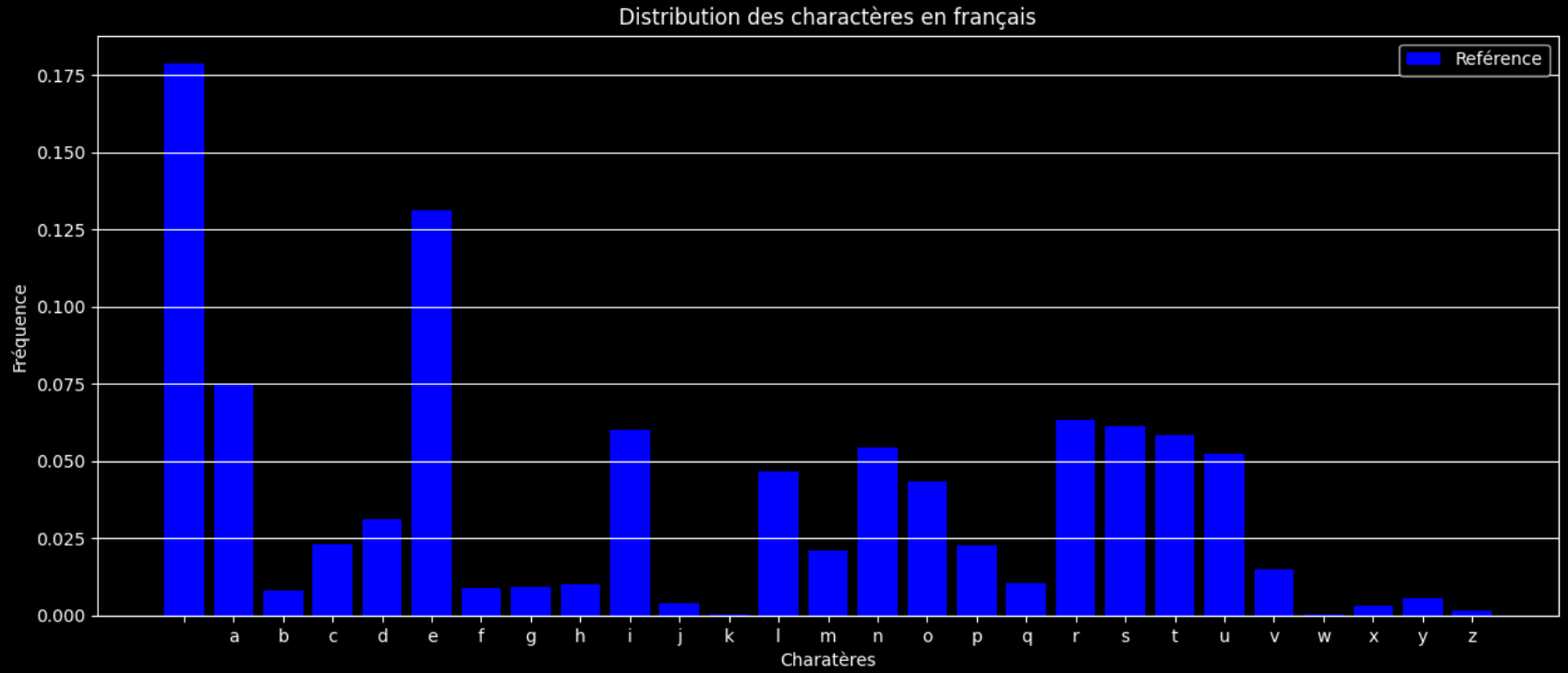
Exemple:

m	e	s	s	a	g	e
12	4	18	18	0	6	4
25	17	5	5	13	19	17
z	r	f	f	n	t	r

- Attention ! Rot13(Rot13(m)) = m

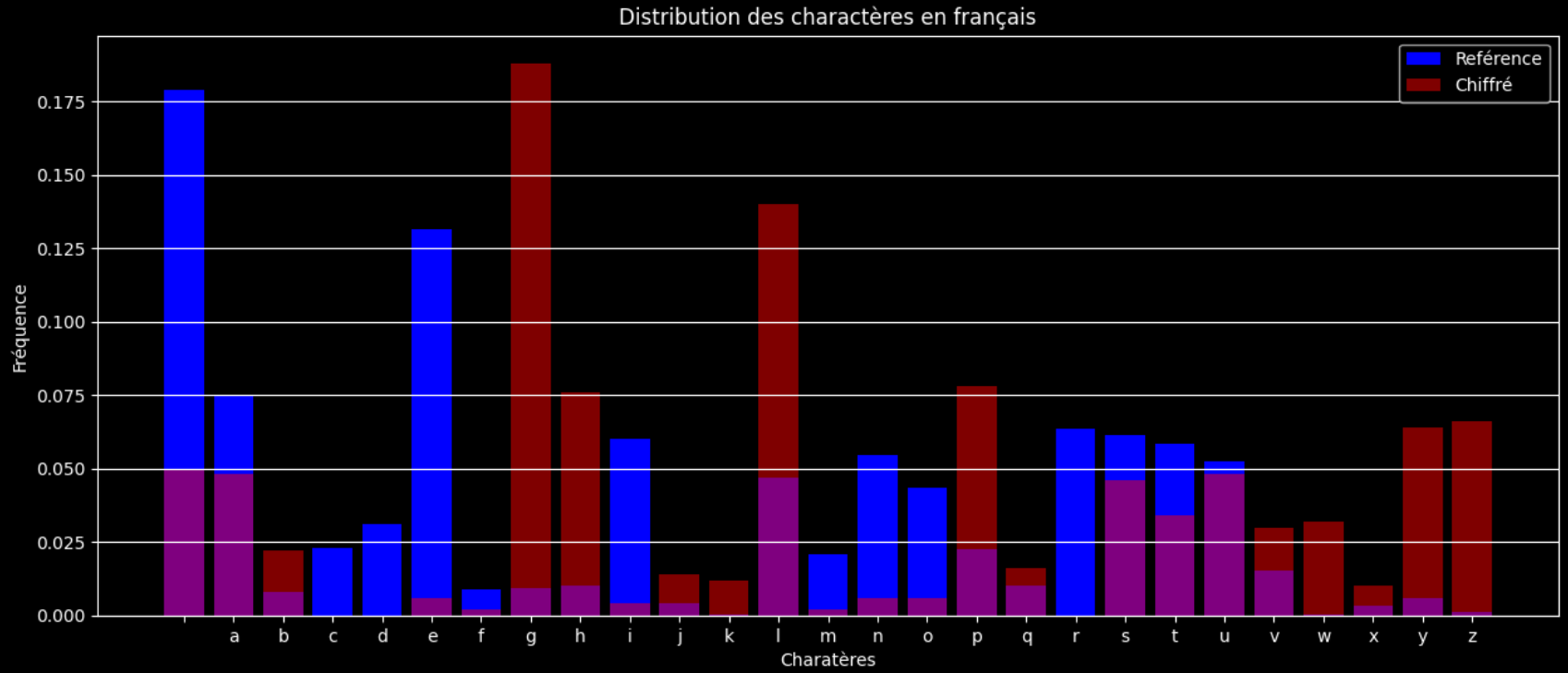
Cryptanalyse : analyse fréquentielle

- **Une langue donnée à une distribution caractéristique d'apparition des lettres**



Cryptanalyse : analyse fréquentielle

- **Comparer la distribution des lettres du chiffré avec la distribution de référence**



Analyse fréquentielle : test χ^2

- Manuellement, on peut tester toutes les clés possibles et essayer de lire résultat

Analyse fréquentielle : test χ^2

- **Manuellement, on peut tester toutes les clés possibles et essayer de lire résultat**
- **Ou, mesurer la distance entre les distributions avec le test statistique χ^2**

$$\chi^2 = \sum_{c \in Alphabet} \frac{(F_c - R_c)^2}{R_c}$$

F_c : la fréquence de la lettre *c* dans le chiffré
R_c : la fréquence de référence pour la lettre c

Analyse fréquentielle : test χ^2

- Manuellement, on peut tester toutes les clés possibles et essayer de lire résultat
- Ou, mesurer la distance entre les distributions avec le test statistique χ^2

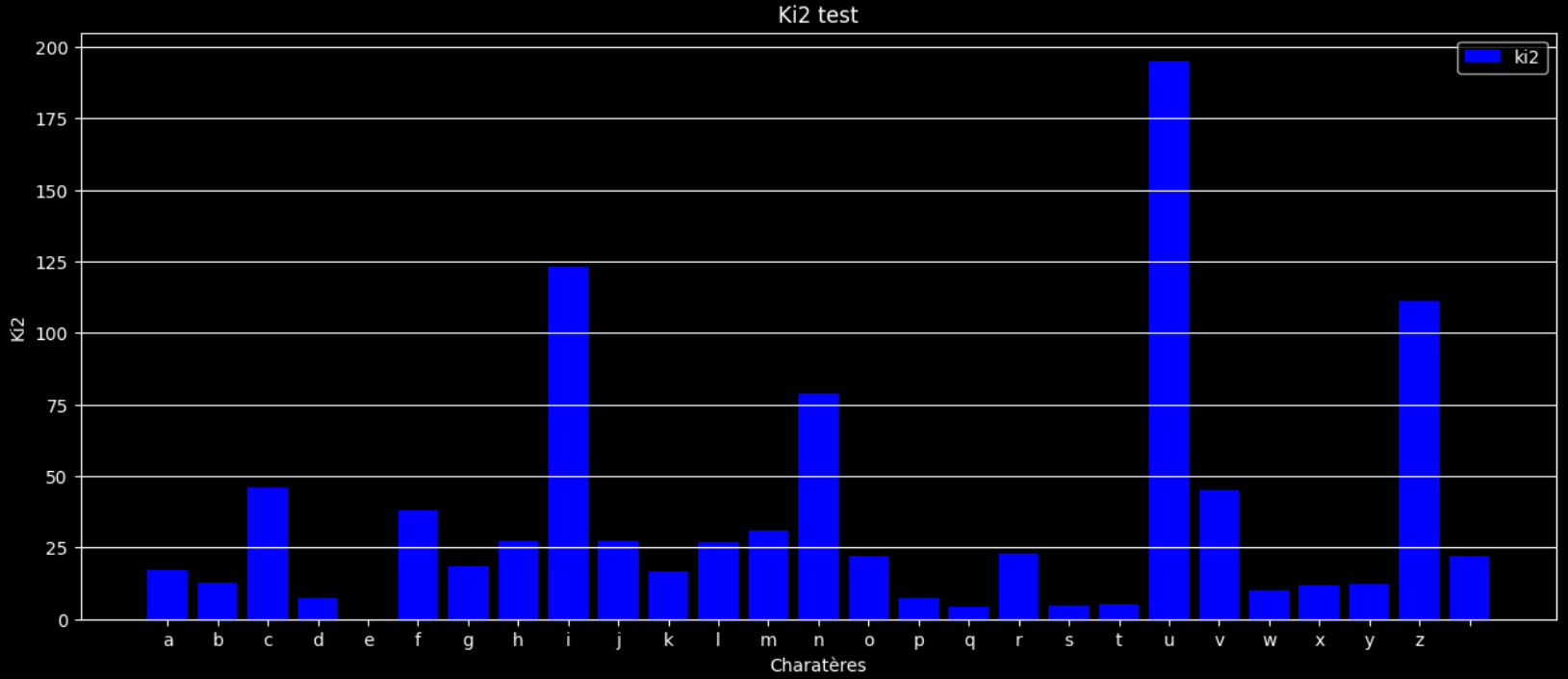
$$\chi^2 = \sum_{c \in Alphabet} \frac{(F_c - R_c)^2}{R_c}$$

F_c : la fréquence de la lettre ***c*** dans le chiffré
R_c : la fréquence de référence pour la lettre c

- La lettre donnant la valeur minimale pour le test χ^2 est la clé

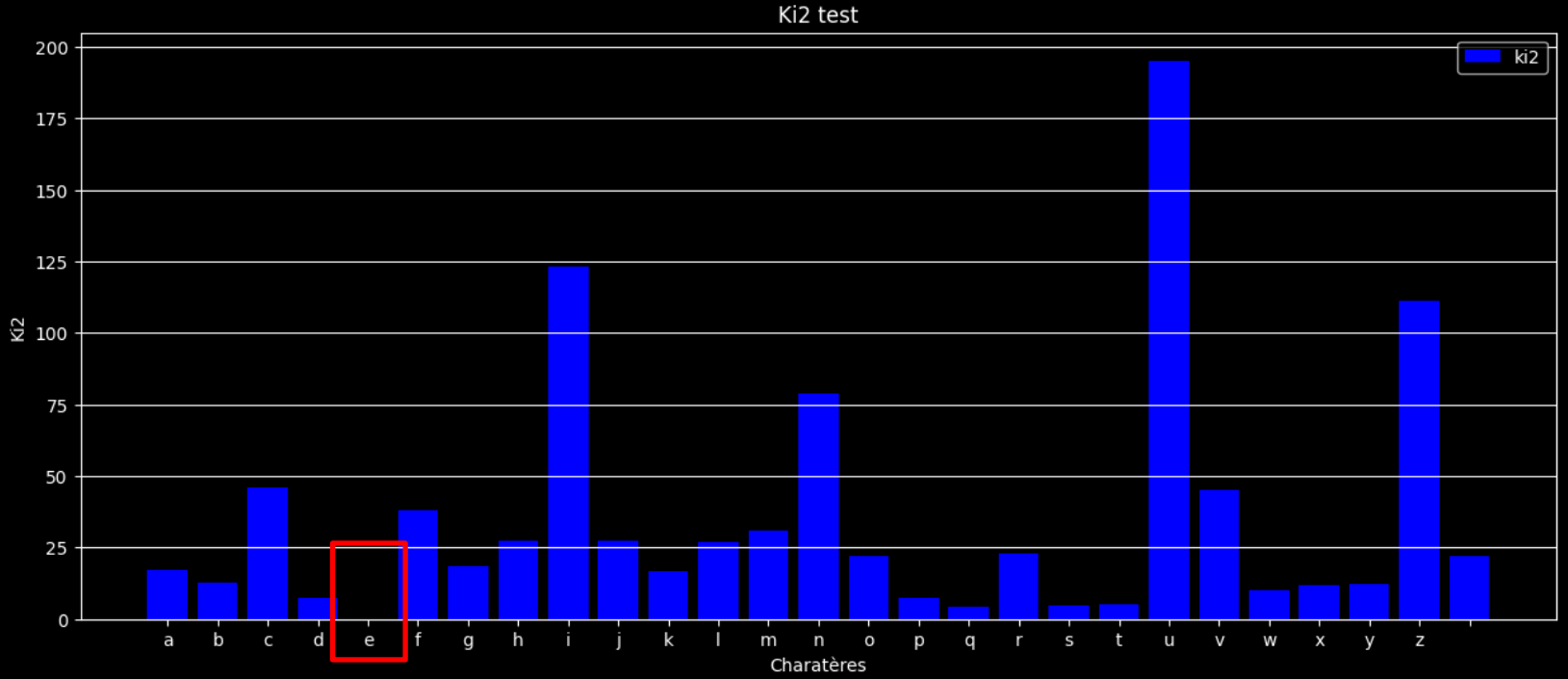
Analyse fréquentielle : test χ^2

- La lettre donnant la valeur minimale pour le test χ^2 est la clé



Analyse fréquentielle : test χ^2

- La lettre donnant la valeur minimale pour le test χ^2 est la clé, *e* est la clé



Chiffrement de Vigenère

- *Traicté des chiffres, ou Secrètes manières d'escrire, 1586*

Chiffrement de Vigenère

- *Traicté des chiffres, ou Secrètes manières d'escrire, 1586*

- Version latine du « tserouf », méthode méditative juive d'Abraham Aboulafia (1240)

אל	בת	גש	דר	הק	וץ	זפ	חע	טס	ין	כם
אב	גת	דש	הר	וק	זץ	חפ	טע	יס	כן	לם
אג	דת	הש	ור	זק	חץ	טפ	יע	בס	לן	בם
אד	בג	הת	וש	זר	חק	טץ	יפ	כע	לס	מג
אה	בד	ות	וש	הר	טק	יצ	כפ	לע	מס	נג
או	בה	גר	זת	חש	טר	יק	כצ	לפ	מע	נס
אז	בו	גה	הת	טש	יר	כק	לצ	מפ	נע	רס
אח	בז	גו	דה	טת	יש	כר	לק	מצ	נפ	סע
אט	בח	גו	דו	ית	כש	לר	מק	נצ	ספ	הע
אי	בט	גח	דז	הו	כת	לש	מר	נק	סצ	עפ
אכ	בי	גט	דח	הז	לת	מש	נר	סק	עצ	ופ
אל	בכ	גר	דט	החו	מת	נש	סר	עק	פר	פג
אמ	בל	גב	די	הט	וח	נת	סש	ער	פק	זצ
אנ	בם	גל	דכ	הי	וט	זח	סת	עש	פר	צק
אס	בנ	גם	דל	הכ	וי	זט	עת	פש	צר	חק
אע	בס	גן	דם	הל	וך	זי	חת	פת	צש	קר
אפ	בע	גס	דנ	הם	ול	זכ	חי	סת	קש	צר
אצ	בפ	גע	דס	הנ	ום	זל	חב	טי	קת	רש
אק	בצ	גפ	דע	הס	ון	זמ	חל	טנ	רת	יש
אר	בק	גצ	דפ	הע	וס	זנ	חמ	טל	יכ	שת
אש	בר	גק	דצ	הפ	וע	זס	חנ	טמ	יל	בת
את	בש	גר	דק	הצ	ופ	וע	חס	טנ	יס	כל
אל	בם	גנ	דס	הע	ופ	וצ	חק	טר	יש	כת
איק	בכר	גלש	דתת	הגך	וסם	זען	חפף	טצץ		

Chiffrement de Vigenère

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

Chiffrement de Vigenère

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

← **Chiffrement de César**

← **Chiffrement ROT13**

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré :

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré : N

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré : N I

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré : N I X

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré : N I X T

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

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

Exemple : clé BEF

Clair : M E S S A G E
Clé : B E F B E F B
Chiffré : N I X T E L F

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre
- C'est une substitution polyalphabétique

Chiffrement de Vigenère

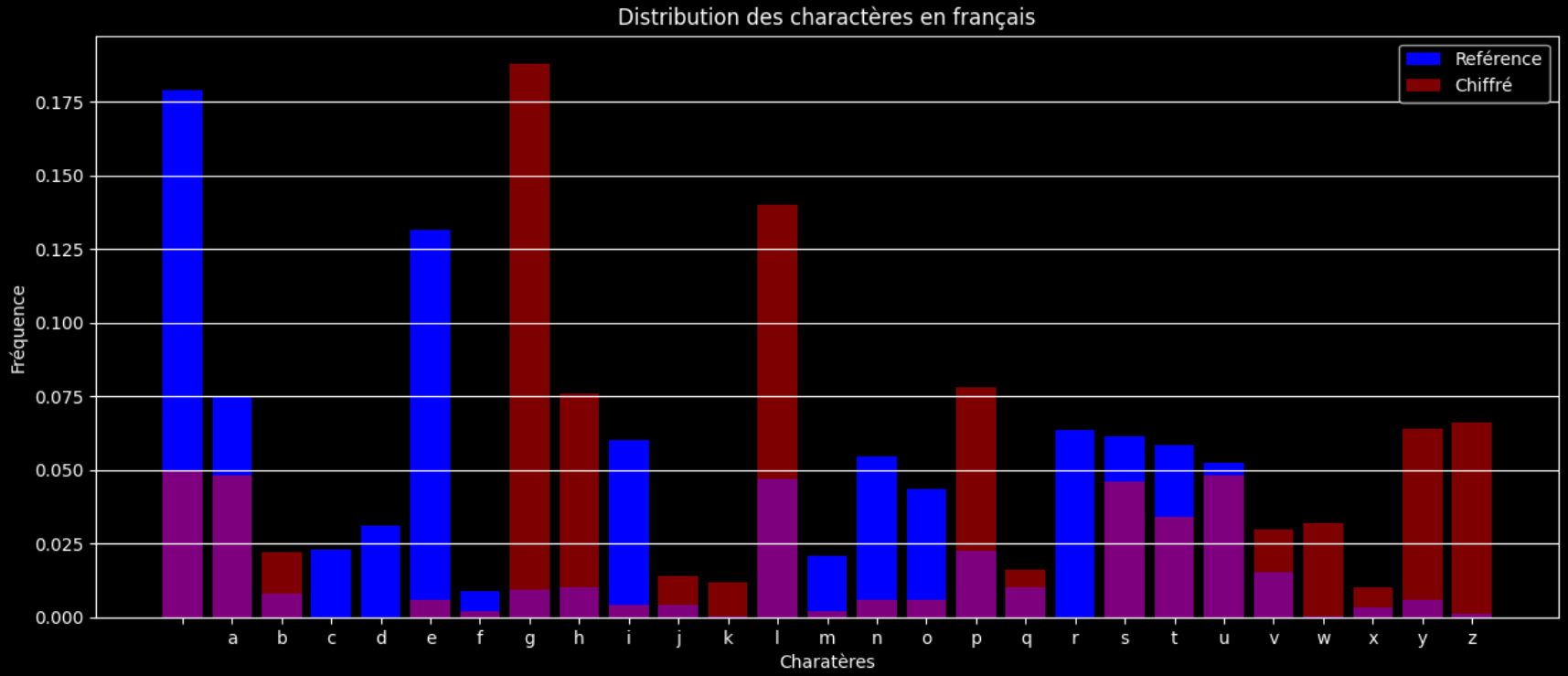
- La clé est un mot au lieu d'une seule lettre
- C'est une substitution polyalphabétique
- Cassé par Kasiski en 1863

Chiffrement de Vigenère

- La clé est un mot au lieu d'une seule lettre
- C'est une substitution polyalphabétique
- Cassé par Kasiski en 1863
- Résiste aux attaques par analyse fréquentielle

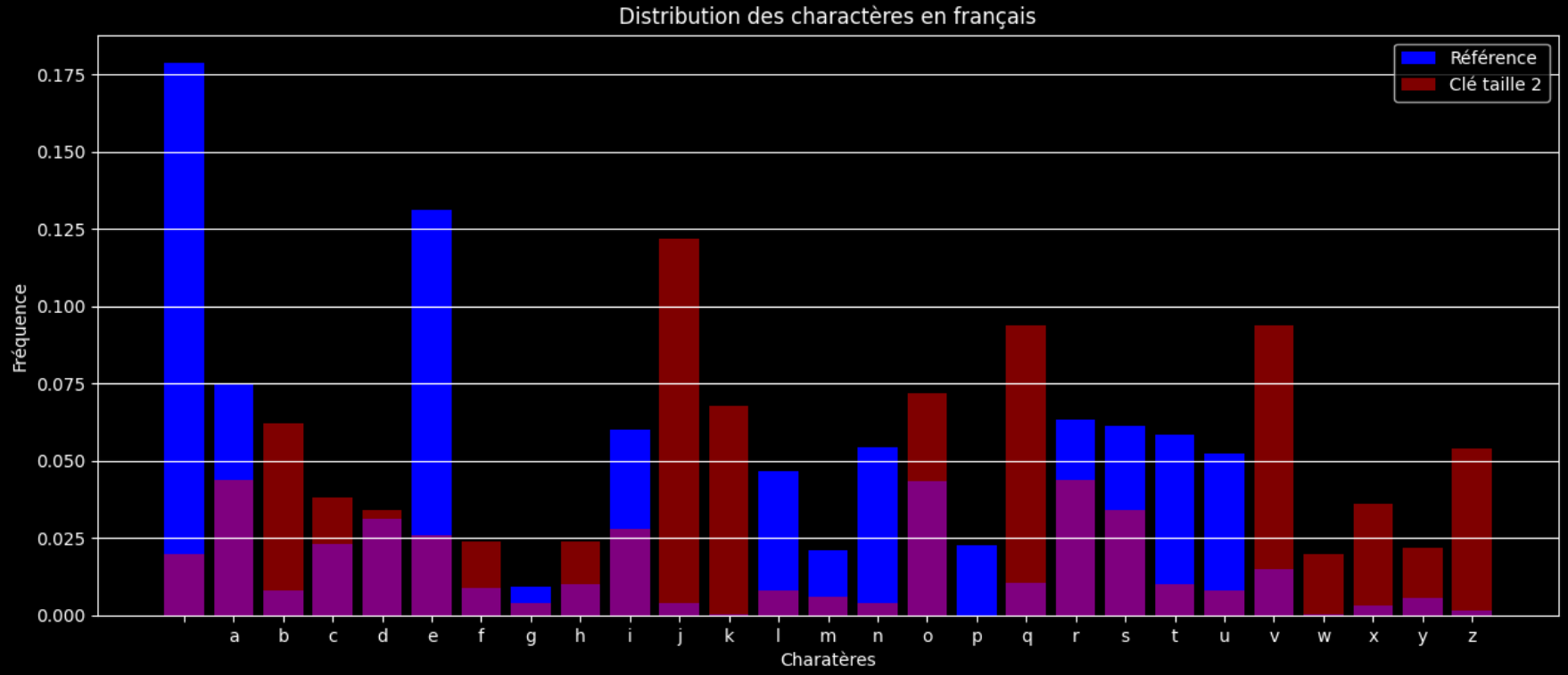
Vigenère : analyse fréquentielle

- **Mot clé de taille 1 (César)**



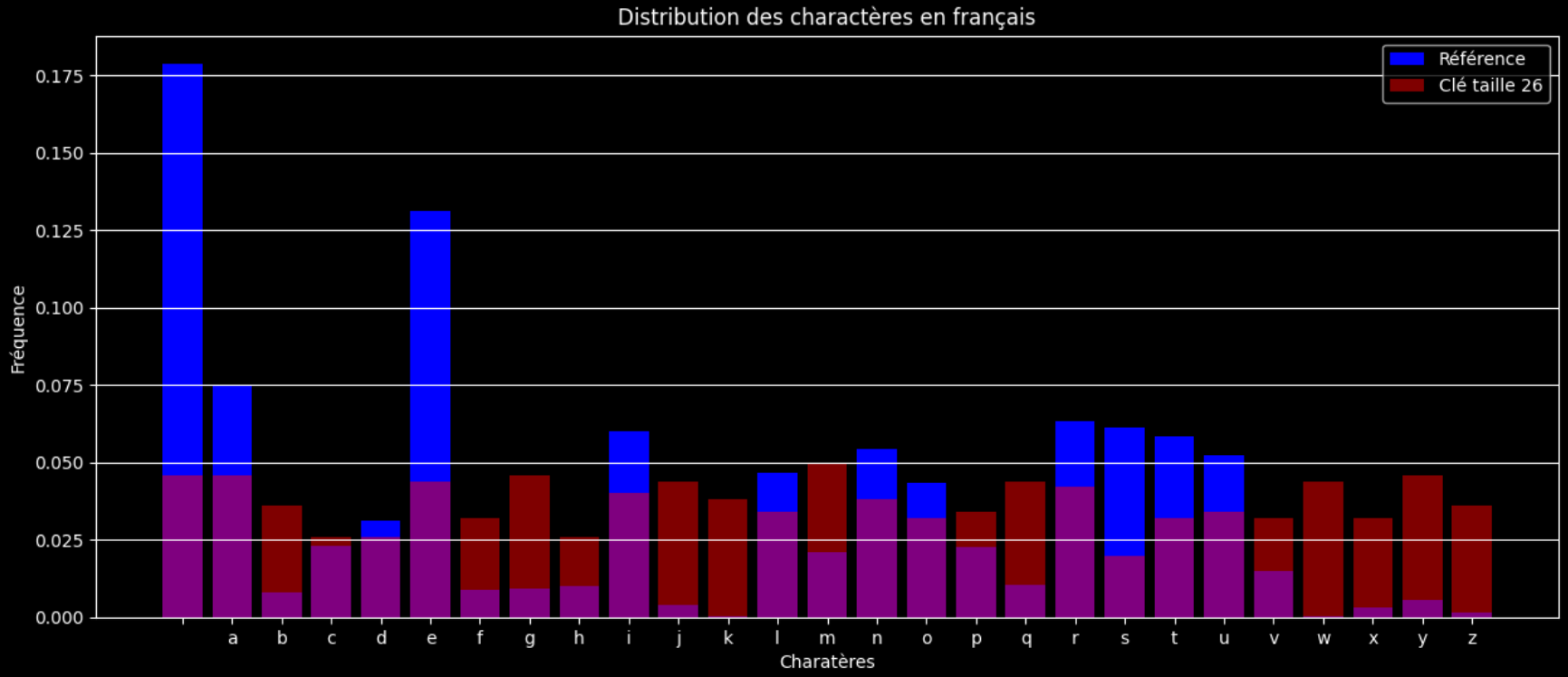
Vigenère : analyse fréquentielle

- **Mot clé de taille 2**



Vigenère : analyse fréquentielle

- **Mot clé de taille 26**



Vigenère : analyse fréquentielle

- **Les chiffrés de Vigenère sont plus aléatoires**
  - La distribution des lettres se rapproche de la distribution uniforme

Vigenère : analyse fréquentielle

- **Les chiffrés de Vigenère sont plus aléatoires**
  - La distribution des lettres se rapproche de la distribution uniforme
- **Comment mesure-t-on l'aléatoire d'un chiffré ?**

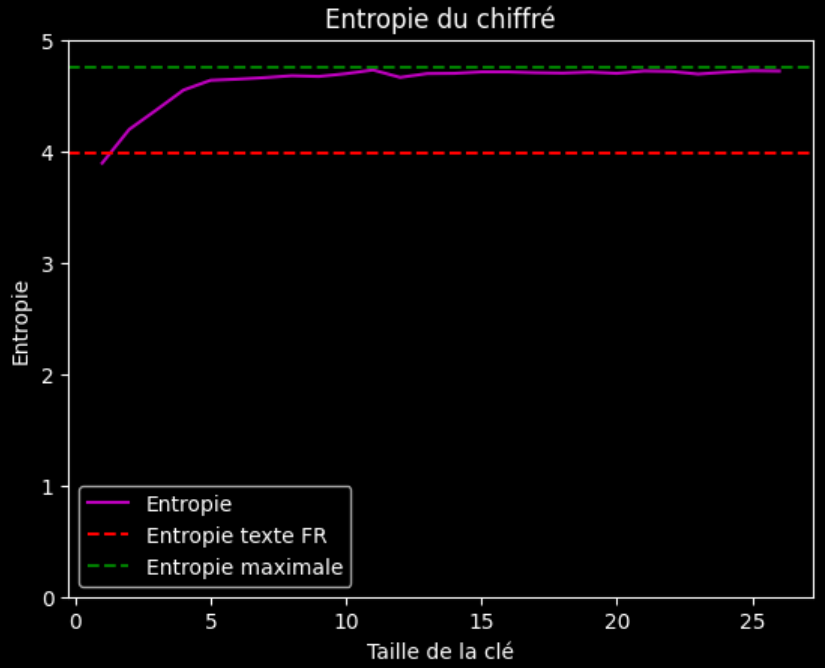
Vigenère : analyse fréquentielle

- **Les chiffrés de Vigenère sont plus aléatoires**
  - La distribution des lettres se rapproche de la distribution uniforme
- **Comment mesure-t-on l'aléatoire d'un chiffré ? L'entropie**

$$H(X) = -\sum_{c \in Alphabet} p(X = c)\log_2(p(X = c))$$

Vigenère : analyse fréquentielle

- **Les chiffrés de Vigenère sont plus aléatoires**
  - La distribution des lettres se rapproche de la distribution uniforme
- **Comment mesure-t-on l'aléatoire d'un chiffré ? L'entropie**



Cryptanalyse Vigenère : indice de coïncidence

- **C’est un indice caractéristique de chaque langue basé sur la fréquence des lettres**

$$IC = \sum_{c \in Alphabet} \frac{n_c(n_c - 1)}{n(n-1)}$$

n_c **: Nombre de *c* dans le texte**
n **: Nombre total de lettres dans le texte**

Cryptanalyse Vigenère : indice de coïncidence

- **C’est un indice caractéristique de chaque langue basé sur la fréquence des lettres**

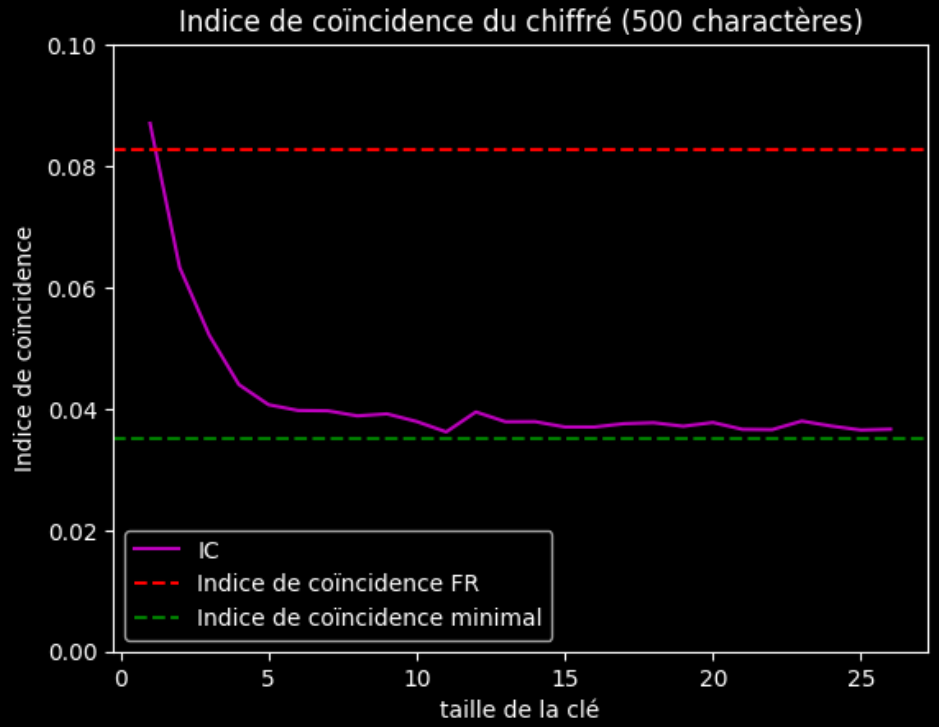
$$IC = \sum_{c \in Alphabet} \frac{n_c(n_c - 1)}{n(n-1)}$$

n_c **: Nombre de *c* dans le texte**
n **: Nombre total de lettres dans le texte**

- **En français (sans ‘ ‘) l’indice vaut environ 0,0746, en anglais 0,067, …**

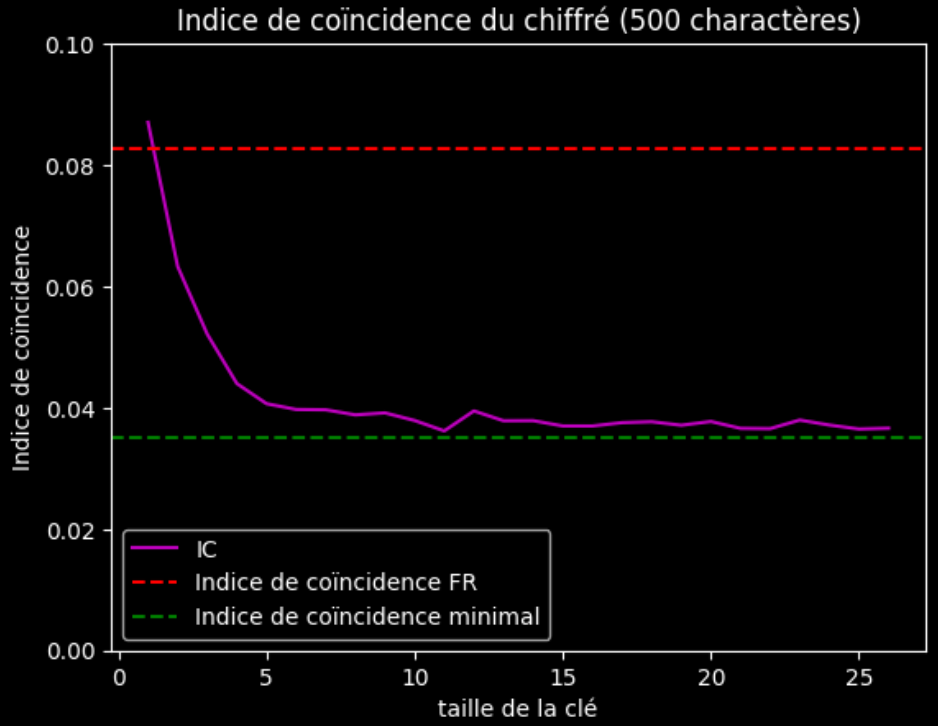
Cryptanalyse Vigenère : indice de coïncidence

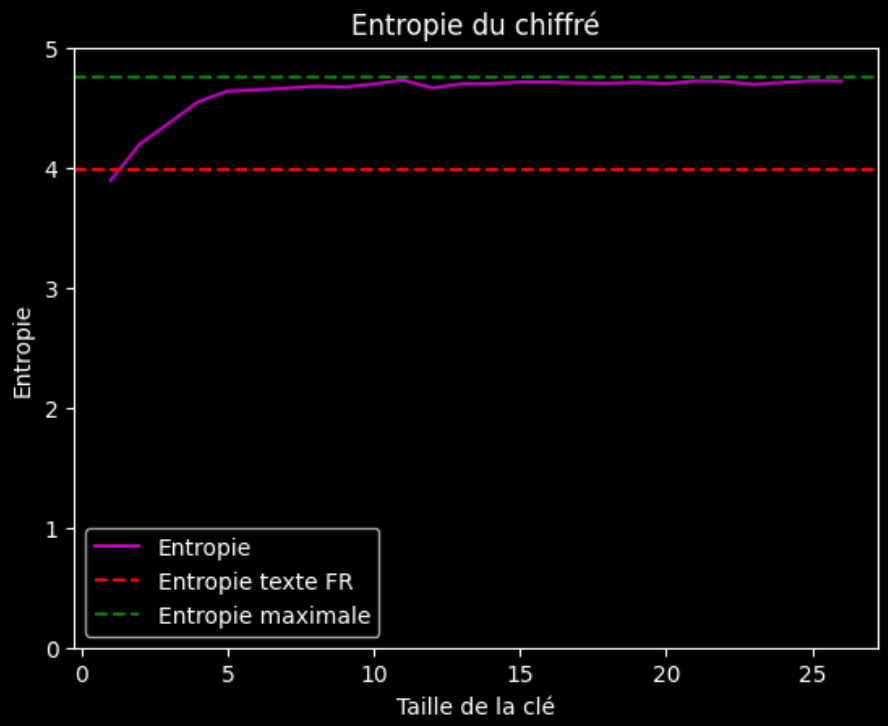
- **C’est un indice caractéristique de chaque langue basé sur la fréquence des lettres**



Cryptanalyse Vigenère : indice de coïncidence

- **C’est un indice caractéristique de chaque langue basé sur la fréquence des lettres**





Cryptanalyse Vigenère : indice de coïncidence

- **Etapes pour décrypter un chiffré de Vigenère :**

1. Trouver la taille du mot clé
2. Trouver le mot clé

Cryptanalyse Vigenère : indice de coïncidence

- **Etapes pour décrypter un chiffré de Vigenère :**

1. Trouver la taille du mot clé
   i. Pour chaque taille de clé possible calculer l'indice de coïncidence
   ii. Si l'indice de coïncidence est proche de celui de référence -> longueur trouvée

Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 2**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

aayqdxzstahplanmgkfswqhelxk xkmkwljuewkujkeakqewqjeqxdamolx lhpltxcsclgdlvdusylxduxmfatfspdmtzxwllpxslmldmktlt
dayqdkmtdbxuoaldbkqdtmtcvetlayrakuxffspampltkyzycvxufulxbsxdldimmkthdqwylxwgxzltblmklxolxkmxdcmcetwdntltcfst
jxsipqspdakfstvslmk dhbfekqxuf

gqrzgigpdokvabvlpwegpnqvzurgtqwbicqinwpigiovrnclhgw pdsbigowotwfbisgx
tingegwizevqbszousudbxignisbpsozwbvaowfbefqdzgwikdhbiexmngrnwdikdocwegdovpebsfpdbxccumokinqfsbizbieviwbdnpgokvncwzbm
ebyvtbdkectyfutepdsumnbinqvrpdaovwbewwdgldouusudspzwbenghncqebee

Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 2**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

aayqdxzstahplanmgkfswqhelxk xkmkwljuewkujkeakqewqjeqxdamolx lhpltxcsclgdlvdusylxduxmfatfspdmtzxwllpxslmldmktlt
dayqdkmtdbxuoaldbkqdtmtcvetlayrakuxffspampltkyzycvxufulxbsxdldimmkthdqwylxwgxzltblmklxolxkmxdcmcetwdntltcfst
jxsipqspdakfstvslmk dhbfekqxuf

gqrzgigpdokvabvlpwegpnqvzurgtqwbicqinwpigiovrnclhgw pdsbigowotwfbisgx
tingegwizevqbszousudbxignisbpsozwbvaowfbefqdzgwikdhbiexmngrnwdikdocwegdovpebsfpdbxccumokinqfsbizbieviwbdnpgokvncwzbm
ebyvtbdkectyfutepdsumnbinqvrpdaovwbewwdgldouusudspzwbenghncqebee

IC1 = 0.051
IC2 = 0.048

Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 2**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

aayqdxzstahplanmgkfswqhelxk xkmkwljuewkujkeakqewqjeqxdamolx lhpltxcsclgdlvdusylxduxmfatfspdmtzxwllpxslmldmktlt
dayqdkmtdbxuoaldbkqdtmtcvetlayrakuxffspampltkyzycvxufulxbsxdldimmkthdqwylxwgxzltblmklxolxkmxdcmcetwdntltcfst
jxsipqspdakfstvslmk dhbfekqxuf

gqrzgigpdokvabvlpwegpnqvzurgtqwbicqinwpigiovrnclhgw pdsbigowotwfbisgx
tingegwizevqbszousudbxignisbpsozwbvaowfbefqdzgwikdhbiexmngrnwdikdocwegdovpebsfpdbxccumokinqfsbizbieviwbdnpgokvncwzbm
ebyvtbdkectyfutepdsumnbinqvrpdaovwbewwdgldouusudspzwbenghncqebee

IC1 = 0.051 < 0.083
IC2 = 0.048 < 0.083

Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 3**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

aqqgzpaklbmpfgqqlu
tmblqewugevqcqgqpabloltlbcgltlguwleubfofudxznlbxombmolbdqqgmkbboxdgqwmkvclgrvubfpaxluykcqublbsvlbmptkqclbgbltlkltlumpcue
bdqlpfo bswqldufuvpmbdgfcqbf

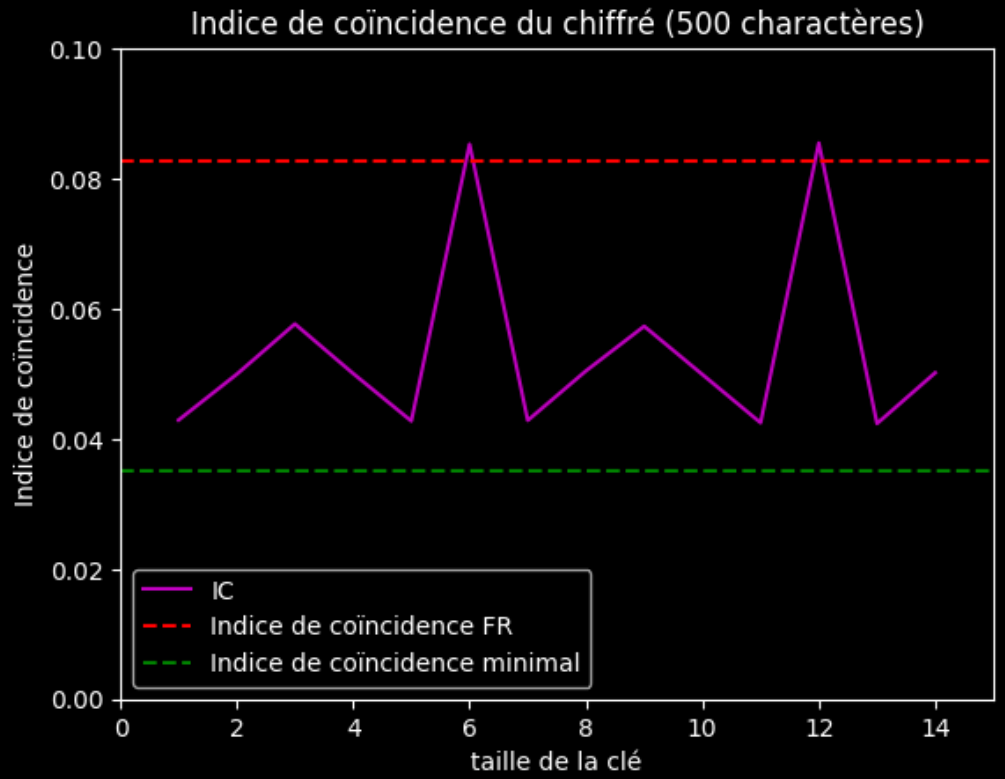
gyzxgtopanlkewnezkgkwwcunkikoknwhe dsog opfxsc dndgyzdqmztspbtgwspslwdatf
fyzkidhuelnknticoteyokeffpbpckoynxsuzbedwinkodnyzwezvbdkcofkedscnwntrcatwxwpgpokstslw nbnkeue

ardisdhvavgwsphvxrxqkijiwpjiareljwxdmixwhwtisxgivesixvxsausdmixilpszlvkwteaddwtdxiambrddtdewadapxssdmctmzivffixixiddmghvww
xmxytbmexyxtxdmmtinvtdsvjeidsdausdszkehheqxe

IC1 = 0.0629 < 0.083
IC2 = 0.0472 < 0.083
IC3 = 0.0606 < 0.083

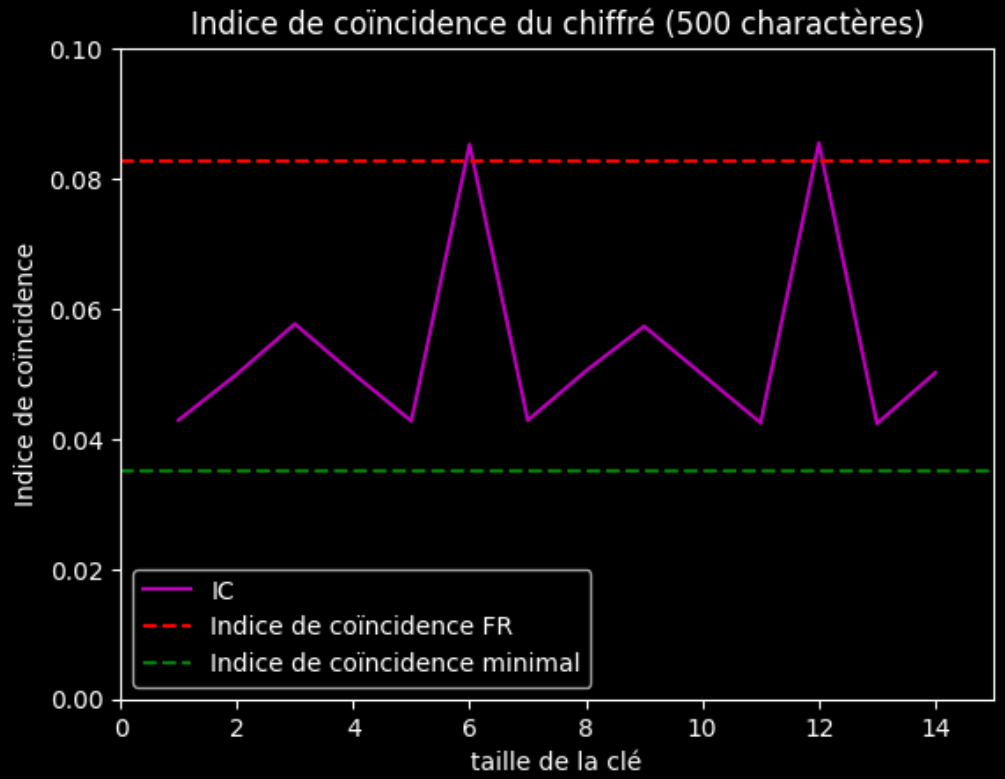
Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé ?**



Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé ? 6**



Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 6**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

6 chiffrés de César

aqzalmfql mleueqqqalllclluluffdzlxmmldqmbodqmvlrufalyculslmtqlglllmcedlf sqdfvmdfqf

gzgoalenzgwcnionh sgofs ngzqzsbgsswaffzihennioeoefbconszewnonzevdcfesnnrawwgosswnnee

adshagshxxkjwjaejxmxhtsgvsxxasmxlslktadtxabdteaaxsmtzvfxxdmhwxxtmxxxmtntsjisasskhex

qgpkbpgqutbqwgvcgpbotbgtgwebouxnbobobqgkbxgwkcgvbpxukqbbvbpkcbbtktupubqpobwluupbgcb

yxtpnkwekkwukkkwedo pxcddydmtptwpldt ykdulktctykfppkyxubdikdywzbkokdcwtctxppktl bku

ridvvwpvrqiipirlwdiwwixieivsudiipzvwedwdimrddwdpsdcmifiiidgvwmybeytdmivdveddudzehqe

Cryptanalyse Vigenère : indice de coïncidence

- **Taille de la clé 6**

agaqyrqzdgxizgsptdaohkpvlaabnvmlgpkwfesgwpqnhqevlzxukr gxtkqmwkbwilcjquienwwkpuijgkieoavkrqnecwlqhjgewq
xpddasmboilgxo wlohtpwlftbxicssgcxl gtdilnvgdeugswyilzxedvuqxbmsfzaotufssupddbmxtizgxnwilslbppxssolzmwlbdvmakotwlftb
edfaqydqzdgkwmitkddbhxbuioeaxlmdnbgkrqndwtdmitkcdvoectwleagydroavkpuexbfsffsppdabmxpclctukmyozkyicnvqxfusfbuilzx
bbisexvdilwdbidmnmpkgtohkdvqnwcywlzxbwmgexbzylvttbbldmkkelcxtoylfxuktmexpddcsmucmentbwidnnqtvlrtpcdfasotv
wjbxeswiwpdqgslpddoaukufssutdvssplzmwkb ednhgbhfneckqqexbuefe

6 chiffrés de César

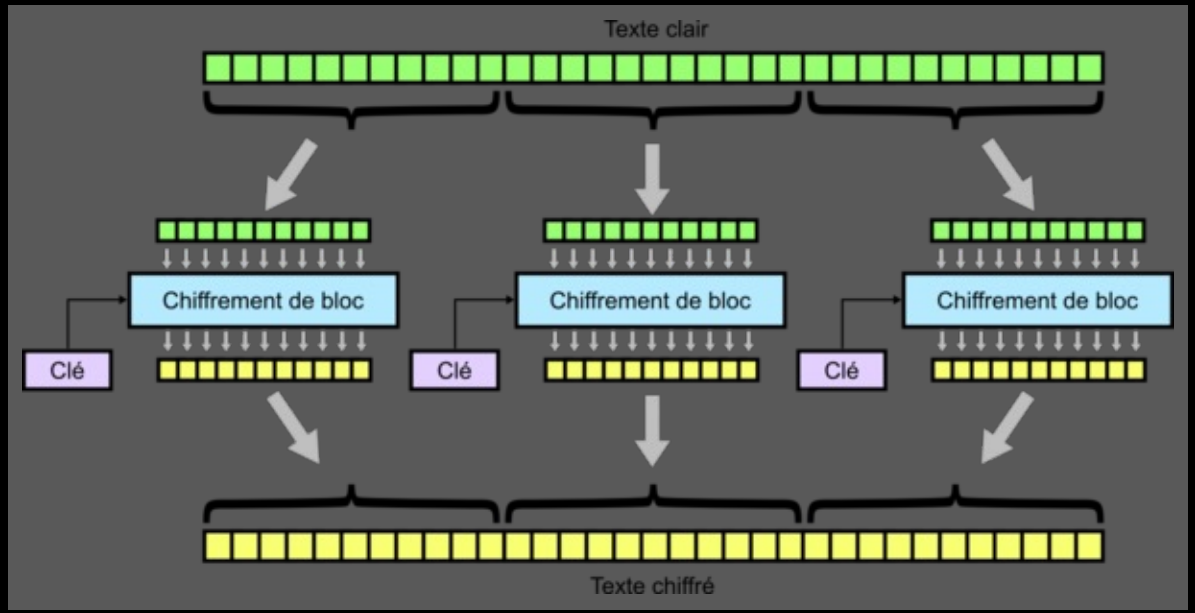
aqzalmfql mleueqqqalllclluluffdzlxmmldqmbodqmvlrufalyculslmtqlglllmcedlf sqdfvmdfqf	M
gzgoalenzgwcnionh sgofs ngzqzsbgsswaffzihennioeoefbconszewnonzevdcfesnnrawwgosswnnee	O
adshagshxxkjwjaejxmxhtsgvsxxasmxlslktadtxabdteaaxsmtzvfxxdmhwxxtmxxxmtntsjisasskhex	T
qgpkbpgqutbqwgvcgpbotbgtgwebouxnbobobqgkbxgwkcgvbpxukqbbvbpkcbbtktupubqpobwluupbgcb	C
yxtpnkwekkwukkkwedo pxcddydmtptwpldt ykdulktctykfppkyxubdikdywzbkokdcwtctxppktl bku	L
ridvvwpvrqiipirlwdiwwixieivsudiipzvwedwdimrddwdpsdcmifiiidgvwmybeytdmivdveddudzehqe	E

Epoque moderne

- On considère deux grande familles de schémas de chiffrement
- Ceux qui chiffrent le message lettre par lettre (ou bit à bit) : chiffrement par flot
- Ceux qui chiffrent le message par bloc de lettres (ou bloc de bits) : chiffrement par bloc

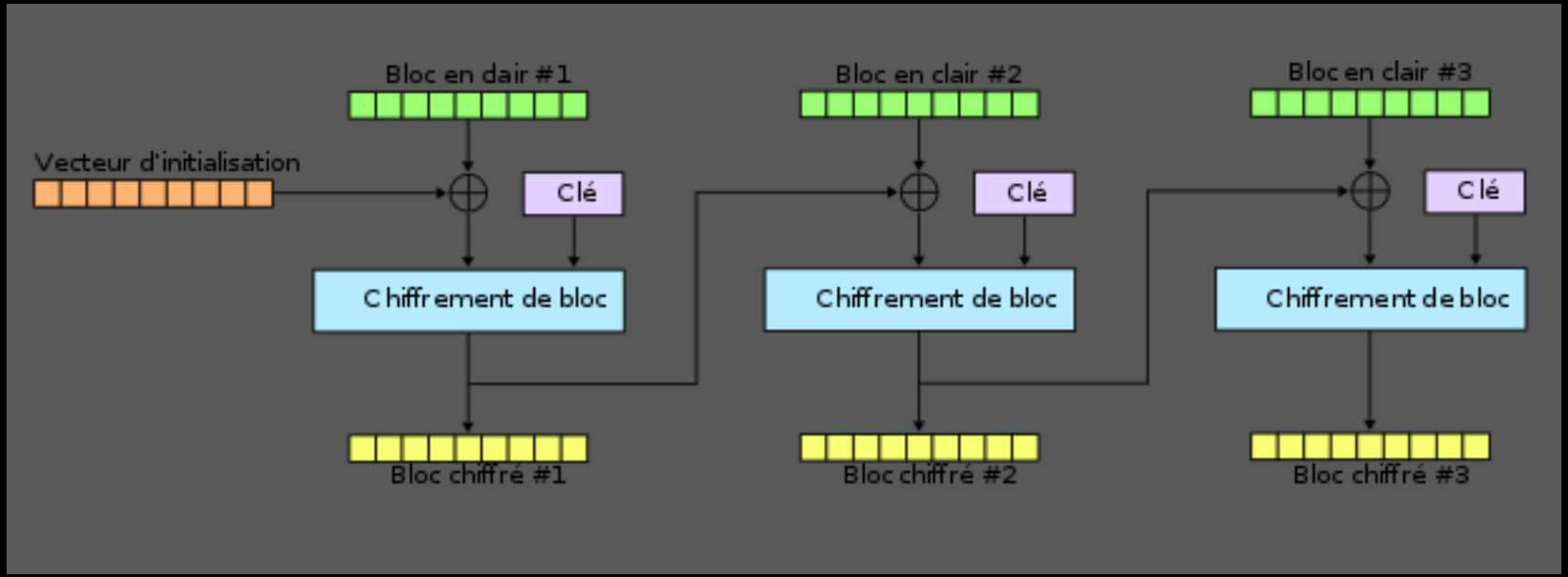
Chiffrement par blocs : différents traitements

- Combiner les blocs (chaînage) améliore la sécurité
- Mode ECB (Electronic Code Book)



Chiffrement par blocs : mode CBC

- **Model CBC (Cipher Block Chaining)**



Chiffrement par blocs : mode OFB

- **Model CBC (Output Feed Back)**

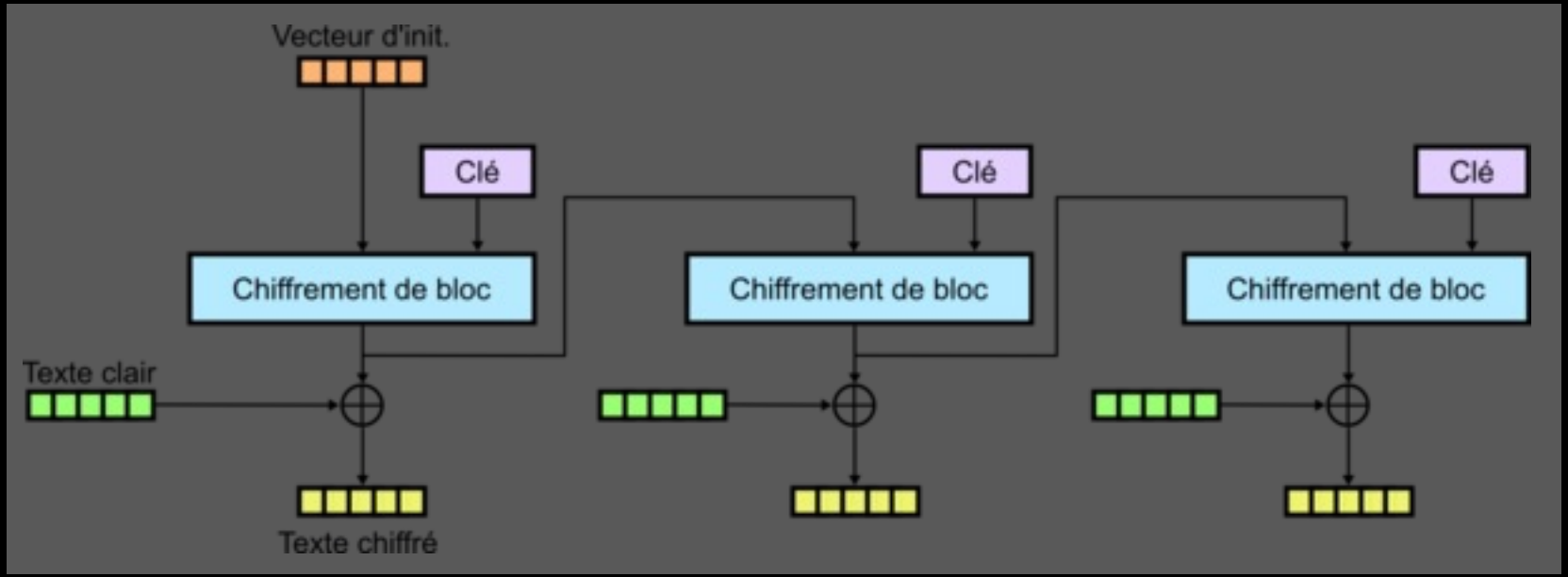
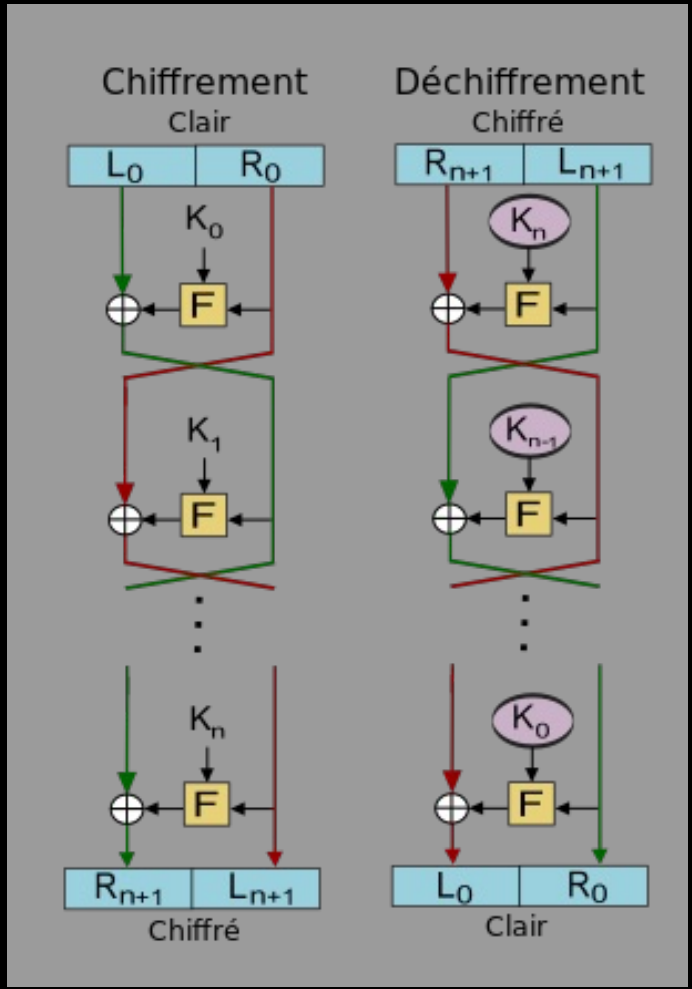


Schéma de Feistel :

- **Schéma souvent utilisé :**



Exemple de schéma de Feistel : D.E.S

- **Data Encryption Standard (D.E.S)**

- **Standard de chiffrement en 1975**
  - Complètement cassé de nos jours

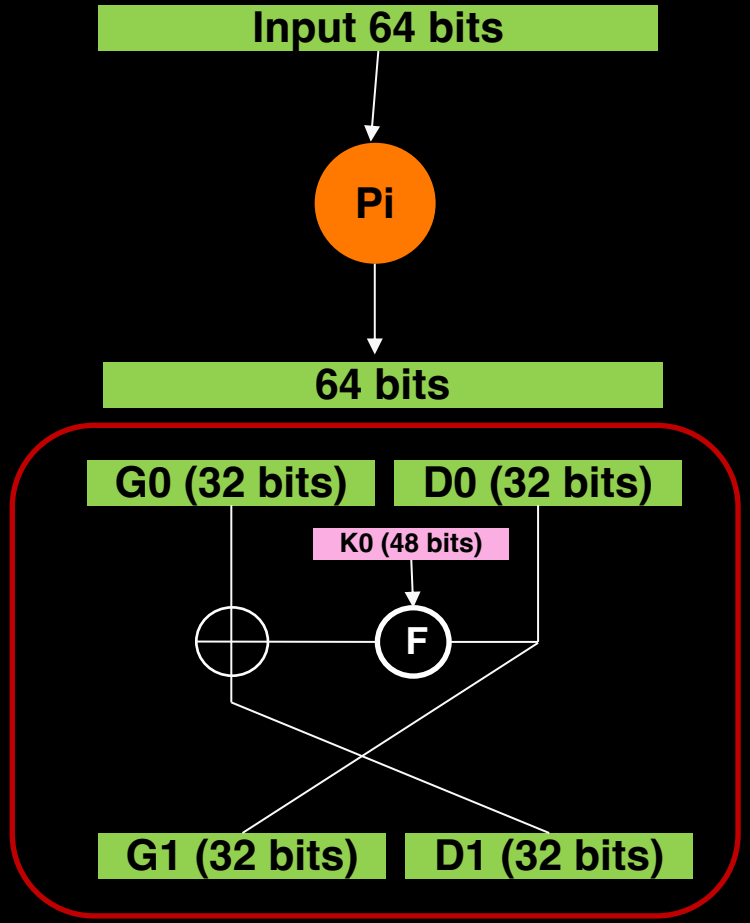
Exemple de schéma de Feistel : D.E.S

- **Data Encryption Standard (D.E.S)**
- **Standard de chiffrement en 1975**
  - Complètement cassé de nos jours
- **Taille des blocs : 64 bits**
- **Taille des clés : 48 bits**
  - Clés dérivée d'une clé maître K de 64 bits
  - K contient des bits de parité -> détection d'erreur lors de la transmission ou stockage

Exemple de schéma de Feistel : D.E.S

- **Combine plusieurs type d'opérations:**
  - Permutations : scytales
  - Substitutions : César, Vigenère, …

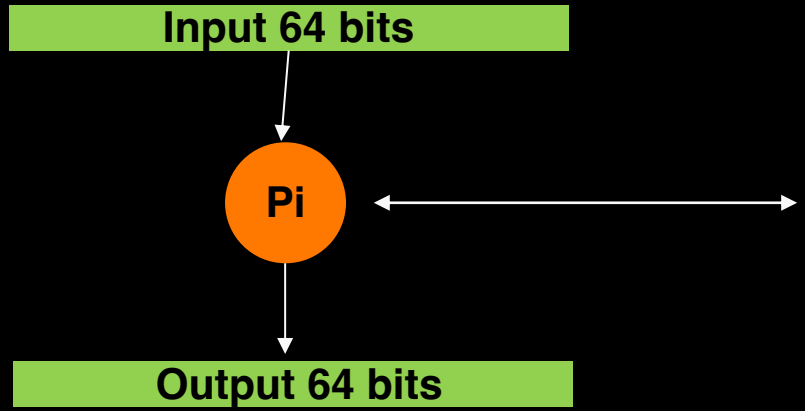
Exemple de schéma de Feistel : D.E.S



1 tour

16 tours au total

D.E.S. : Permutation initiale

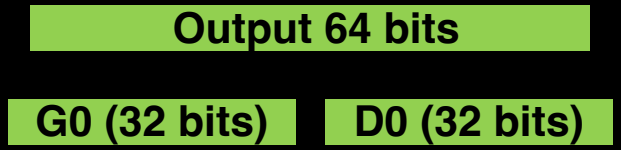


58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

« Matrice » de permutation Pi

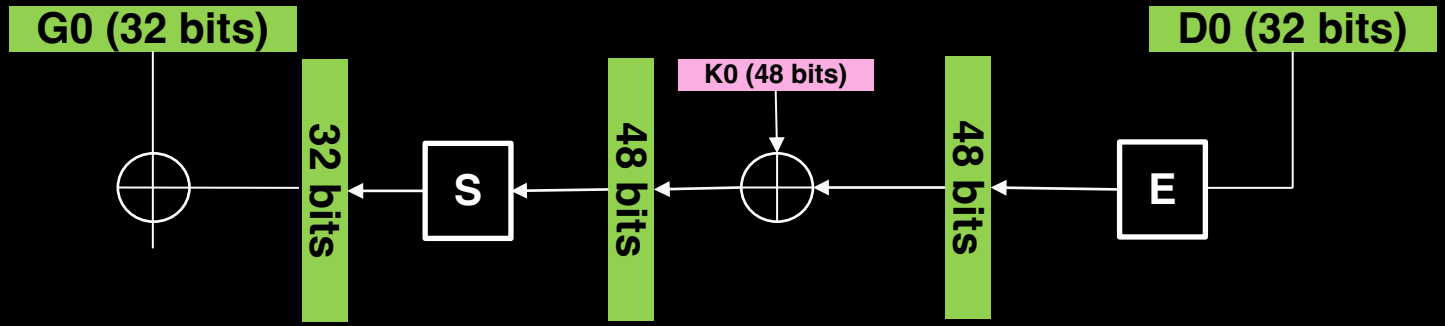
- **bit 1 de output = bit 58 de input**
- **bit 2 de output = bit 50 de input**
- **…**

D.E.S. : tour étape 1

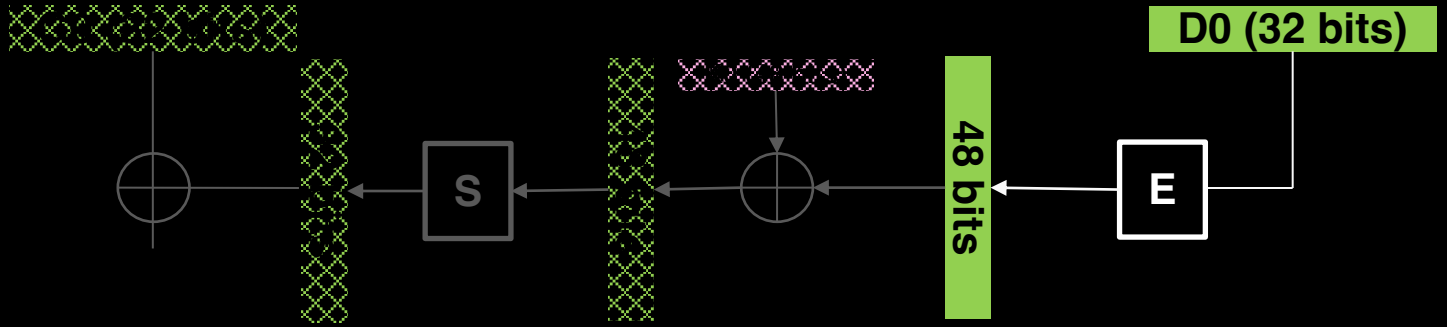


- On coupe en deux blocs de 32 bits

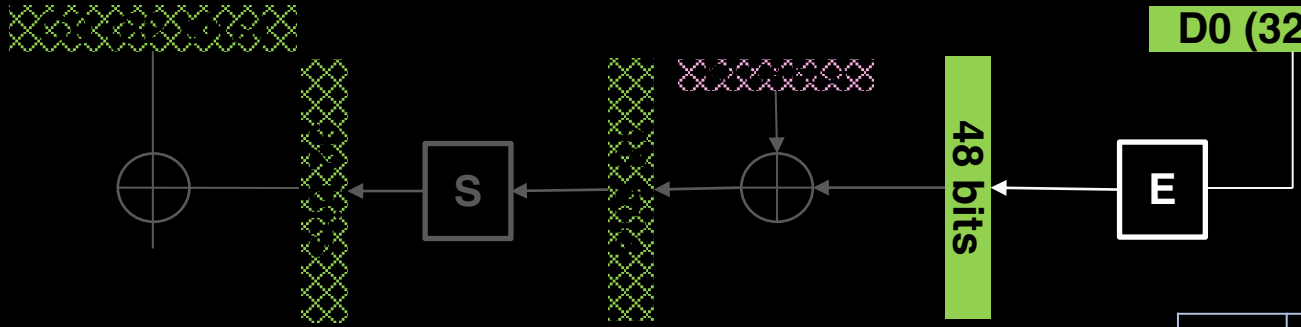
D.E.S. : tour étape 2



D.E.S. : tour étape 2



D.E.S. : tour étape 2

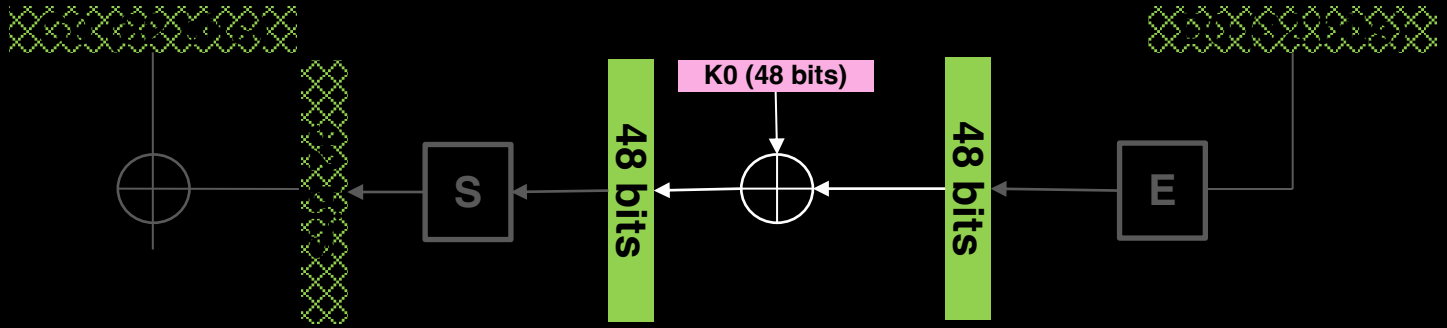


« Matrice » de permutation pour la fonction d'expansion E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

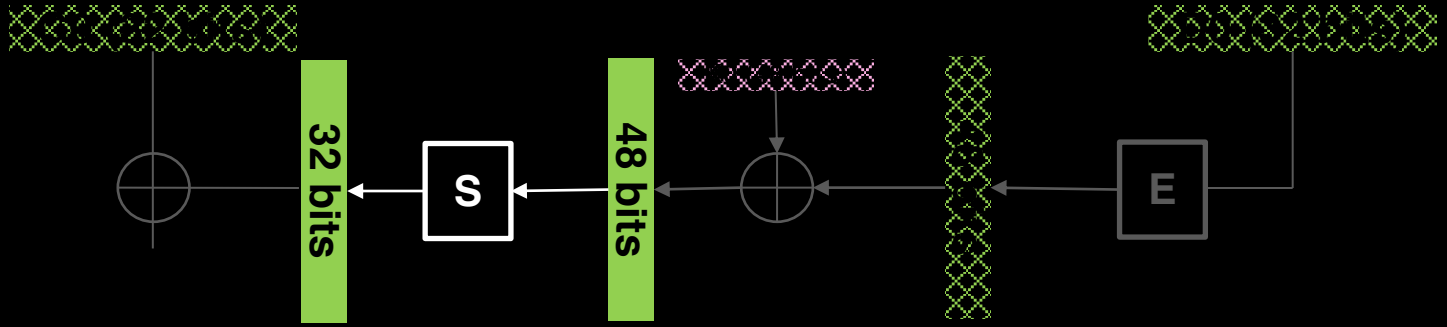
- bit 1 de output = bit 32 de D0
- bit 2 de output = bit 1 de D0
- …

D.E.S. : tour étape 2

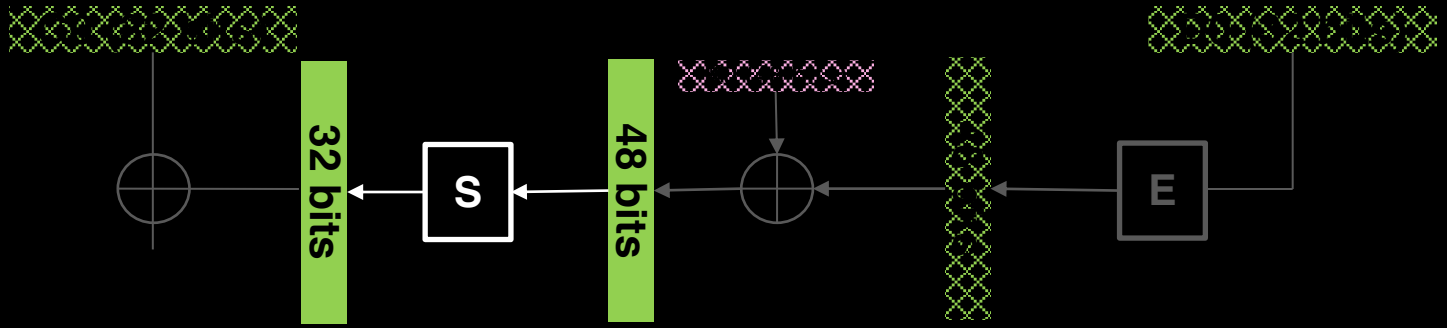


- XOR bit à bit entre la clé K0 et le vecteur en output de E

D.E.S. : tour étape 2

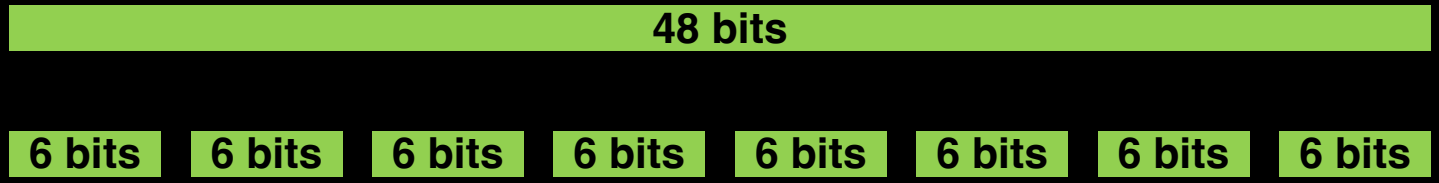


D.E.S. : tour étape 2

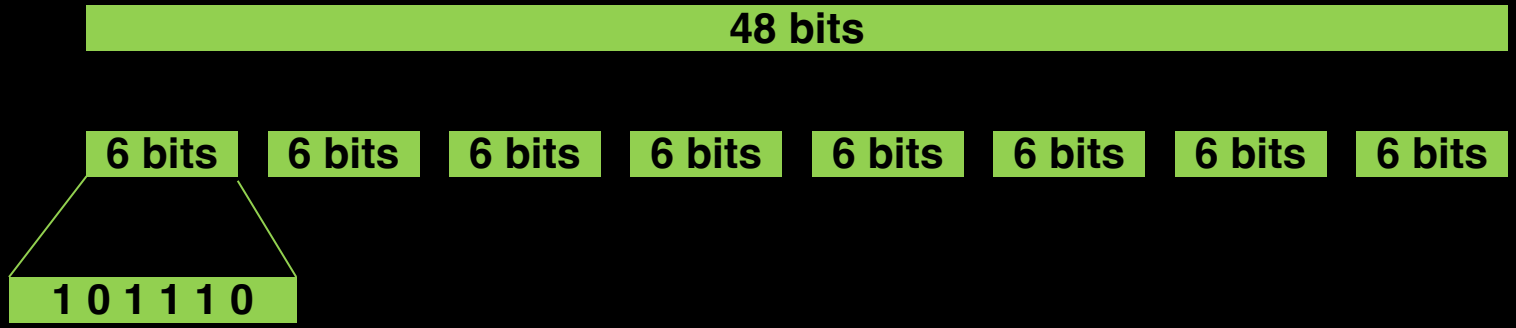


- **Fonction S:**
  - Découpe le vecteur en 8 blocs de 6bits
  - Réduit en 8 blocs de 4 bits par substitution
  - Permute le vecteur de 32 bits

D.E.S. : tour étape 2



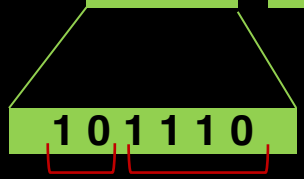
D.E.S. : tour étape 2



D.E.S. : tour étape 2

48 bits

6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

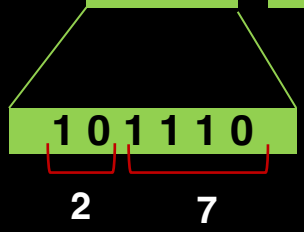
Tableau de substitution S1

- bits 1 et 2 -> n° de ligne
- bits 3, 4, 5, 6 -> n° de colonne

D.E.S. : tour étape 2

48 bits

6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

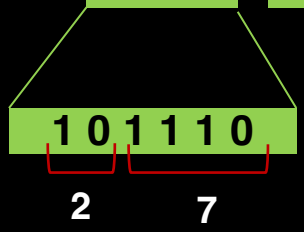
Tableau de substitution S1

- bits 1 et 2 -> n° de ligne
- bits 3, 4, 5, 6 -> n° de colonne

D.E.S. : tour étape 2

48 bits

6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

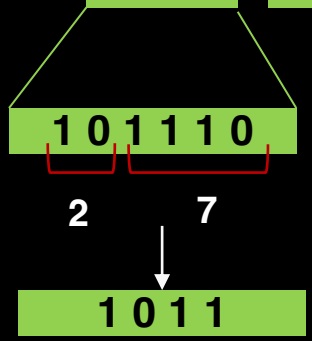
Tableau de substitution S1

- bits 1 et 2 -> n° de ligne
- bits 3, 4, 5, 6 -> n° de colonne

D.E.S. : tour étape 2

48 bits

6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits | 6 bits

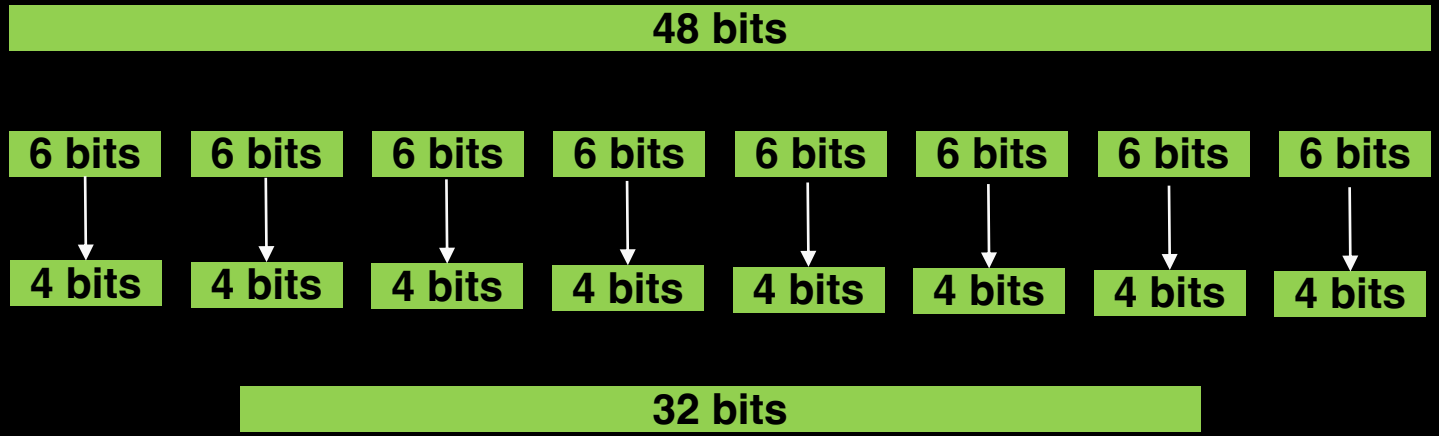


	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tableau de substitution S1

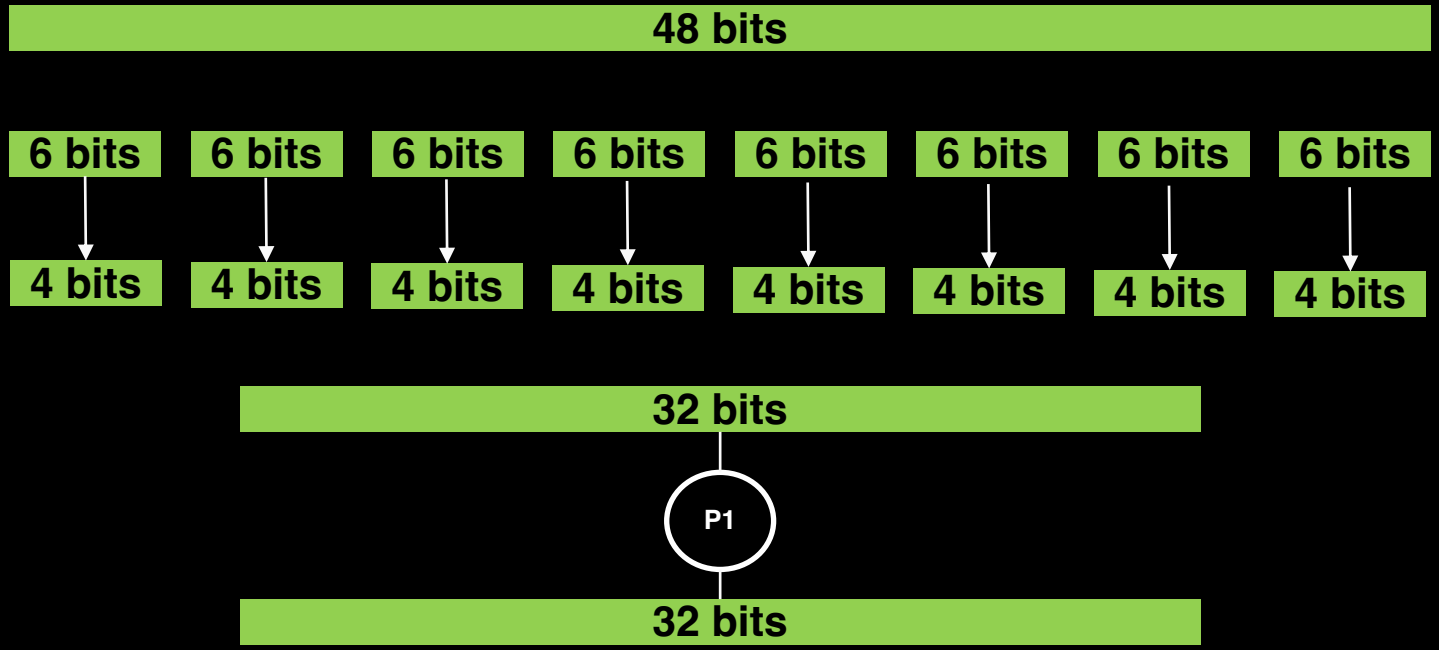
- bits 1 et 2 -> n° de ligne
- bits 3, 4, 5, 6 -> n° de colonne
- On remplace le bloc par la valeur du tableau

D.E.S. : tour étape 2



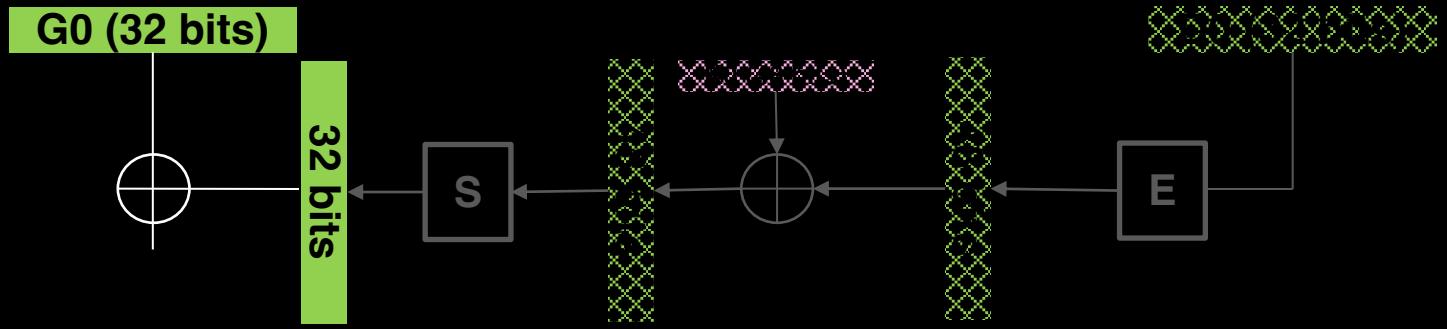
- **On applique la substitution à chaque bloc**
  - Le tableau est différent pour chaque bloc, 8 tableaux aux total

D.E.S. : tour étape 2



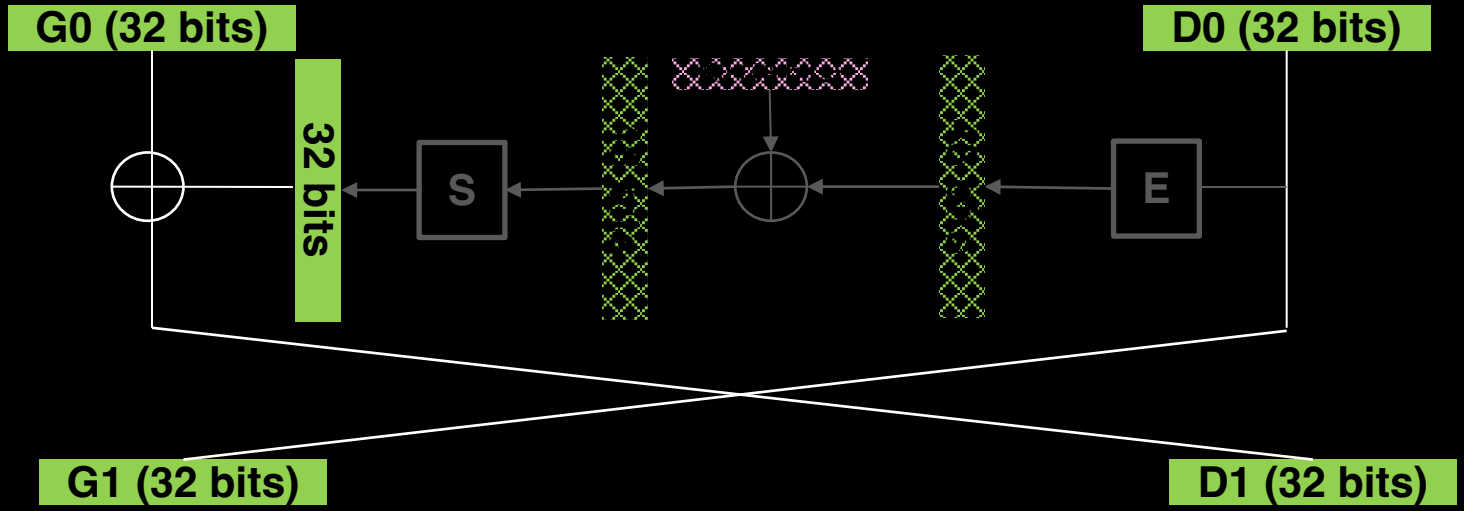
- **On applique la substitution à chaque bloc**
  - Le tableau est différent pour chaque bloc, 8 tableaux aux total
- **On permute le vecteur de 32 bits**

D.E.S. : tour étape 3



- **XOR bit à bit entre les deux vecteurs**

D.E.S. : tour étape 3



- On recommence 1 nouveau tour

D.E.S.

- Les matrices de permutations sont nommées P-box
- Les tableaux de substitutions sont nommées S-box
- Les permutations et substitutions sont toujours inversibles, sinon pas de déchiffrement

D.E.S.

- **Les matrices de permutations sont nommées P-box**
- **Les tableaux de substitutions sont nommées S-box**
- **Les permutations et substitutions sont toujours inversibles, sinon pas de déchiffrement**
- **Pour déchiffrer**
  - Refaire l'algo en commençant avec K15 au premier tour jusqu'à K0 au dernier tour
- **Attention ! D.E.S est complètement cassé, ne pas utiliser en production**

Sécurité parfaite

- **Un chiffrement est difficile à casser lorsque la connaissance du chiffré C n'apporte aucune information sur le clair M**

- **En théorie de l'information on a deux grands principes:**
  - Principe de confusion : la relation entre la clé et le chiffré doit être la plus complexe possible
  - Principe de diffusion : la dépendance entre les bits de sorties et les bits d'entrées doit être minimales

- **La combinaison de substitutions et de permutations est conforme à ces principes**