Manuel de cryptanalyse à l'usage de la NSA

Sylvain Perifel

Université Paris Cité

Fête de la science

Le 14 octobre 2022

Bravo !

Vous venez d'être recruté par la NSA !

La NSA

- National Security Agency
- Création 1952 (Maryland)
- Mission :
  renseignement d'origine électromagnétique
  (cf. réseau Echelon)
- Budget annuel : 10 milliards de dollars
- 22 000 employés

Vos missions (que vous les acceptiez ou non)

- Surveiller ces dangereux citoyens
- Espionner ces dangereux pays
- Communiquer dans le monde hostile

1. Formation accélérée

2. Surveiller ces dangereux citoyens

3. Espionner ces dangereux pays

4. Communiquer dans le monde hostile

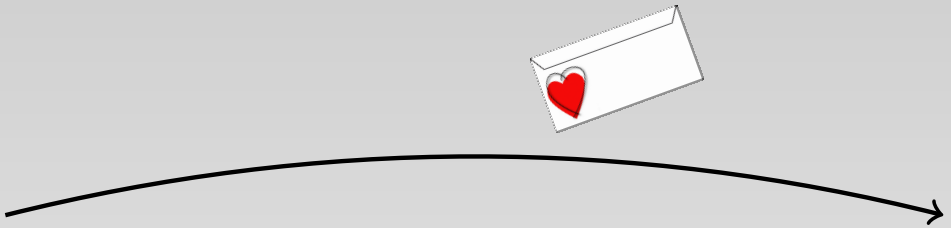
Cryptologie

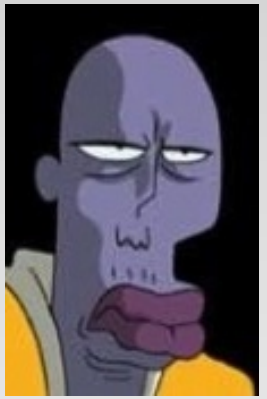
Cryptologie : science des codes secrets

Cryptologie

Cryptologie : science des codes secrets

Cryptographie : coder un message
que seul le destinataire puisse déchiffrer

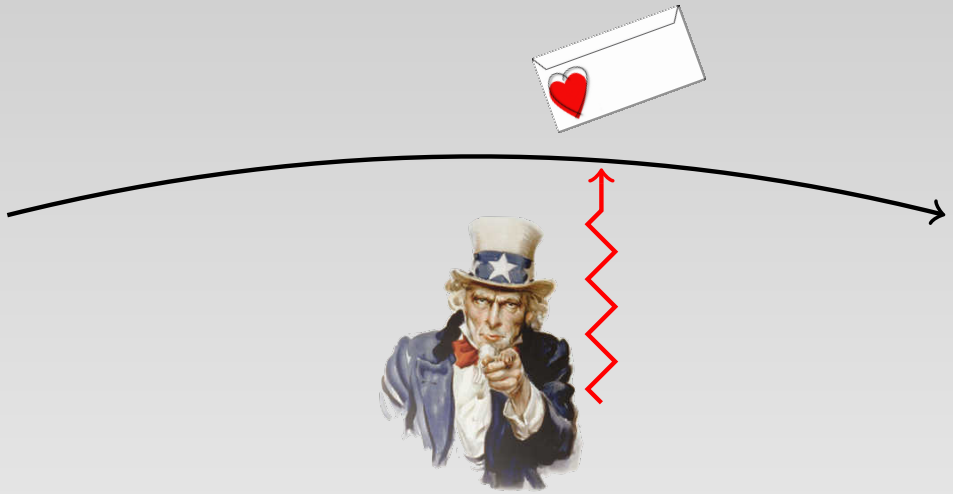




Cryptologie

Cryptologie : science des codes secrets

Cryptographie : coder un message
que seul le destinataire puisse déchiffrer



Cryptanalyse : « casser » un code secret
Trouver comment déchiffrer les messages

Motivation

- Depuis toujours, des besoins de confidentialité :
  - secrets d'États,
  - pendant les guerres, etc.

Motivation

- Depuis toujours, des besoins de confidentialité :
  - secrets d'États,
  - pendant les guerres, etc.
- Premiers codes secrets simplistes il y a plus de 2000 ans

Motivation

- Depuis toujours, des besoins de confidentialité :
  - secrets d'États,
  - pendant les guerres, etc.
- Premiers codes secrets simplistes il y a plus de 2000 ans
- Actuellement, des millions de transactions sur ordinateur
  - codes sophistiqués,
  - apparition du quantique…

1. Formation accélérée

2. Surveiller ces dangereux citoyens

3. Espionner ces dangereux pays

4. Communiquer dans le monde hostile

Une interception !

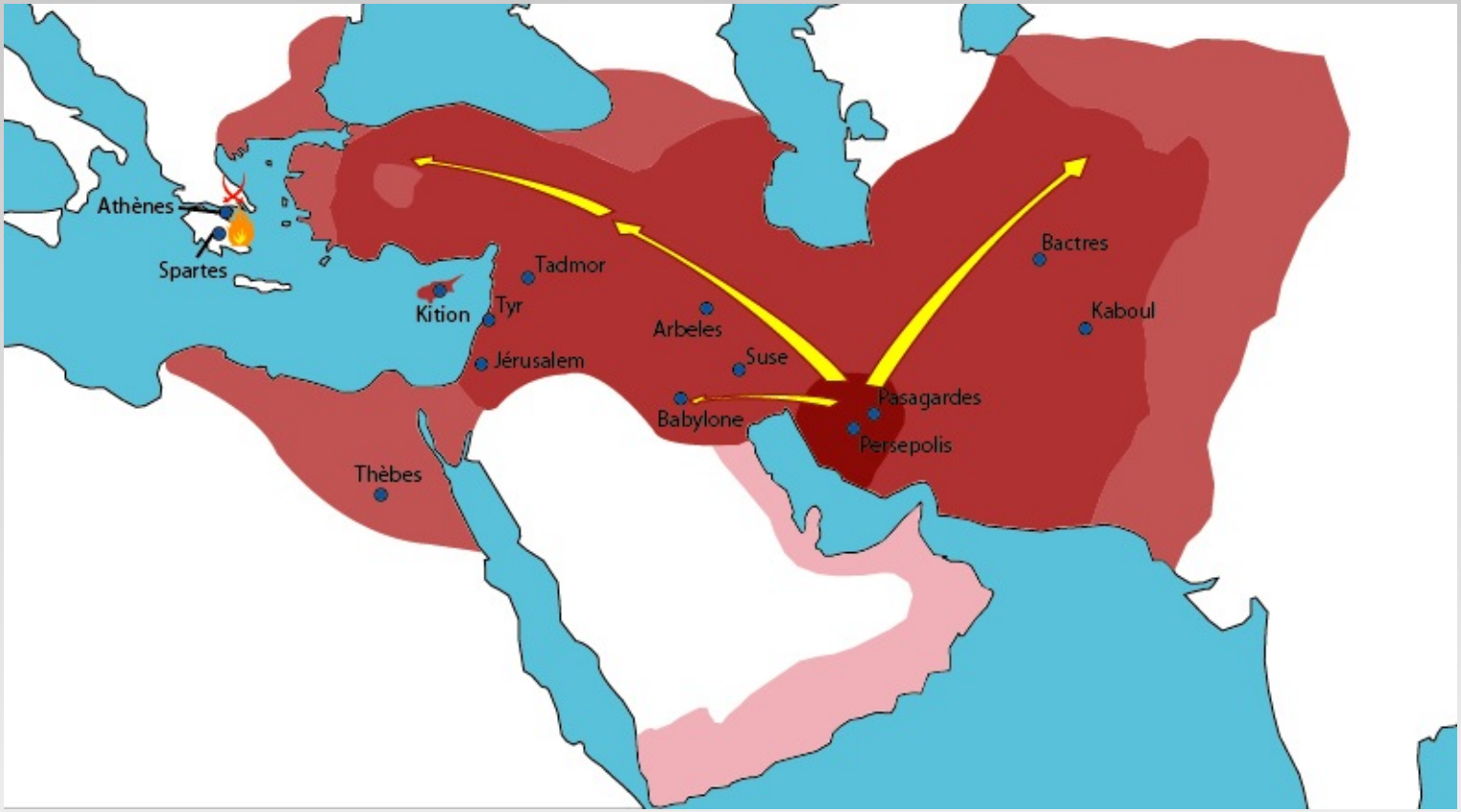
Un dangereux citoyen portait ce message sur lui !

S L C A D I E E F N E L C T A E E

Que pouvait-il bien vouloir dire à nos ennemis ?

Premier pas

- Vers 400 av. J.-C. : attaque de Sparte par les Perses



Premier pas

- Vers 400 av. J.-C. : attaque de Sparte par les Perses
- Un messager parvient à prévenir Sparte avec une scytale

Premier pas

- Vers 400 av. J.-C. : attaque de Sparte par les Perses
- Un messager parvient à prévenir Sparte avec une scytale

- Sparte repousse l’attaque

Un autre message !

On a intercepté la réponse au message précédent !

KFFPAK CK MVXXPAQJK RK EKFFPZK

(Heureusement le dangereux citoyen a été jeté en prison)

Vite, qu'est-ce que ça peut vouloir dire ?

Deuxième pas

- Jules César utilisait de nombreux codes
- P. ex. remplacer une lettre par la lettre venant trois places après elle dans l'alphabet :

a	b	c	…	w	x	y	z
D	E	F	…	Z	A	B	C

Deuxième pas

- Jules César utilisait de nombreux codes
- P. ex. remplacer une lettre par la lettre venant trois places après elle dans l'alphabet :

a	b	c	…	w	x	y	z
D	E	F	…	Z	A	B	C

Exemple :

v	e	n	i		v	i	d	i		v	i	c	i
Y	H	Q	L		Y	L	G	L		Y	L	F	L

Deuxième pas

- Jules César utilisait de nombreux codes
- P. ex. remplacer une lettre par la lettre venant trois places après elle dans l'alphabet :

a	b	c	…	w	x	y	z
D	E	F	…	Z	A	B	C

- Si on identifie $\begin{cases} \text{les lettres} & \text{a} & \text{b} & \text{c} & \ldots & \text{z} \\ \text{aux nombres} & 0 & 1 & 2 & \ldots & 25, \end{cases}$

alors il suffit d'ajouter 3 à chaque lettre pour chiffrer le message, en revenant à 0 si on dépasse 25 (on compte *modulo* 26)

Deuxième pas

- Jules César utilisait de nombreux codes
- P. ex. remplacer une lettre par la lettre venant trois places après elle dans l'alphabet :

a	b	c	…	w	x	y	z
D	E	F	…	Z	A	B	C

- Si on identifie $\begin{cases} \text{les lettres} & \text{a} & \text{b} & \text{c} & \ldots & \text{z} \\ \text{aux nombres} & 0 & 1 & 2 & \ldots & 25, \end{cases}$

  alors il suffit d'ajouter 3 à chaque lettre pour chiffrer le message, en revenant à 0 si on dépasse 25 (on compte *modulo* 26)
- Pour décoder, on retranche 3 à chaque lettre

Substitution mono-alphabétique

- Code de César : plutôt que d'ajouter 3, on peut ajouter n'importe quel nombre entre 1 et 25
- Clé : l'entier de décalage (3 ou autre) $\rightarrow$ 25 clés possibles
- Avec la clé, on peut coder et décoder : l'expéditeur et le destinataire doivent connaître la clé.

Substitution mono-alphabétique

- Code de César : plutôt que d'ajouter 3, on peut ajouter n'importe quel nombre entre 1 et 25
- Clé : l'entier de décalage (3 ou autre) $\rightarrow$ 25 clés possibles
- Avec la clé, on peut coder et décoder : l'expéditeur et le destinataire doivent connaître la clé.

Si, plutôt que de décaler d'un pas fixé, on réalise une permutation quelconque des lettres

Par exemple	a	b	c	d	e	…	w	x	y	z
	M	E	B	T	A	…	C	S	U	Q

Substitution mono-alphabétique

- Code de César : plutôt que d'ajouter 3, on peut ajouter n'importe quel nombre entre 1 et 25
- Clé : l'entier de décalage (3 ou autre) $\rightarrow$ 25 clés possibles
- Avec la clé, on peut coder et décoder : l'expéditeur et le destinataire doivent connaître la clé.

Si, plutôt que de décaler d'un pas fixé, on réalise une permutation quelconque des lettres

alors il y a $26 \times 25 \times 24 \times \cdots \times 2 \times 1$ clés possibles (factorielle de 26), soit $\simeq 4.10^{26} = 400\,000\,000\,000\,000\,000\,000\,000\,000$

Substitution mono-alphabétique

- Code de César : plutôt que d'ajouter 3, on peut ajouter n'importe quel nombre entre 1 et 25
- Clé : l'entier de décalage (3 ou autre) $\rightarrow$ 25 clés possibles
- Avec la clé, on peut coder et décoder : l'expéditeur et le destinataire doivent connaître la clé.

Si, plutôt que de décaler d'un pas fixé, on réalise une permutation quelconque des lettres

alors il y a $26 \times 25 \times 24 \times \cdots \times 2 \times 1$ clés possibles (factorielle de 26), soit $\simeq 4.10^{26} = 400\,000\,000\,000\,000\,000\,000\,000\,000$

Pour échanger des messages, il suffit de connaître la permutation des lettres (l'alphabet chiffré).

Le code mono-alphabétique en pratique

- Alice et Bob doivent se rencontrer physiquement pour s'accorder sur la permutation des lettres (l'alphabet chiffré)
  $\rightarrow$ ils apprennent l'alphabet chiffré par cœur.

a	b	c	d	e	…	w	x	y	z
M	E	B	T	A	…	C	S	U	Q

Le code mono-alphabétique en pratique

- Alice et Bob doivent se rencontrer physiquement pour s'accorder sur la permutation des lettres (l'alphabet chiffré) $\rightarrow$ ils apprennent l'alphabet chiffré par cœur.
- Alice transforme son message clair selon la permutation des lettres, et l'envoie à Bob.

r e n d e z v o u s
X A F T A Q L D R I

c e s o i r
B A I D G X

Le code mono-alphabétique en pratique

- Alice et Bob doivent se rencontrer physiquement pour s'accorder sur la permutation des lettres (l'alphabet chiffré) $\rightarrow$ ils apprennent l'alphabet chiffré par cœur.
- Alice transforme son message clair selon la permutation des lettres, et l'envoie à Bob.
- Pour décoder le message, Bob utilise la même permutation à l'envers.

X A F T A Q L D R I

r e n d e z v o u s

B A I D G X

c e s o i r

Cryptanalyse du code mono-alphabétique

- Ce genre de code servit jusqu'à la fin du Moyen Âge en Europe.

Cryptanalyse du code mono-alphabétique

- Ce genre de code servit jusqu'à la fin du Moyen Âge en Europe.

- Mais à cette époque, on savait déjà casser ce code :
  Marie Stuart (reine d'Écosse) a été exécutée en 1587 car ses messages secrets concernant l'assassinat de la reine Élizabeth ont été déchiffrés.

Cryptanalyse du code mono-alphabétique

- Ce genre de code servit jusqu'à la fin du Moyen Âge en Europe.
- Mais à cette époque, on savait déjà casser ce code : Marie Stuart (reine d'Écosse) a été exécutée en 1587 car ses messages secrets concernant l'assassinat de la reine Élizabeth ont été déchiffrés.
- La cryptanalyse de ce code est due aux Arabes dès le IX^{e} siècle : leur civilisation était alors beaucoup plus avancée qu'en Europe et très prospère.
- Al-Kindi décrit le procédé : analyse de fréquences.

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

`KFFPAK CK MVXXPAQJK RK EKFFPZK`

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
e    e  e         e  e  e    e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e												

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
ess  e  e        e  e  ess  e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s											

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
essa e  e     a   e  e  essa e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s	a										

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
essaie  e     ai  e  e  essa e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s	a	i									

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
essaie de     ai  e le  essa e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s	a	i			l				d		

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
essaie de  nnai  e le  essa e
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s	a	i	n		l				d		

Analyse de fréquences

- Certaines lettres sont plus fréquentes que d'autres en français : e (15 %), a (10 %), i et s (8 %), etc.
- Si dans le texte chiffré, une lettre apparaît plus que les autres, elle code probablement le e ; la deuxième lettre la plus fréquente peut être a, i ou s, etc.
- Déchiffrons le code (sans connaître l'alphabet chiffré) :

```
KFFPAK CK MVXXPAQJK RK EKFFPZK
essaie de connaitre le message
```

Fréquences :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
7	4	3	2	2	1	1	1	1	1	1	1	1

Tentatives :

K	F	P	A	X	Q	R	J	E	V	C	M	Z
e	s	a	i	n	t	l	r	m	o	d	c	g

1. Formation accélérée

2. Surveiller ces dangereux citoyens

3. Espionner ces dangereux pays

4. Communiquer dans le monde hostile

Vous avez reçu un message…

Nous avons intercepté ce texte d'un dangereux pays…

VEJ NAMDRXIJEQS JB BEWFEEEQ K MRDCUVO VELCE
OGFXIFYE EK IOUID UNKBXTZZZS ZIC PIZOLRJONK
ZGVVODEDPZT HRO LVFDS SRDS EP BELSONK PFRV
XDTVTZTJ NEE GLD LV OONMPDSVJONK GUOCBXT
UP FOLQ V OIODE JLMIRW BAJPO QLP XEJ ZVAJDQS
UFBIXPMNKBC TIPYBCBXT UPHAEQ ENV
CQVFIETZZZ CFJWUETETV IOS GCALVQKIIPE N FKD
RZPZ A P MORUCQ QLB VELCE CYXSNVD ULJ LXT LY
YOEAO A XLSNVO ZRFWQTRFBEJ OQ TFRC LVD BAPP
ENZDEEQ SYUJ

Au travail !

Vous avez reçu un message…

Fréquences :

A	B	C	D	E	F	G	H	I	J	K	L	M
9	13	13	16	30	13	5	2	14	14	9	17	6

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	22	16	13	12	12	14	11	20	4	11	6	16

Le chiffre de Vigenère

Diplomate français (1523–1596)

TRAICTE'

DES CHIFFRES,

OV SECRETES

MANIERES

D'ESCRIRE:

PAR

BLAISE DE VIGENERE,

BOVRBONNOIS.

2295

antes muerto que mudado

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.

M. D. LXXXVI.

AVEC PRIVILEGE DV ROY.

Le chiffre de Vigenère

- Plutôt que de décaler les lettres selon un alphabet fixé, on les décale selon une clé que l'on répète

Le chiffre de Vigenère

- Plutôt que de décaler les lettres selon un alphabet fixé, on les décale selon une clé que l'on répète

Exemple : si la clé est ALICE

Texte clair : « Bob gare à toi »

texte	b (1)	o (14)	b (1)	g (6)	a (0)	r (17)
clé	A (0)	L (11)	I (8)	C (2)	E (4)	A (0)
code	B (1)	Z (25)	J (9)	I (8)	E (4)	R (17)

texte	e (4)	a (0)	t (19)	o (14)	i (8)
clé	L (11)	I (8)	C (2)	E (4)	A (0)
code	P (15)	I (8)	V (1)	S (18)	I (8)

Texte chiffré : BZJ IERP I VSI

Le chiffre de Vigenère

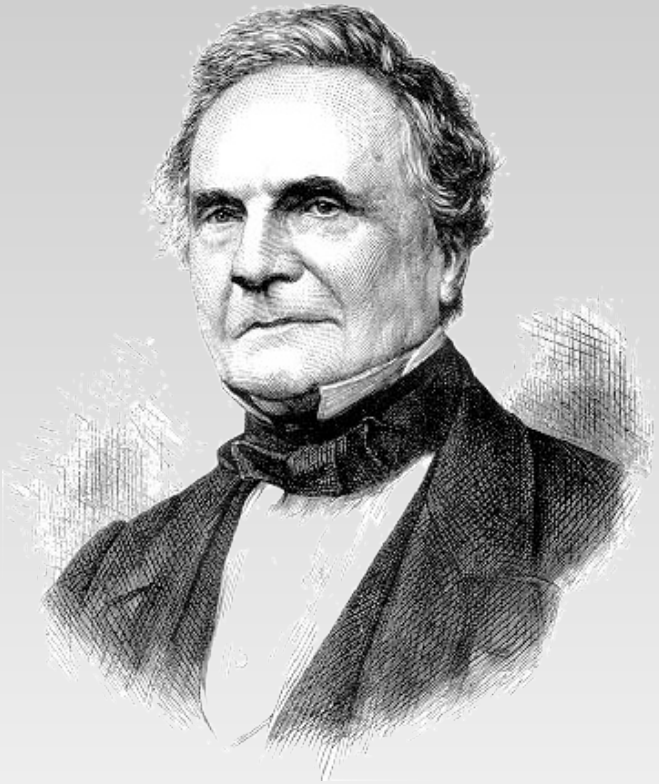
- Plutôt que de décaler les lettres selon un alphabet fixé, on les décale selon une clé que l'on répète

Avantages :

- une même lettre du message chiffré peut coder des lettres différentes du texte clair ;
- l'analyse de fréquences ne fonctionne plus ;
- facile à mettre en œuvre : il suffit de connaître la clé pour coder et pour décoder ;
- code réputé indéchiffrable…

Cryptanalyse du chiffre de Vigenère

- … indéchiffrable pendant 300 ans.
- En 1854, Charles Babbage réussit la cryptanalyse du chiffre de Vigenère.



Cryptanalyse du chiffre de Vigenère

- … indéchiffrable pendant 300 ans.
- En 1854, Charles Babbage réussit la cryptanalyse du chiffre de Vigenère.
- Si deux suites de lettres (p. ex. MGHQ) se répètent dans le texte chiffré, il est probable qu'elles viennent de deux mots identiques codés par une même partie de la clé.
- Si ces suites sont séparées d'une distance d, alors la taille de la clé divise d.
- En étudiant plusieurs répétitions, on en déduit la taille de la clé et on peut faire une analyse de fréquences pour chaque lettre de la clé.

Le texte du dangereux pays

VEJ NAMDRXIJEQS JB BEWFEEEQ K MRDCUVO VELCE
OGFXIFYE EK IOUID UNKBXTZZZS ZIC PIZOLRJONK
ZGVVODEDPZT HRO LVFDS SRDS EP BELSONK PFRV
XDTVTZTJ NEE GLD LV OONMPDSVJONK GUOCBXT
UP FOLQ V OIODE JLMIRW BAJPO QLP XEJ ZVAJDQS
UFBIXPMNKBC TIPYBCBXT UPHAEQ ENV
CQVFIETZZZ CFJWUETETV IOS GCALVQKIIPE N FKD
RZPZ A P MORUCQ QLB VELCE CYXSNVD ULJ LXT LY
YOEAO A XLSNVO ZRFWQTRFBEJ OQ TFRC LVD BAPP
ENZDEEQ SYUJ

Le texte du dangereux pays

VEJ NAMDRXIJEQS JB BEWFEEEQ K MRDCUVO VELCE
OGFXIFYE EK IOUID UNKBXTZZZS ZIC PIZOLRJONK
ZGVVODEDPZT HRO LVFDS SRDS EP BELSONK PFRV
XDTVTZTJ NEE GLD LV OONMPDSVJONK GUOCBXT
UP FOLQ V OIODE JLMIRW BAJPO QLP XEJ ZVAJDQS
UFBIXPMNKBC TIPYBCBXT UPHAEQ ENV
CQVFIETZZZ CFJWUETETV IOS GCALVQKIIPE N FKD
RZPZ A P MORUCQ QLB VELCE CYXSNVD ULJ LXT LY
YOEAO A XLSNVO ZRFWQTRFBEJ OQ TFRC LVD BAPP
ENZDEEQ SYUJ

distance entre blocs verts : 232 ; rouges : 56 → taille de clé 8 (pgcd)

Le texte du dangereux pays

0 : VXBKVXOXCODODODEOOXVMOVBCXEEWOKDOVSXOZBCEY

1 : EIEMEIUTPNELSNTENNTOIQAITTNTUSIRRENTARELNU

2 : JJWRLFIZIKDVEKVGMKUIRLJXIUVZEGIZULVLXFJVZJ

3 : NEFDCYDZZZPFPPTLPGPOWPDPPPCZTCPPCCDYLWODD

4 : AQECEEUZOGZDBFZDDUFDBXQMYHQZEAEZQEUYSQQBE

5 : MSEUOENSLVTSERTLSOOEAESNBAVCTLNAQCLONTTAE

6 : DJEVGKKZRVHSLVJVVCLJJJUKCEFFVVFPLYJEVRFPQ

7 : RBQOFIBIJORRSXNOJBQLPZFBBQIJIQKMBXLAOFRPS

Le texte du dangereux pays

0 : VXBKVXOXCODODODEOOXVMOVBCXEEWOKDOVSXOZBCEY

→ plus fréquent O

1 : EIEMEIUTPNELSNTENNTOIQAITTNTUSIRRENTARELNU

→ E, N, T

2 : JJWRLFIZIKDVEKVGMKUIRLJXIUVZEGIZULVLXFJVZJ

→ I, J, V

3 : NEFDCYDZZZPFPPTLPGPOWPDPPPCZTCPPCCDYLWODD

→ P

4 : AQECEEUZOGZDBFZDDUFDBXQMYHQZEAEZQEUYSQQBE

→ E, Q

5 : MSEUOENSLVTSERTLSOOEAESNBAVCTLNAQCLONTTAE

→ E

6 : DJEVGKKZRVHSLVJVVCLJJJUKCEFFVVFPLYJEVRFPQ

→ V

7 : RBQOFIBIJORRSXNOJBQLPZFBBQIJIQKMBXLAOFRPS

→ B

Le texte du dangereux pays

0 : VXBKVXOXCODODODEOOXVMOVBCXEEWOKDOVSXOZBCEY
→ plus fréquent O → clé K
1 : EIEMEIUTPNELSNTENNTOIQAITTNTUSIRRENTARELNU
→ E, N, T → clé A
2 : JJWRLFIZIKDVEKVGMKUIRLJXIUVZEGIZULVLXFJVZJ
→ I, J, V → clé R
3 : NEFDCYDZZZPFPPTLPGPOWPDPPPCZTCPPCCDYLWODD
→ P → clé L
4 : AQECEEUZOGZDBFZDDUFDBXQMYHQZEAEZQEUYSQQBE
→ E, Q → clé M
5 : MSEUOENSLVTSERTLSOOEAESNBAVCTLNAQCLONTTAE
→ E → clé A
6 : DJEVGKKZRVHSLVJVVCLJJJUKCEFFVVFPLYJEVRFPQ
→ V → clé R
7 : RBQOFIBIJORRSXNOJBQLPZFBBQIJIQKMBXLAOFRPS
→ B → clé X

Le texte déchiffré !

Texte clair (clé KARLMARX) :

« Les communistes se refusent à masquer leurs opinions et leurs intentions. Ils proclament ouvertement que leurs buts ne peuvent être atteints que par le renversement violent de tout l'ordre social passé. Que les classes dirigeantes tremblent devant une révolution communiste ! Les prolétaires n'ont rien à y perdre que leurs chaînes. Ils ont un monde à gagner. Prolétaires de tous les pays, unissez-vous ! »

(Karl Marx et Friedrich Engels, 1848)

Malgré Babbage…

- En vrai : symboles 0 et 1.

Malgré Babbage…

- En vrai : symboles 0 et 1.

- « Masque jetable » – si la clé est :
  - aussi longue que le texte,
  - aléatoire,

  alors le message est indéchiffrable.

Malgré Babbage…

- En vrai : symboles 0 et 1.
- « Masque jetable » – si la clé est :
  - aussi longue que le texte,
  - aléatoire,

  alors le message est indéchiffrable.
- Objectif : échanger une clé aléatoire de manière sécurisée
  → protocole quantique BB84 (sûr en théorie).


(B)

(B)


1. Formation accélérée

2. Surveiller ces dangereux citoyens

3. Espionner ces dangereux pays

4. Communiquer dans le monde hostile

1850–1920

- De 1850 à 1920 : plus de code fiable !
- Développement du télégraphe

1850–1920

- De 1850 à 1920 : plus de code fiable !
- Développement du télégraphe
  puis de la radio au début du XX^{e} siècle
  $\Rightarrow$ besoin de codes sûrs

1850–1920

- De 1850 à 1920 : plus de code fiable !
- Développement du télégraphe
  puis de la radio au début du XX^{e} siècle
  $\Rightarrow$ besoin de codes sûrs
- Première Guerre mondiale, juin 1918 : les Allemands veulent prendre Paris

1850–1920

- De 1850 à 1920 : plus de code fiable !
- Développement du télégraphe
  puis de la radio au début du XX^{e} siècle
  $\Rightarrow$ besoin de codes sûrs
- Première Guerre mondiale, juin 1918 : les Allemands veulent prendre Paris
- Message codé pour avertir leurs troupes :
  code “ADFGVX”
- Les Alliés parviennent à déchiffrer le message à temps
  et repoussent les Allemands.

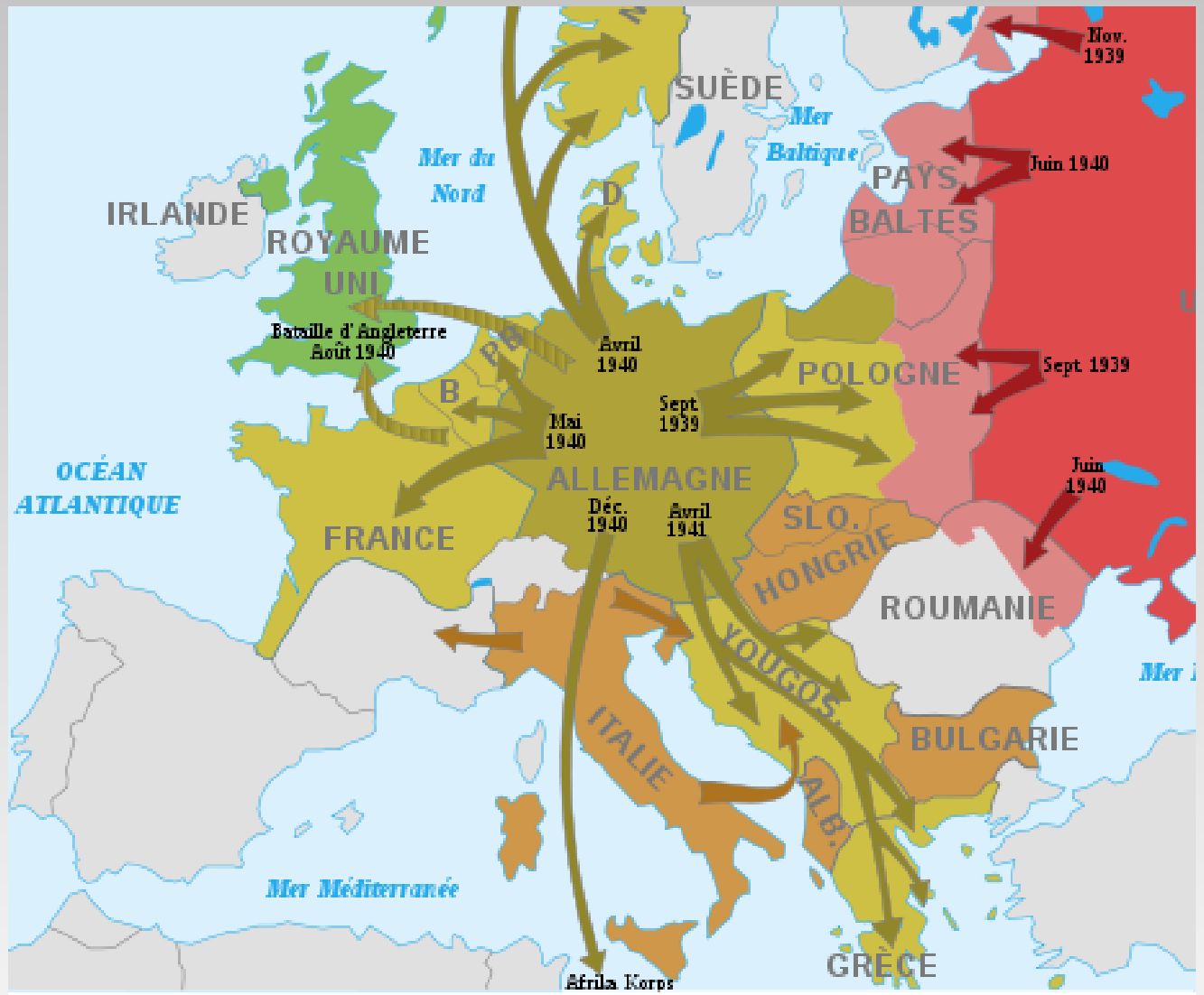
1850–1920

- De 1850 à 1920 : plus de code fiable !
- Développement du télégraphe
  puis de la radio au début du XX^{e} siècle
  $\Rightarrow$ besoin de codes sûrs
- Première Guerre mondiale, juin 1918 : les Allemands veulent prendre Paris
- Message codé pour avertir leurs troupes :
  code “ADFGVX”
- Les Alliés parviennent à déchiffrer le message à temps
  et repoussent les Allemands.

À partir de 1920 : développement de machines à coder.

Enigma

Seconde Guerre mondiale (1939–1945)

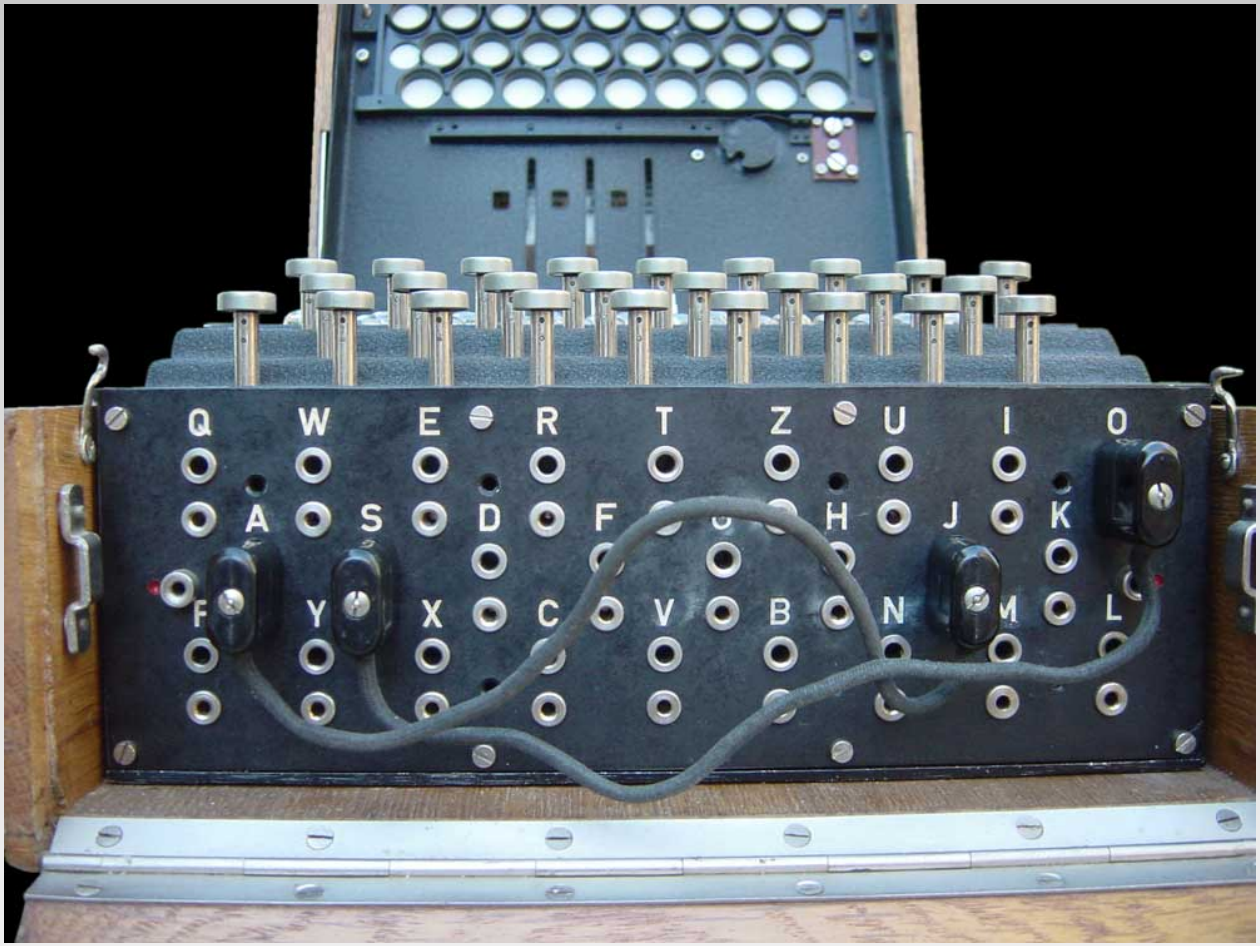


Enigma

- Interceptions radio → codes fiables indispensables
- Machine Enigma mise au point par les Allemands

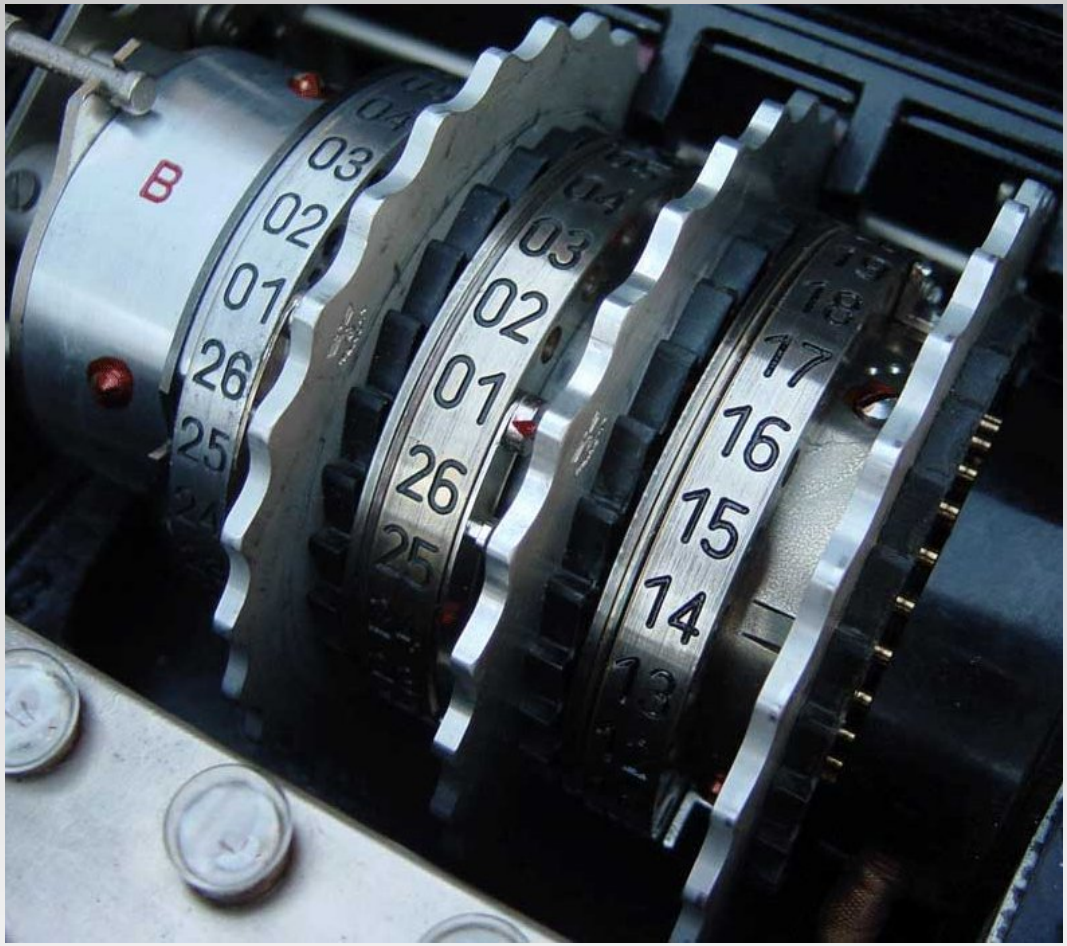
Enigma

- Interceptions radio $\rightarrow$ codes fiables indispensables
- Machine Enigma mise au point par les Allemands



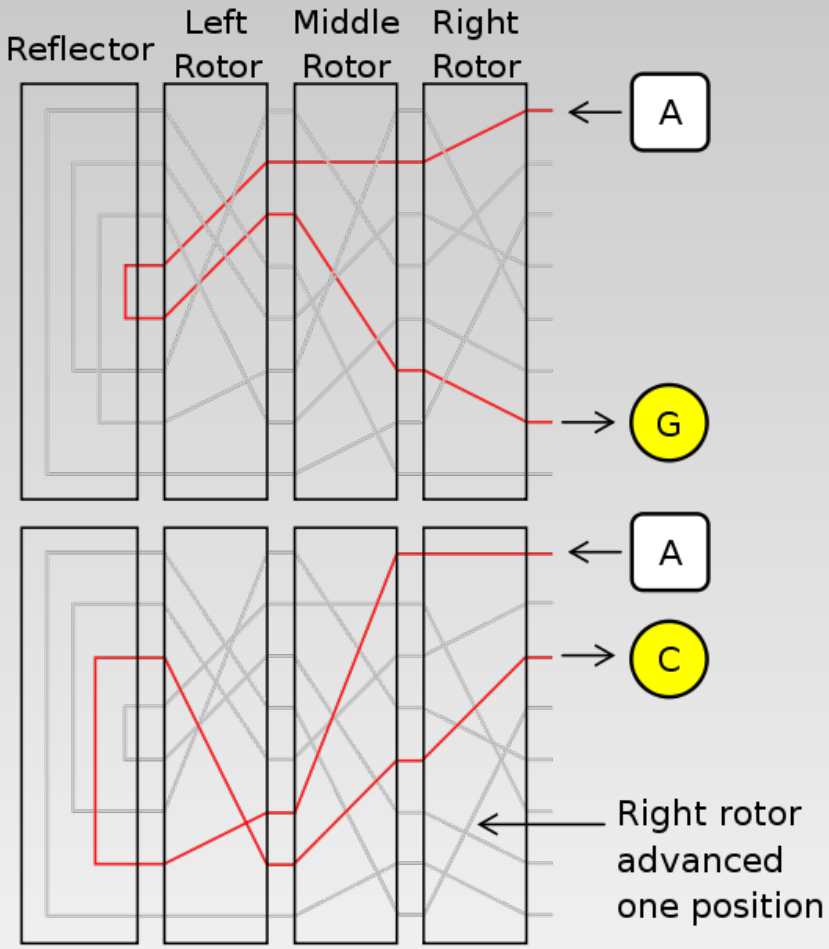
Enigma

- Interceptions radio $\rightarrow$ codes fiables indispensables
- Machine Enigma mise au point par les Allemands



Enigma

- Interceptions radio → codes fiables indispensables
- Machine Enigma mise au point par les Allemands



Enigma

- Interceptions radio → codes fiables indispensables
- Machine Enigma mise au point par les Allemands

Enigma

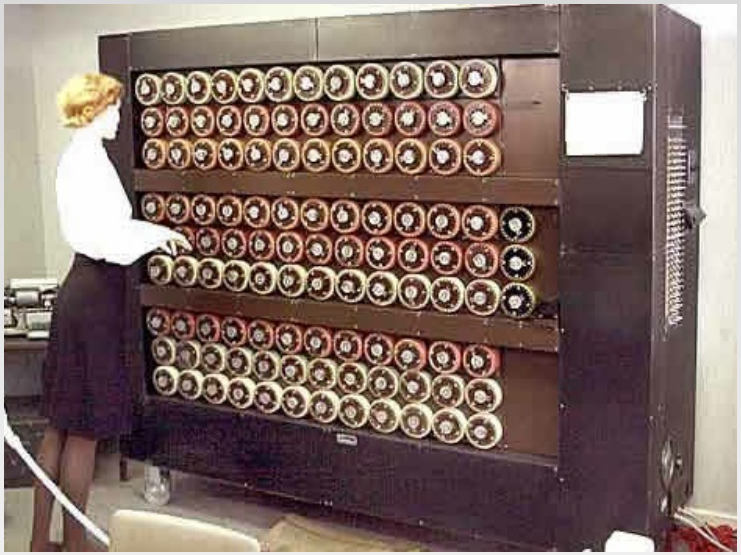
- Code Enigma réputé inviolable

Enigma

- Code Enigma réputé inviolable
- Avant la guerre, Marian Rejewski (services secrets polonais) réussit à déchiffrer les messages d'une première version d'Enigma grâce à des répétitions dans le code.

Enigma

- Code Enigma réputé inviolable
- Avant la guerre, Marian Rejewski (services secrets polonais) réussit à déchiffrer les messages d'une première version d'Enigma grâce à des répétitions dans le code.
- Mécanisation du processus de décodage (« bombes de Rejewski »).



Enigma

- Code Enigma réputé inviolable
- Avant la guerre, Marian Rejewski (services secrets polonais) réussit à déchiffrer les messages d'une première version d'Enigma grâce à des répétitions dans le code.
- Juste avant l'invasion de la Pologne, l'Angleterre récupère les travaux de Rejewski.
- Les Allemands améliorent nettement leur machine : la méthode de Rejewski ne fonctionne plus !

Enigma

- Code Enigma réputé inviolable
- Avant la guerre, Marian Rejewski (services secrets polonais) réussit à déchiffrer les messages d'une première version d'Enigma grâce à des répétitions dans le code.
- Juste avant l'invasion de la Pologne, l'Angleterre récupère les travaux de Rejewski.
- Les Allemands améliorent nettement leur machine : la méthode de Rejewski ne fonctionne plus !
- Alan Turing (services secrets anglais) parvient à déchiffrer les messages des nouvelles machines
- Les Alliés peuvent lire les messages ennemis.

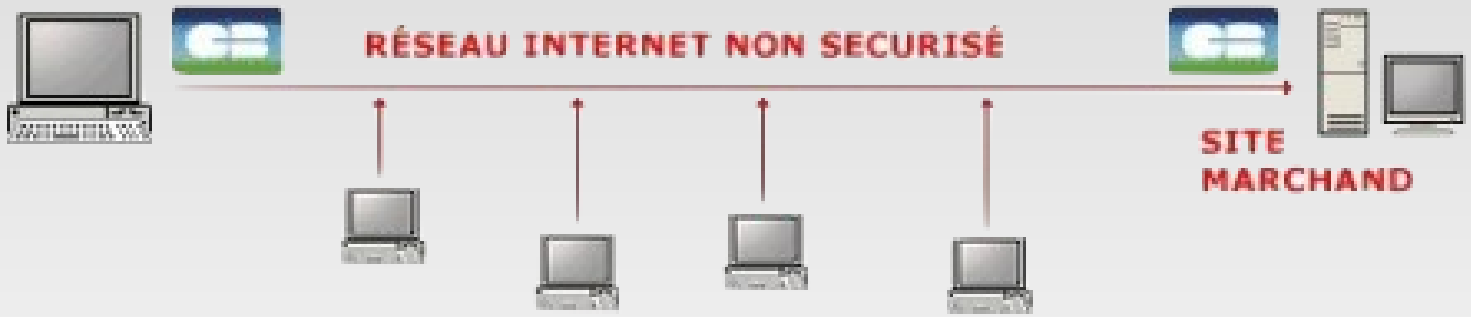
Enigma

L'échange des clés ?

- Jusqu'à présent : pour envoyer un message il faut d'abord s'échanger physiquement la clé
  - se mettre d'accord sur une substitution
  - envoyer des carnets de codes à ses troupes…

L'échange des clés ?

- Jusqu'à présent : pour envoyer un message il faut d'abord s'échanger physiquement la clé
  - se mettre d'accord sur une substitution
  - envoyer des carnets de codes à ses troupes…
- Aujourd'hui : Internet, commerce électronique…
- On ne peut plus échanger physiquement les clés
- Est-il possible d'envoyer des messages codés sans échange de clés ?



L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

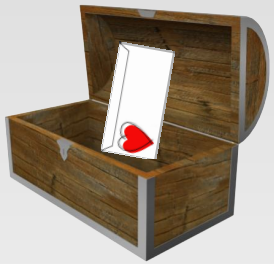
- A demande à B un coffre dont seul B a la clé ;

L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

- A demande à B un coffre dont seul B a la clé ;
- A met le message dans le coffre

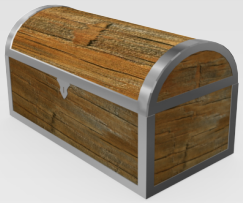


L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

- A demande à B un coffre dont seul B a la clé ;
- A met le message dans le coffre et le ferme ;

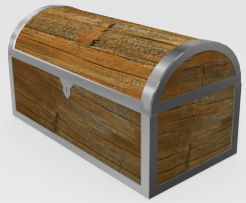


L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

- A demande à B un coffre dont seul B a la clé ;
- A met le message dans le coffre et le ferme ;
- A le renvoie à B ;



L'échange des clés

Diffie, Hellman, Merkle 1976

Si Alice veut envoyer un message à Bob :

- A demande à B un coffre dont seul B a la clé ;
- A met le message dans le coffre et le ferme ;
- A le renvoie à B ;
- B ouvre le coffre avec sa clé et lit le message.

Fonction à sens unique

- Trouver ce qui peut servir de « coffre »

Fonction à sens unique

- Trouver ce qui peut servir de « coffre »
- $\rightarrow$ une fonction de codage $f_c(x)$
  - facile à calculer = coder le message (fermer le coffre)
  - pour les intrus, difficile à inverser = percer le code (ouvrir le coffre sans la clé)
  - facile à inverser pour B (ouvrir le coffre avec la clé)
- B doit disposer d'une information supplémentaire :
  $\rightarrow$ une clé secrète
- Tout le monde peut lui envoyer des messages chiffrés
  $\rightarrow$ une clé publique

Cryptographie à clé publique

- B diffuse dans un annuaire une clé publique (pour que tout le monde puisse coder un message à son attention)
- Il garde pour lui la clé secrète correspondante

Cryptographie à clé publique

- B diffuse dans un annuaire une clé publique (pour que tout le monde puisse coder un message à son attention)
- Il garde pour lui la clé secrète correspondante

- Si A veut lui envoyer un message, elle l'encode grâce à la clé publique de B

Cryptographie à clé publique

- B diffuse dans un annuaire une clé publique (pour que tout le monde puisse coder un message à son attention)
- Il garde pour lui la clé secrète correspondante
- Si A veut lui envoyer un message, elle l'encode grâce à la clé publique de B
- B peut lire le message grâce à sa clé privée

Le système RSA

Rivest, Shamir, Adleman 1977

Le système RSA

- Fonction à sens unique : le produit de deux entiers
- Facile à calculer : par exemple, $13 \times 17 = 221$
- Difficile à inverser : par exemple,
  trouver les facteurs de 437 ???

Le système RSA

- Fonction à sens unique : le produit de deux entiers
- Facile à calculer : par exemple, $13 \times 17 = 221$
- Difficile à inverser : par exemple,
  trouver les facteurs de 437 ??? (réponse : 19×23)

RSA en théorie

- B choisit deux grands nombres premiers p et q
- Il calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$

RSA en théorie

- B choisit deux grands nombres premiers p et q
- Il calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$
- Il choisit $c < \phi(n)$ premier avec $\phi(n)$
  (exposant de chiffrement)
- Il calcule d tel que $cd \equiv 1 \mod \phi(n)$
  (exposant de déchiffrement)

RSA en théorie

- B choisit deux grands nombres premiers p et q
- Il calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$
- Il choisit $c < \phi(n)$ premier avec $\phi(n)$
  (exposant de chiffrement)
- Il calcule d tel que $cd \equiv 1 \mod \phi(n)$
  (exposant de déchiffrement)
- Clé publique : couple (n, c) / clé privée : d

RSA en théorie

- B choisit deux grands nombres premiers p et q
- Il calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$
- Il choisit $c < \phi(n)$ premier avec $\phi(n)$
  (exposant de chiffrement)
- Il calcule d tel que $cd \equiv 1 \mod \phi(n)$
  (exposant de déchiffrement)
- Clé publique : couple (n, c) / clé privée : d
- Pour coder un message M :
  - A le convertit en un entier
  - Elle consulte la clé publique de B
    et calcule $C \equiv M^c \mod n$
  - Elle envoie C à B

RSA en théorie

- B choisit deux grands nombres premiers p et q
- Il calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$
- Il choisit $c < \phi(n)$ premier avec $\phi(n)$
  (exposant de chiffrement)
- Il calcule d tel que $cd \equiv 1 \mod \phi(n)$
  (exposant de déchiffrement)
- Clé publique : couple (n, c) / clé privée : d
- Pour coder un message M :
  - A le convertit en un entier
  - Elle consulte la clé publique de B
    et calcule $C \equiv M^c \mod n$
  - Elle envoie C à B
- Pour décoder C :
  - B calcule $M \equiv C^d \mod n$

RSA en pratique

- Utilisé pour toute transaction sur Internet

- p et q doivent avoir de l'ordre de 300 chiffres

RSA en pratique

- Utilisé pour toute transaction sur Internet

- p et q doivent avoir de l'ordre de 300 chiffres
- Relativement lent pour coder un message
- $\rightarrow$ on utilise donc RSA pour échanger des clés secrètes et ensuite on utilise ces clés avec d'autres algorithmes pour coder le message

RSA en pratique

- Utilisé pour toute transaction sur Internet

- p et q doivent avoir de l'ordre de 300 chiffres
- Relativement lent pour coder un message
- $\rightarrow$ on utilise donc RSA pour échanger des clés secrètes et ensuite on utilise ces clés avec d'autres algorithmes pour coder le message
-  Si p et q sont trop petits ou mal choisis, on peut casser le code RSA.

Certifications de niveau supérieur

- Ordinateur quantique et algorithme de Shor (1994)
- Cryptographie quantique
- Courbes elliptiques, logarithme discret

Pour aller plus loin :

- Simon Singh, *Histoire des codes secrets*
- Didier Müller,
  `http://apprendre-en-ligne.net/crypto`

Félicitations