

HISTOIRE DE LA CRYPTOGRAPHIE

DE L'ANTIQUITÉ À LA SECONDE GUERRE MONDIALE

Yann Rotella

UVSQ - Université Paris-Saclay

22 janvier 2026



PLAN DU COURS

L'ANTIQUITÉ

DES PREMIÈRES NOTIONS MODERNES

LES MACHINES À CHIFFRER

ENIGMA ET LA CRYPTANALYSE

CACHER DES MESSAGES

-1600 Sur une tablette d'argile, en enlevant des lettres (Irak)

DÉFINITION (STÉGANOGRAPHIE)

Dissimuler une information. Steganos « étanche, hermétique » et graphein.

Il n'y a pas de notion de clef secrète. Une fois la technique découverte, le message peut être retrouvé.

Exemple le plus connu : l'encre invisible.

- ▶ Dans les pixels d'une image ;
- ▶ Tatouer sur la tête (Grèce Antique) ;

L'ANTIQUITÉ

Transpositions

Substitutions

DES PREMIÈRES NOTIONS MODERNES

Quelques exemples historiques

Le chiffre de Battista (Vigenère)

LES MACHINES À CHIFFRER

Le principe de Kerckhoffs

Exemples historiques

ENIGMA ET LA CRYPTANALYSE

CHIFFREMENTS PAR TRANSPOSITIONS

DÉFINITION

*Un chiffrement par **transposition** est un mécanisme qui consiste à permuter les lettres d'un message.*

Exemple : Chiffrer les messages de 7 lettres

- ✍ Quel est l'espace des messages ? Quel est l'espace des clefs ?
- ✍ Chiffrer BONJOUR avec la clef $1 \rightarrow 3, 2 \rightarrow 6, 3 \rightarrow 4, 4 \rightarrow 1, 5 \rightarrow 5, 6 \rightarrow 7$ et $7 \rightarrow 2$.
- ✍ Décrire proprement la fonction de chiffrement et la fonction de déchiffrement.
- ✍ Indépendamment de la sécurité, pourquoi est-ce compliqué d'utiliser un tel chiffrement ?

EXEMPLES HISTORIQUES

- ▶ La scytale (Sparte, -400)



- ▶ Le chiffre Rail Fence (Guerre de Sécession)

C	Y	T	G	A	H	E
R	P	O	R	P	I	

- ✍ Identifier les problèmes.

CHIFFREMENTS PAR SUBSTITUTION

DÉFINITION

Un chiffrement par **substitution** est un mécanisme qui consiste à remplacer chaque lettre par une autre (ou la même). Un chiffrement par substitution est donc défini par une **permutation** de l'alphabet.

- ☞ Donner l'espace des messages et donner l'espace des clefs.
- ▶ On peut utiliser un alphabet différent pour les messages chiffrés (chiffre des templiers).

Le chiffre de César (Guerre des Gaules, alphabet grec, décalage de 3)

- ▶ $A = 0, B = 1, \dots, Z = 25$
- ▶ $\mathcal{K} = \{0, 1, \dots, 25\} = \mathbb{Z}/26\mathbb{Z}$
- ▶ $\mathcal{M} = \{A, B, \dots, Z\}^* = (\mathbb{Z}/26\mathbb{Z})^*$
- ☞ Décrire mathématiquement la fonction de chiffrement et la fonction de déchiffrement.
- ☞ On observe un message chiffré, comment pouvons-nous le décrypter ?

L'ANTIQUITÉ

Transpositions
Substitutions

DES PREMIÈRES NOTIONS MODERNES

Quelques exemples historiques
Le chiffre de Battista (Vigenère)

LES MACHINES À CHIFFRER

Le principe de Kerckhoffs
Exemples historiques

ENIGMA ET LA CRYPTANALYSE

TAILLE DES CLEFS ET CRYPTANALYSE

Le nombre de clefs possibles doit être grand.

Pour un chiffrement par substitution général, il y a $26! \approx 2^{88}$ clefs possibles.

L'analyse des fréquences

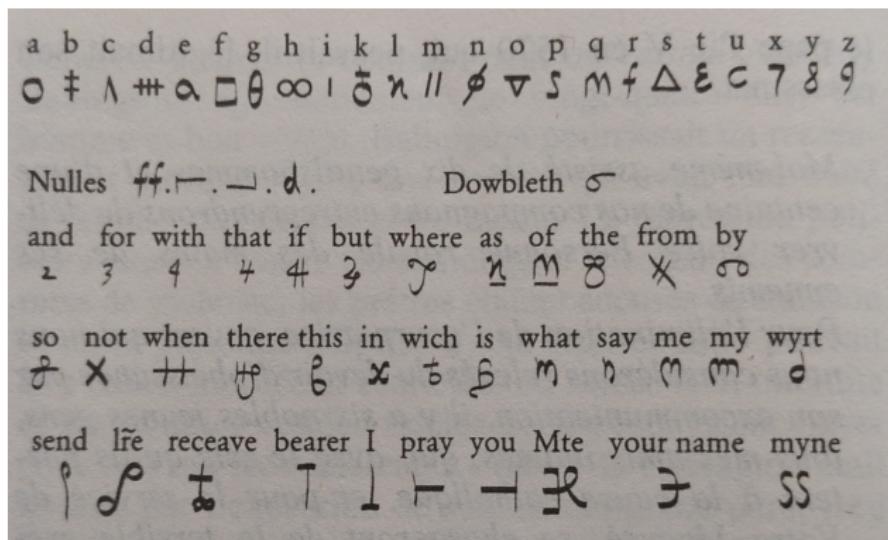
- ▶ Al-Kindi, Bagdad, 9ème siècle.
- ▶ **Observation :** Dans (toutes) les langues utilisant un alphabet, certaines lettres ou combinaisons de lettres apparaissent avec une **fréquence** différente.
- ▶ **Cryptanalyse** : langue connue, texte long. On observe dans le texte chiffré les lettres (ou symboles) les plus fréquentes. Celles-ci correspondent (très probablement) aux lettres les plus fréquentes de la langue d'origine.
- ▶ Avancée : on peut continuer de proche en proche avec les bigrammes fréquents pour trouver d'autres lettres.
- ▶ Les chiffrements par substitution monoalphabétique ont été utilisés jusqu'au 15ème siècle.

DU 16ÈME AU 18ÈME SIÈCLE

- ▶ Chiffrement **homophonique** : chaque lettre est remplacée par (plusieurs) lettres, dont le nombre est proportionnel à la fréquence d'apparition. L'alphabet de sortie est donc plus grand.
- ▶ Rajout de **caractères nuls** dans le texte chiffré.
- ▶ Chiffrement de **bigrammes** par un autre caractère.
- ▶ Chiffrement de **mots fréquents** par un autre caractère.

EXEMPLES HISTORIQUES

- Marie Stuart, Reine d'écosse, 16ème siècle ;



- Correspondance de Charles Quint, 16ème siècle (déchiffrée en 2022) ;
- Chiffre de Louis XIV.

UNE SOLUTION POLYALPHABÉTIQUE

- ▶ Giovani Battista Bellaso (1553)
- ▶ Blaise de Vigenère (1586)
- ▶ Le chiffre d'Alberti (1466)

$$\mathcal{K} = \{A, \dots, Z\}^n = (\mathbb{Z}/26\mathbb{Z})^n$$

$$\begin{aligned}\text{Enc} : (\mathbb{Z}/26\mathbb{Z})^n \times (\mathbb{Z}/26\mathbb{Z})^* &\rightarrow (\mathbb{Z}/26\mathbb{Z}) \\ (\textcolor{red}{k}, \textcolor{blue}{m}) &\mapsto \textcolor{green}{c}\end{aligned}$$

Soit $\ell \in \mathbb{N}$ le nombre de lettres de $\textcolor{blue}{m}$.

$$\forall 0 \leq i < \ell, \textcolor{green}{c}_i = \textcolor{blue}{m}_i + \textcolor{red}{k}_i \bmod n$$

- ✍ Déchiffrer le message **CKRPJIGVLCXAKUCBTWP** avec la clef **CRYPTO**.

CRIPTANALYSE

- ▶ Charles Babbage (1792 - 1871)
- ▶ Friedrich Wilhelm Kasisiki (1805 - 1881)
- Si on connaît la taille de la clef (n), que pouvons-nous faire ?

Autre observation : Dans (toutes) les langues, il y a des répétitions assez fréquentes.

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

- ▶ Les **mêmes séquences** de lettres sont chiffrées avec la **même partie** de la clé !

UN EXEMPLE COMPLET

XAUNMEESYIEDTLLFGSNBWQ
UFXPQTYORUTYIINUMQIEUL
SMFAFXGUTYBXXAGBHMIFII
MUMQIDEKRIFRIRZQUHIENO
OOIGRMLYETYOVQRYSIXEOK
IYPYOIGRFBWPIYRBQURJIY
EMJIGRYKXYACPPQSPBVESI
RZQRUFREDYJIGRYKXBLOPJ
ARNPUGEFBWMILXMZSMZYXP
NBPUMYZMEEFBUGENLRDEPB
JXONQEZTMBWOEFIIPAHPHQ
BFLGDEMFWFAHQ

XAUNMEESYIEDTLLFGSNBWQ
UFXPQTYORUTYIIN**UMQI**EUL
SMFAFXGUTYBXXAGBHMIFII
MUMQIDEKRIFRIRZQUHIENO

UN EXEMPLE COMPLET

Séquence répétée	Espace de répétition	Longueurs de clé possibles								
		2	3	4	5	6	7-9	10	11-14	15
UMQI	30	✓	✓		✓	✓		✓		✓
OIGR	25				✓					
JIGRY	30	✓	✓		✓	✓		✓		✓

Séquence répétée	Espace de répétition	Longueurs de clé possibles								
		2	3	4	5	6	7-9	10	11-14	15
UMQI	30	✓	✓		✓	✓		✓		✓
OIGR	25				✓					
JIGRY	30	✓	✓		✓	✓		✓		✓

Taille de la clef k : 5 lettres. $k = k_0||k_1||k_2||k_3||k_4$

- ▶ chiffre polyalphabétique composé de 5 chiffres

RÉCUPÉRER k_1

XAUNMEESYIEDTLLFGSNBWQ
UFXPQTYORUTYIINUMQIEUL
SMFAFXGUTYBXXAGBHMIFII
MUMQIDEKIRFRIRZQUHIENO
OOIGRMLYETYOVQRYSIXEOK
IYPYOIGRFBWPIYRBQURJIY
EMJIGRYKXYACPPQSPBVESI
RZQRUFREDYJIGRYKXBLOPJ
ARNPUGEFBWMILXMZSMZYXP
NBPUMYZMEEFBUGENLRDEPB
JXONQEZEZMBWOEFIIPAHPHQ
BFLGDEMFWFAHQ

XAUNMEESYIEDTLLFGSNBWQ
UFXPQTYORUTYIINUMQIEUL
SMFAFX**GH**MIFII
MUMQ**I**DEK**R**FRIRZ**Q**U**H**ENO
OOIGRMLY**E**TYOV**Q**RYSIX**E**OK
IYPOIGRFB**W**PIYRB**Q**UR**J**Y
EM**J**IG**R**YKXYACPPQSPB**V**ESI
RZ**Q**RU**F**REDYJIG**R**YKXB**L**OPJ
ARN**P**UGEF**B**WMILXMZSMZYXP
NBPUMYZ**M**EEFBUGENLR**D**EPB
JXONQE**Z**TMB**W**OE**F**II**P**AHPHQ
BFLGDEM**F**WFAHQ

FRÉQUENCES DES LETTRES EN POSITION 0 MODULO 5

X X X

ET ON CONTINUE

XAUNMEESYIEDTLLFGSNBWQ
UFXPQTYORUTYIINUMQIEUL
SMFAFXGUTYBXXAGBHMIFII
MUMQIDEKRIFRIRZQUHIENO
OOIGRMLYETYOVQRYSIXEOK
IYPYOIGRFBWPIYRBQURJIY
EMJIGRYKXYACPPQSPBVESI
RZQRUFREDYJIGRYKXBLOPJ
ARNPUGEFBWMILXMZSMZYXP
NBPUMYZMEEFBUGENLRDEPB
JXONQEZTMBWOEFIIPAHPHQ
BFLGDEMFWFAHQ

X**AUNMEESYIEDTLLFGSNBWQ**
UFXPQTYORUTYI**INUMQIEUL**
SMFAFXGUTYBXXAGBH**MIFII**
MUMQIDEKRIFRIRZQUHIENO

L'ANTIQUITÉ

Transpositions
Substitutions

DES PREMIÈRES NOTIONS MODERNES

Quelques exemples historiques
Le chiffre de Battista (Vigenère)

LES MACHINES À CHIFFRER

Le principe de Kerckhoffs
Exemples historiques

ENIGMA ET LA CRYPTANALYSE

18ÈME - 20ÈME SIÈCLE : LES MACHINES À CHIFFRER

- ▶ 1795 : le cylindre de **Jefferson**



- ▶ Fin du 19ème siècle : **Guglielmo Marconi** invente la **télégraphie sans fil**

LE PRINCIPE DE KERCKHOFFS - 1883

Dans un contexte de guerre Franco-Prussienne, les français s'intéressent à la cryptographie.

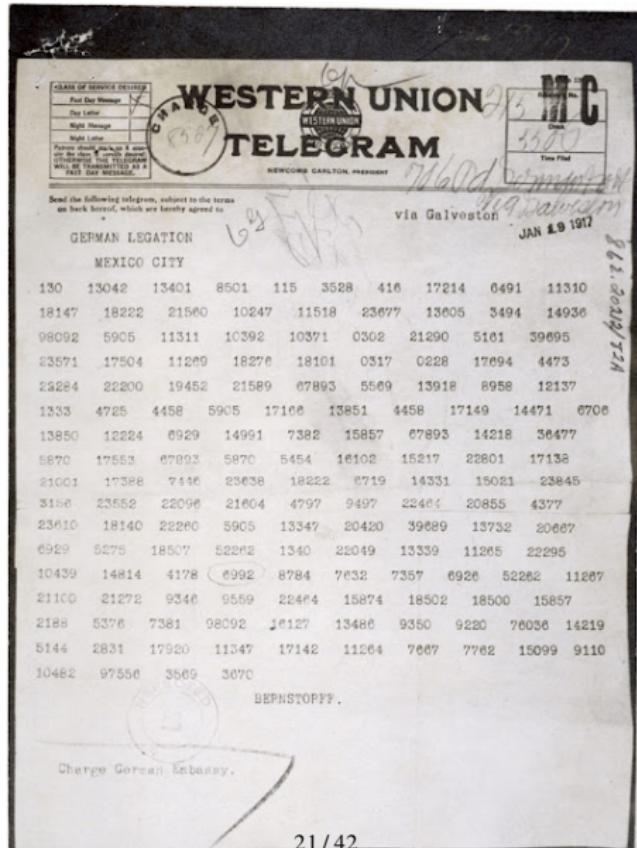
Auguste Kerckhoffs, *La cryptographie militaire*

La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé.

Claude Shannon :

L'adversaire connaît le système.

PREMIÈRE GUERRE MONDIALE - LE TÉLÉGRAMME DE ZIMMERMANN



PREMIÈRE GUERRE MONDIALE - LE TÉLÉGRAMME DE ZIMMERMANN

- ▶ le 16 janvier 1917
- ▶ Arthur Zimmermann, ministre des affaires étrangères de l'empire Allemand
- ▶ Alliance avec le Mexique contre les États-Unis
- ▶ Intercepté le 17 janvier
- ▶ Décrypté par les Alliés
- ▶ Entraîne les États-Unis dans la Guerre

PREMIÈRE GUERRE MONDIALE - LE CHIFFRE ADFGVX

- ▶ Substitutions et transpositions
- ▶ Les Français et Britanniques mettent plus de ressources dans la **cryptanalyse**.
- ▶ Message cryptanalysé par George Painvin, Bureau du Chiffre le 2 juin 1918 :
 « Acheminez munitions. Urgence. Même de jour si Camouflés »
- ▶ Perte de surprise, bataille perdue par les Allemands.

L'ANTIQUITÉ

Transpositions

Substitutions

DES PREMIÈRES NOTIONS MODERNES

Quelques exemples historiques

Le chiffre de Battista (Vigenère)

LES MACHINES À CHIFFRER

Le principe de Kerckhoffs

Exemples historiques

ENIGMA ET LA CRYPTANALYSE

ENIGMA

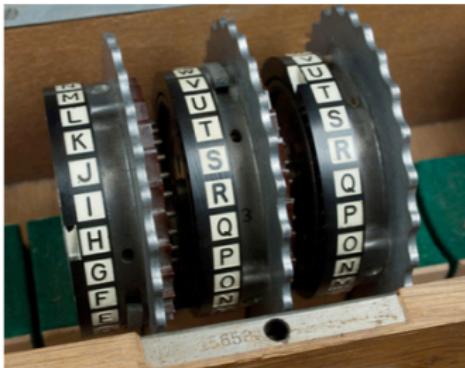
- ▶ Inventée par l'ingénieur allemand Arthur Scherbius en 1918.
- ▶ Modèle A de la machine présenté à Berlin en 1923 (prix éq : 30000 euros)
- ▶ D'autres modèles ont été utilisés par l'armée et la marine allemande.

Parties principales :

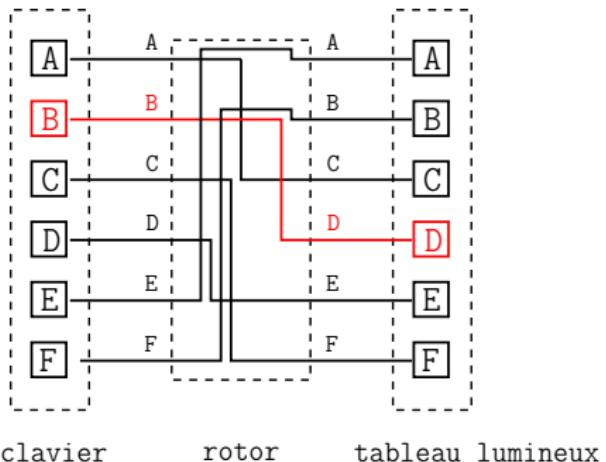
- ▶ Clavier
- ▶ Tableau lumineux
- ▶ Rotors
- ▶ Tableau des connexions
- ▶ Réflecteur



LES ROTORS



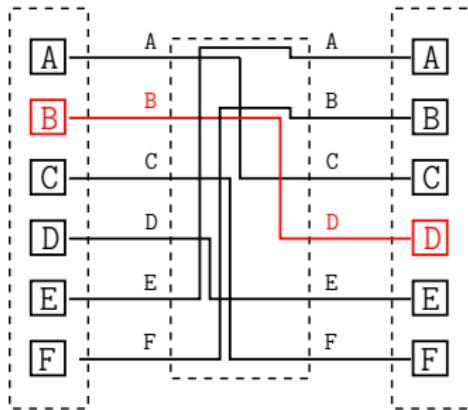
MACHINE AVEC UN ROTOR



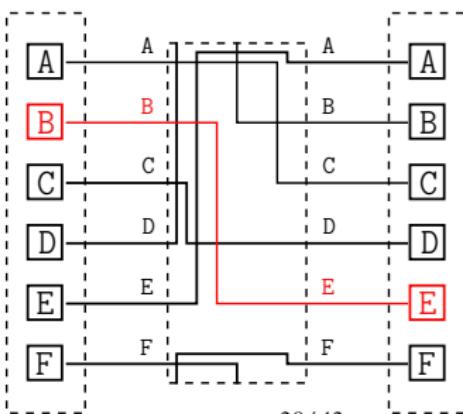
- ▶ Substitution monoalphabétique

A	B	C	D	E	F
C	D	F	E	A	B

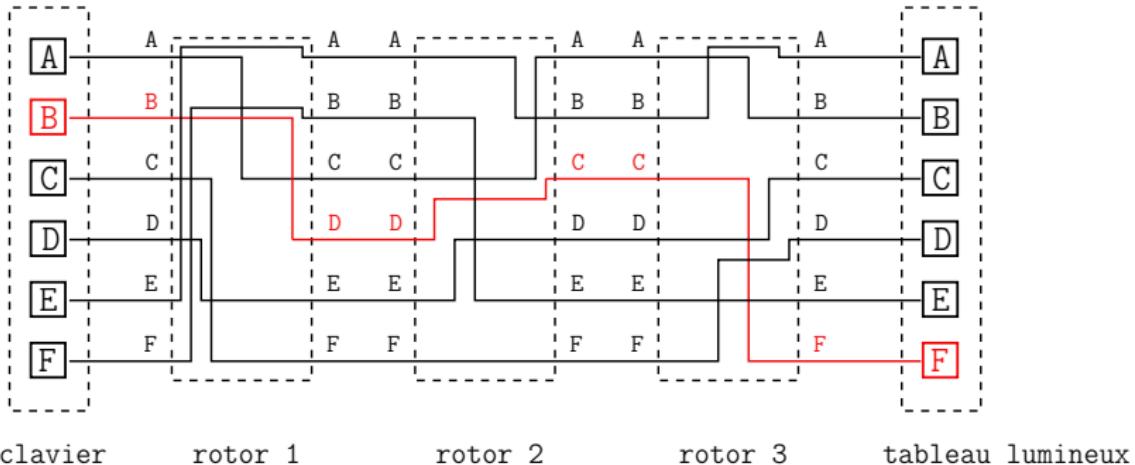
ON TOURNE LE ROTOR POUR UNE NOUVELLE LETTRE



clavier rotor tableau lumineux

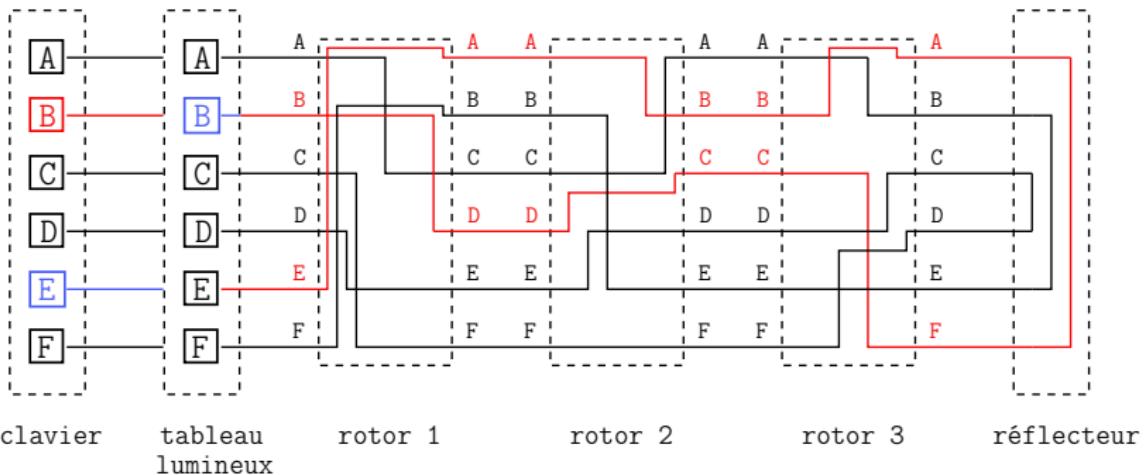


MACHINE À TROIS ROTORS



- ▶ Les câblages internes de chacun des trois rotors sont **différents**.
- ▶ Chaque nouveau rotor représente 26 alphabets différents.
- ▶ Substitution avec 26^3 alphabet différents.

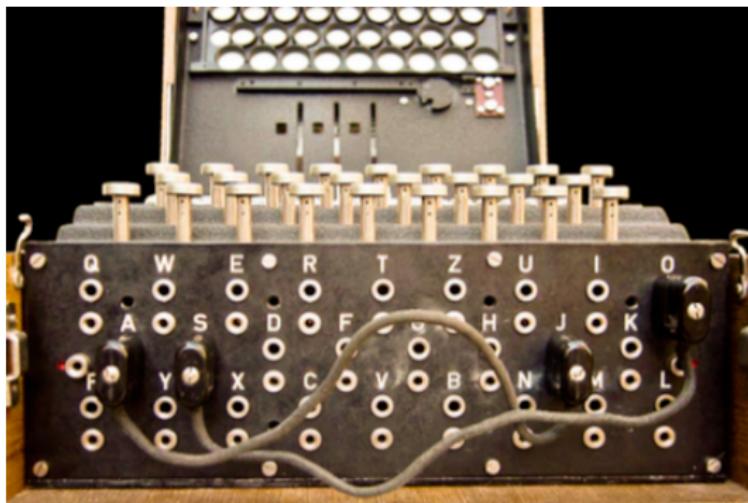
MACHINE À TROIS ROTORS AVEC RÉFLECTEUR



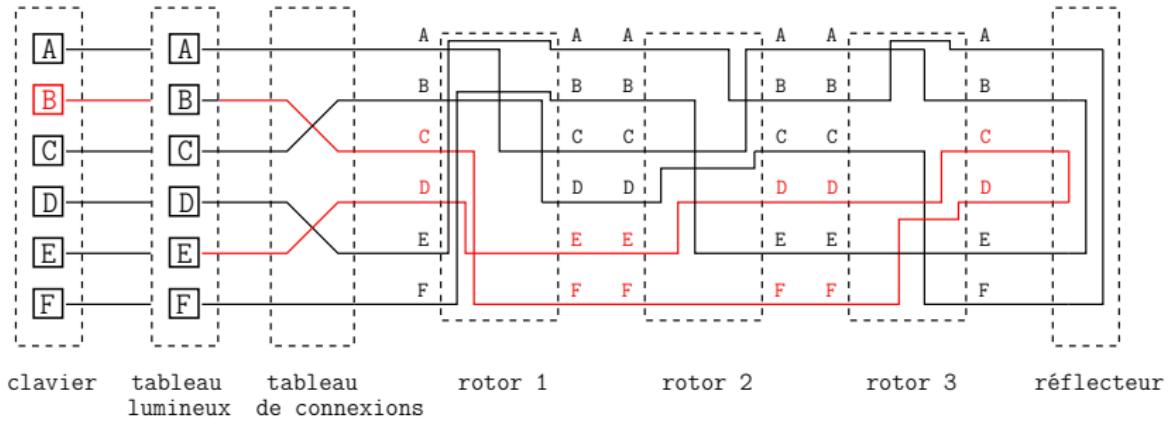
✍ À quoi sert le réflecteur ?

Le processus de déchiffrement et de chiffrement est le même !

AJOUT DU TABLEAU DE CONNEXIONS



AJOUT DU TABLEAU DE CONNEXIONS



Clé secrète : ordre des rotors + positions des rotors + 6 couples de lettres transposées.

$$6 \times 26^3 \times 100\,391\,791\,500 \approx 2^{53} \text{ possibilités.}$$

ENIGMA AVANT LA GUERRE

Nombre de clefs possibles :

- ▶ 3 rotors parmi 5 : 10 possibilités
- ▶ Ordre des rotors : 6 possibilités
- ▶ Position initiale des rotors : $26 \times 26 \times 26$ possibilités
- ▶ Tableau de connexion : 150 738 274 937 250 possibilités

Le nombre de clefs secrètes pour Enigma est de 2^{67} .

LA RÉPUTATION DE LA MACHINE

- ▶ Interception dès 1926 des messages chiffrés par Enigma.
- ▶ Anglais, français et américains abandonnent tout espoir.
- ▶ Seule une nation s'y attaque : la Pologne.



Marian Rejewski
mathématicien polonais du
Biuro Szyfrow.

CARNET DE CODES

GEHEIM	STADTTON	JULI 1940		
Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31 IV V I 24 17 18 AQ CT DV EN FW GP IX JS KR LO BEA KZG SIK VHO				
30 II V III 23 11 01 AL BS ED FR GH JN PY QZ TW VX ZUF SIC FDR BBD				
29 V III I 19 02 21 AR DS CF DE GQ HI JK LS QX AFU DZG LDU CBB				
28 IV III II 18 07 18 AR DS CF DE GQ HI JK LS QX AFU DZG LDU CBB				
27 IV III II 02 07 18 AC BP EZ FX GV HK LT MR NU QW ZDN MCV FCK CBJ				
26 IV III II 02 19 20 AR BX CQ DO EI HS LD PW TZ VY SQW JVL HUA LSP				
25 III I IV 06 13 13 BX CE DR EG HV IN LY MI OS UW PWC MPI RAJ YWW				
24 V I IV 19 02 06 AL CM DO ED HH IK SZ TU VY WW FDC PHY KWT DLH				
23 II V I 19 04 12 BE CK DX EG HI MK NP QV RS VZ WDC QXK YTB NDF				
22 IV III V 01 13 01 AS EG DU GY IK LZ MO NW QX RV EGD UUV ODC INH				
21 IV III V 01 13 01 AS EG DU GY IK LZ MO NW QX RV EGD UUV ODC INH				
20 IV III V 25 11 10 AS EG DU GY IK LZ MO NW QX RV EGD UUV ODC INH				
19 IV I V 02 04 15 CS DR EF IN JQ KT QX BR RU VY AWD DAC YII KHW				
18 III IV I 09 09 21 AV BK CS QG HD JP LO MN UZ NX RWD XWU OWU CII				
17 II I V 24 09 05 AX CJ DY EW GD HV IN MS QR UV ORA YCH ULB BOY				
16 III II IV 24 15 14 CV DJ EX FW GD HV IZ MI QX RY GJM QME GVO BUR				
15 IV I V 19 03 14 AR BV FK GO IZ JT LR MV NP WY CTQ JIS PCQ QPR				
14 I III V 08 14 02 AL CG DG FY HK JW MS NV Q2 TU QNT ZAI YNC JPA				
13 IV I V 08 14 02 AL CG DG FY HK JW MS NV Q2 TU QNT ZAI YNC JPA				
12 IV I V 19 11 10 CS DR EF GY HS IZ JV MV PG MX VWD QME VOB KZC				
11 III V I 03 03 18 AD BI GS DU EZ FS HQ KO LM TW YEU CZL XLS AJL				
10 I V II 22 24 26 AN BQ DJ EI KV HV KR LR MS XY CQO VEZ YFK HMA				
09 III II I 09 19 12 BR CT DS EI HW IZ JV LR NO QV RLP YMK TON EGA				
08 I IV V 02 01 06 AG CV DN LL EL IT JV MY QU SZ RXJ URK ANN ZDD				
07 I V IV 06 18 10 AX BP CQ FE FI GV HJ KU MV SZ BIF CJN QNT TSM				
06 V II IV 20 01 05 BG CW DT EF JV LZ NY QR PS UX KWD MFT ITD GJD				
05 IV I V 07 09 15 AR DS CF DE GQ HI JK LS QX FWD ITV BOL QZP				
04 V IV III 25 15 09 BEQ GM HI IO JS KZ PR UV VWD QME VOB KZC				
03 V III I 06 05 10 DV DR EX FY HI JM KZ LQ MS PU GDM INT COF THR				
02 II V I 23 09 21 AP CX DV EU FT GS HI KM LZ NR TSW USU CFL VUU				
01 III I II 16 12 02 AD BY CM DR GI KV LQ RW SZ TU KDT UNT KRL LUB				

- ▶ Tag = jour
- ▶ Walzenlage = position des rotors
- ▶ Ringstellung = Position des anneaux (chaque rotor)
- ▶ Steckerverbindungen = connexions enfichables
- ▶ Kenngruppen = groupe clés

NOTION DE PROTOCOLE

- ▶ Chaque message est précédé d'un mot de 3 lettres aléatoires, répété.
- ▶ Ces 3 lettres (en clair) donnent la position des rotors à utiliser pour déchiffrer la suite du message.

Observation :

Le message-clé est **répété**.

COMMENT EXPLOITER CECI ?

Stratégie générale :

- ▶ Le nombre de clef est trop grand (2^{67}) ;
- ▶ Il faut donc un moyen pour récupérer une **partie** de la clef **indépendamment** de l'autre partie.
- ▶ Dans notre cas : on cherche la **position** des rotors, et sans se préoccuper du tableau de connexions.

Il nous faut donc un **critère** distinguant sur ce que l'on connaît (une propriété observable et vraie lorsque les rotors sont à la bonne position), qui ne dépende pas du tableau de connexion.

 Objectif du TD sur Enigma !

LA CRYPTANALYSE PENDANT LA GUERRE

- ▶ Constructions de machines automatiques (bombes de Rejewski) permettant de trouver la clef du jour en 2 heures.

En 1938, les allemands renforcent la sécurité d'Enigma :

- ▶ ajout de 2 nouveaux rotors
- ▶ Les connexions passent de 6 à 10

Abandon du message-clef...

LES CRYPTANALYSTES DU BLETCHLEY PARK



- ▶ Familiarisation avec les méthodes polonaises.
- ▶ Nouveaux **raccourcis** à la recherche.
- ▶ Exploitation des “**cillies**” (lettres se suivant au tableau, initiales de la petite amie de l’opérateur,...)

LA CONTRIBUTION D'ALAN TURING

Casser ENIGMA **sans utiliser** l'hypothèse de la **répétition** du message-clé.



- ▶ Méthode des **mots probables** (“cribs”)

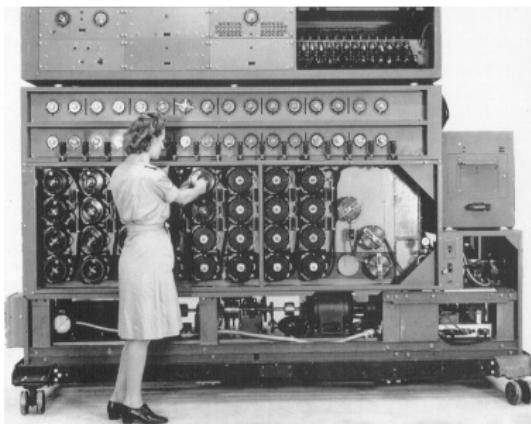
→ 1 054 560 possibilités.

Alan Turing
1912-1954

LES BOMBES DE TURING

Automatisation de la recherche de la clé.

20 280 essais/s pour les plus rapides (50 s pour retrouver la clé).



RÉFÉRENCES

- ▶ "*L'histoire des codes secrets*", Simon Singh.
- ▶ "*Handbook of Applied Cryptography*", Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone (livre gratuit en version électronique) <http://cacr.uwaterloo.ca/hac/>
- ▶ "*Cryptographie : théorie et pratique*", D. Stinson (en ligne)
[http://www.icst.pku.edu.cn/course/Cryptography/CryptographyTheoryandpractice\(3ed\).pdf](http://www.icst.pku.edu.cn/course/Cryptography/CryptographyTheoryandpractice(3ed).pdf)
- ▶ "*Introduction to Modern Cryptography*", J. Katz and Y. Lindell.
- ▶ "*Understanding Cryptography*", C. Paar and J. Pelzl.