ENIGMA

Christina Boura

christina.boura@uvsq.fr

2 février 2018

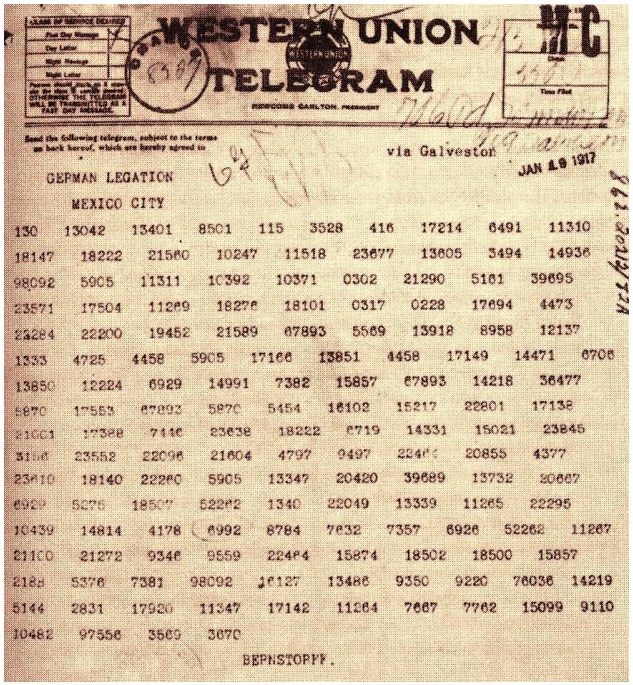
La cryptographie au début du 20^{e} siècle

- **Fin du 19^{e} siècle**
  - Chiffre de Vigenère brisé par Babbage et Kasiski.
  - Situation désastreuse pour la cryptographie.

- Marconi invente la télégraphie sans fil.
  - Les messages atteignent aussi bien l'ennemi que le destinataire choisi.
  - Besoin d'un chiffrement fort.

La cryptographie pendant la Première Guerre Mondiale

- Absence totale de chiffres efficaces.
- Chiffrements allemands crypnanalysés “efficacement” par les alliés (ex. chiffre ADFGVX).
- La cryptanalyse par les Britanniques du télégramme de Zimmermann, a entraîné les États-Unis dans la guerre.


WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10462 97556 3569 3070

BEPNSTORFF.

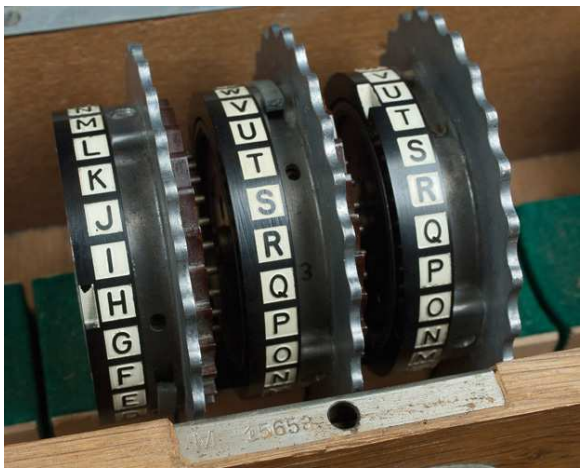
Enigma

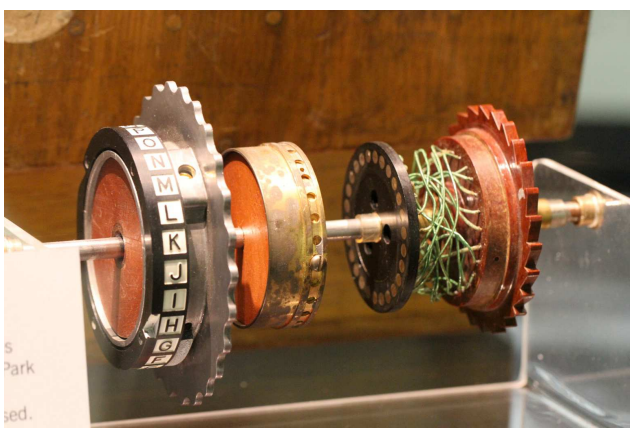
- Inventée par l'ingénieur allemand Arthur Scherbius en 1918.
- Modèle A de la machine présenté à Berlin en 1923 (prix éq : 30000 euros)
- D'autres modèles ont été utilisés par l'armée et la marine allemande.

Parties principales :

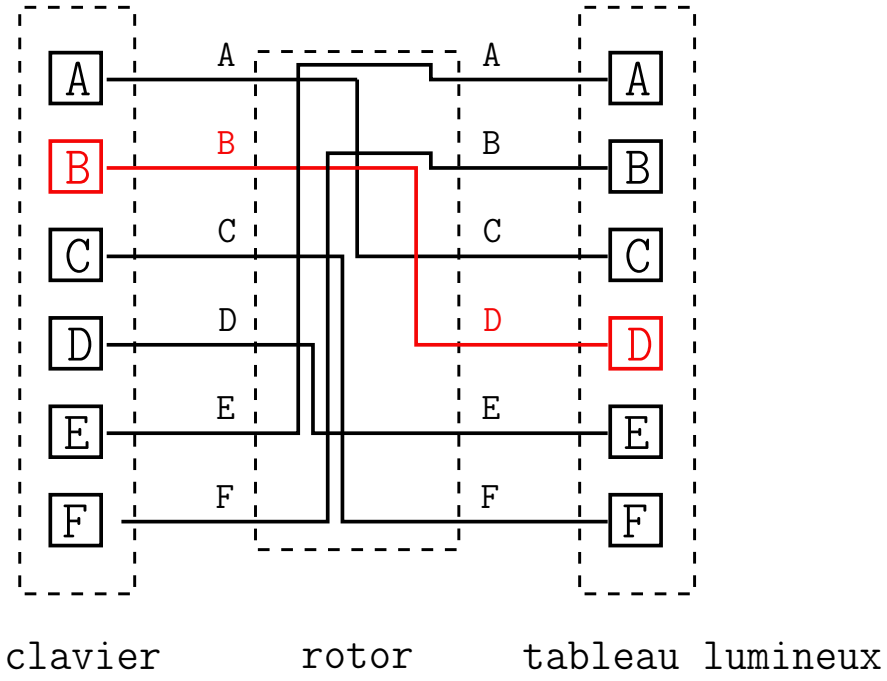
- Clavier
- Tableau lumineux
- Rotors
- Tableau des connexions
- Réflecteur

Les rotors





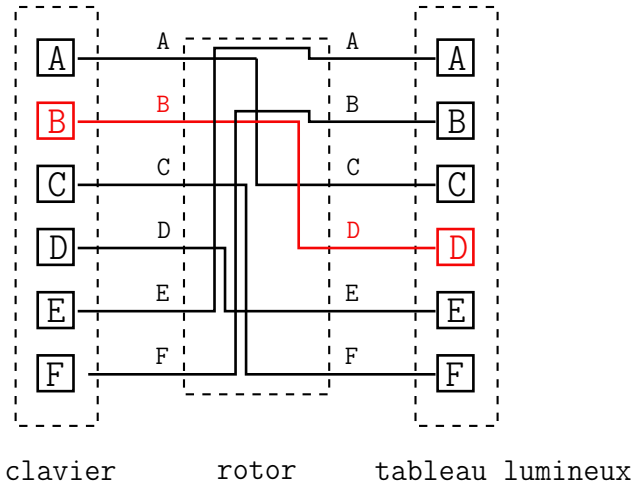
Machine avec un rotor

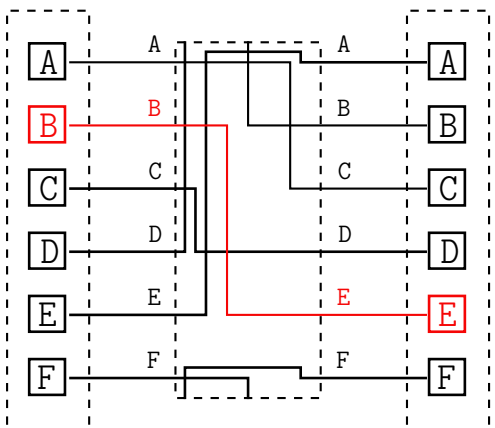


- Substitution monoalphabétique

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

On tourne le rotor d'une position après chaque lettre

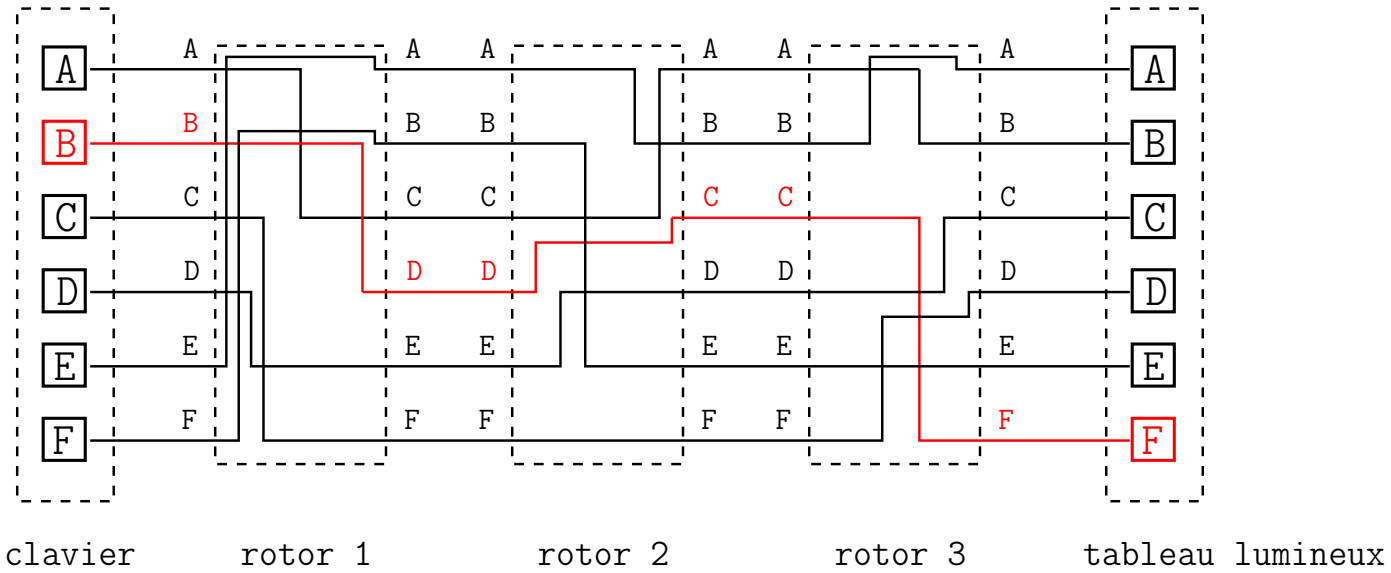




Substitution avec 26 alphabets différents

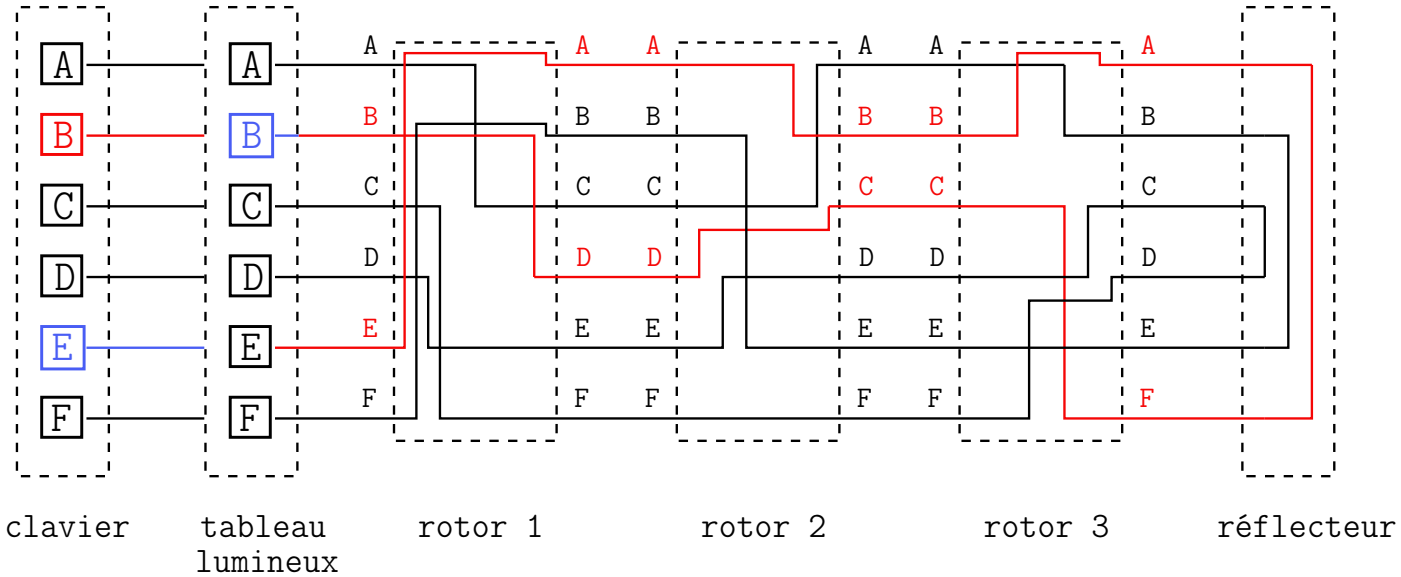
1.	A	B	C	D	E	F
	C	D	F	E	A	B
2.	A	B	C	D	E	F
	C	E	D	F	A	B
3.	A	B	C	D	E	F
	D	C	E	F	A	B
4.	A	B	C	D	E	F
	B	D	E	F	A	C
5.	A	B	C	D	E	F
	C	D	E	F	B	A
6.	A	B	C	D	E	F
	C	D	E	A	F	B

Machine à trois rotors



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

Machine à trois rotors avec réflecteur

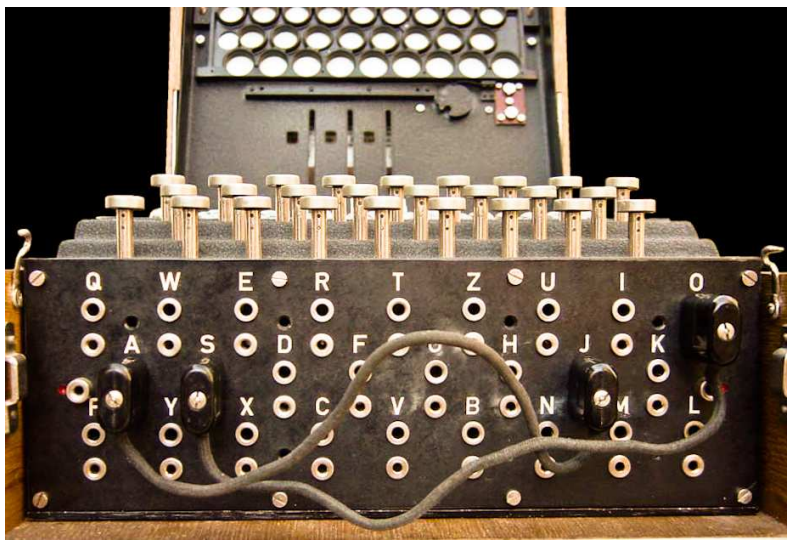


Chiffrement et déchiffrement sont des processus identiques.

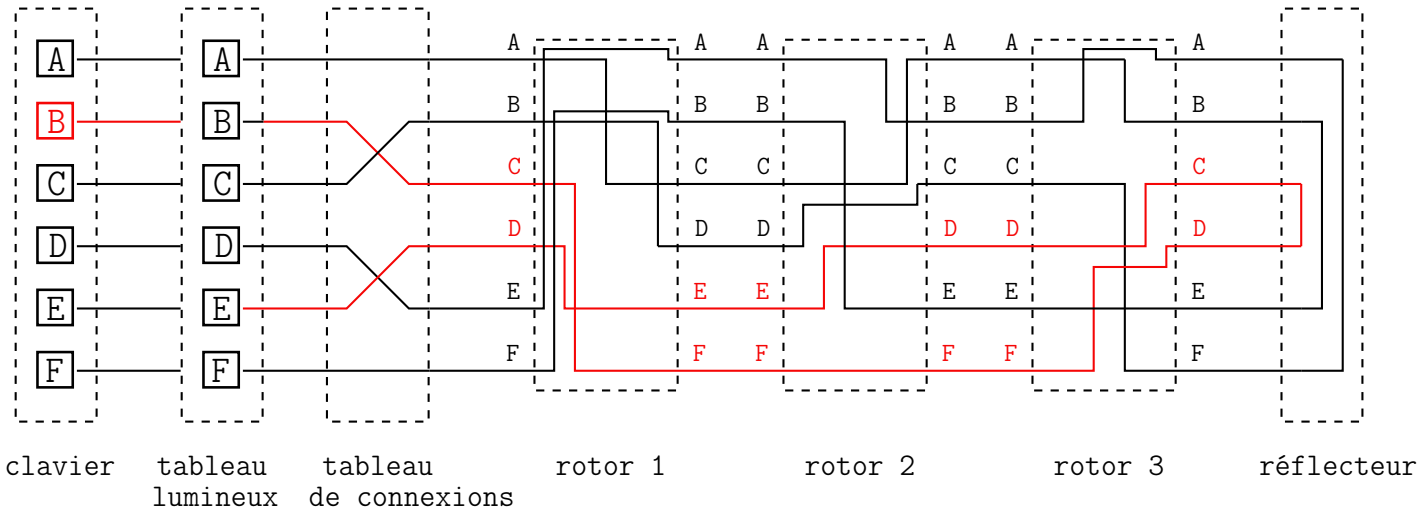
Clé secrète : ordre des rotors + positions de départ des rotors.

$$6 \times 26^3 = 105\,456 \text{ possibilités.}$$

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 au début de la guerre

Nombre de clés secrètes :

3 rotors choisis parmi 5	10 possibilités
Ordre de trois rotors	6 possibilités
Position initiale des rotors	$26^3 = 17\,576$ possibilités
Tableau de connexions	$150\,738\,274\,937\,250$ possibilités
(10 paires de lettres)	

Au total : $\approx 2^{67}$ possibilités.

Enigma paraît invincible

- 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 des codes

GEHEIM! STAUNTON JULI 1940

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	IV V I	24 17 13	AQ CT DV EN FW GP IX JS KR LO	BZA KZO SIK VMO
30	II V III	22 11 01	AL BS EU FR GM IO PY QZ TW VX	ZUF SIC FDH BKU
29	V III I	09 25 21	AK BU CI DE GQ HM LT OZ RV WY	AFU WWW TSM UVX
28	IV II III	12 07 08	BW DZ EY FR GT HJ IV LS NQ OX	EPK PLF PIR NCY
27	IV III II	02 03 15	AC BP EZ FX GV HK LT MR NU QW	ZON KOV FCE CDJ
26	IV II III	19 20 20	AK BX CQ DO EI HS LR PW TZ VY	SQW JVL MUA LSP
25	III I IV	06 13 13	BX CE DR FG HV IN LY MT OS UW	PWC MPI RAJ VWW
24	V I IV	19 02 06	AL CM DO EP HN IK SZ TU VY WX	FPC PHY KWY RLH
23	II V I	10 04 12	BE CK DX FG HI MO NP QU RS VZ	WDS QXB YYB NDF
22	I III V	01 13 01	AS BC DU GY IK LZ MO NW QX RV	EGD UUY ODC INE
21	IV V I	22 01 01	AF CX DR GN HV JL KZ OW QS UY	LFE RJG ROD GFU
20	I III V	25 11 10	AP BE FG IZ KT LN OR QX UW VY	YMY BFL FDS DBG
19	IV I V	02 04 15	CS DW EF IN JQ KT OX PZ RV UY	AVD OAG YZI XKV
18	III IV I	08 09 21	AY BK CS GQ HR JP LO MN UZ WX	NPU XWU OWU CTI
17	II I V	26 09 05	AX CJ DY EW GP HO IN MS QR UV	ORH YCH ULT BQY
16	III II IV	24 15 14	CV DJ EK FW GP HS IZ MT QX RY	GJH QHK GVO BUR
15	IV I V	13 03 16	AE BV FK GO IZ JT LR MX NP WY	QTQ JIS PCQ QPB
14	I III V	08 14 02	AL CP DG FY HK JW MS NV QZ TU	ONI ZAI YNC JPA
13	IV I V	10 06 10	CZ DR EF GT HS IU LO MV PQ WX	VXD QEM VOS ECZ
12	I II V	14 21 06	AK BD CL EJ FI GX OR PZ QT VW	OWC EZZ QXC CAT
11	III V I	03 03 18	AP BI CS DU EZ FN HQ KO LM TW	YEU CZL KLS AJL
10	I V II	22 24 26	AN BQ DJ EI GU HV KR LP MS XY	CQQ VEZ YFK NWA
09	III II I	05 19 12	BR CT DS EU HW IZ JP LX NO QV	RLP YWX IQN EGA
08	I IV V	02 01 06	AG CV DH EL FR IT JY MW QU SZ	RXJ URE ANN ZDD
07	I IV V	06 15 10	AX BP CQ DR FI GY HJ KU MV SZ	BIF CJM ONT TSM
06	V II IV	20 01 05	BG CW DI EF JV LZ NY OR PS UX	KWR MFT ITD GJD
05	IV V I	07 06 12	AI CU DT GS HK JQ LM NV PZ XY	FYB ITV BOL YID
04	V IV III	25 15 09	AF EQ GW HX IO JN KZ MS PR UY	CFY NRA CNL MVE
03	V III I	06 05 10	AV DR EX FY HI JM KZ LQ NS PU	GCN TBT OOW TNH
02	II V I	23 09 21	AP CX DV EU FT GS HI KM LZ NR	TSW USU CFL VVU
01	III I II	16 12 02	AO BY CM DH GI KV LQ RW SZ TU	EDT UMT ERL LUB

1. Tableau des connexions : `(A, L), (C, F), (J, Y), (K, N), (P, W), (T, X)`
2. Ordre des rotors : `II, III, I`
3. Positions de départ des rotors : `G-V-R`

Observation principale

- Utilisation des réglages du jour pour transmettre un nouveau *message-clé*, unique pour chaque message.
- Message-clé : orientation des rotors, par exemple : `VRD`

Observation cruciale :

Le message-clé est tapé deux fois.

Exemple : `VRDVRD`

Établissement des relations

	1re	2e	3e	4e	5e	6e
1er message	L	O	K	R	G	M
2e message	M	V	T	X	Z	E
3e message	J	K	T	M	P	E
4e message	D	V	P	P	Z	X

Établissement des relations

	1re	2e	3e	4e	5e	6e
1er message	L	O	K	R	G	M
2e message	M	V	T	X	Z	E
3e message	J	K	T	M	P	E
4e message	D	V	P	P	Z	X

1re lettre	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4re lettre	P M RX

Établissement des relations

	1re	2e	3e	4e	5e	6e
1er message	L	O	K	R	G	M
2e message	M	V	T	X	Z	E
3e message	J	K	T	M	P	E
4e message	D	V	P	P	Z	X

1re lettre	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4re lettre	FQHPLWOGBMVRXUYCZITNJEASDK

Les chaînes de Rejewski

1re lettre	ABCDEFGHIJKLMNOPQRSTUVWXYZ
4re lettre	FQHPLWOGBMVRXUYCZITNJEASDK

A → F → W → A	3 liens
B → Q → Z → K → V → E → L → R → I → B	9 liens
C → H → G → O → Y → D → P → C	7 liens
J → M → X → S → T → N → U → J	7 liens

(AFW)(BQZTVELRI)(CHSOYDPC)(JMXGKNUJ)

S'affranchir du tableau de connexions

Par le tableau de connexions

Avant : S $\leftrightarrow$ G

Après : T $\leftrightarrow$ K

A $\rightarrow$ F $\rightarrow$ W $\rightarrow$ A

B $\rightarrow$ Q $\rightarrow$ Z $\rightarrow$ K $\rightarrow$ V $\rightarrow$ E $\rightarrow$ L $\rightarrow$ R $\rightarrow$ I $\rightarrow$ B

C $\rightarrow$ H $\rightarrow$ G $\rightarrow$ O $\rightarrow$ Y $\rightarrow$ D $\rightarrow$ P $\rightarrow$ C

J $\rightarrow$ M $\rightarrow$ X $\rightarrow$ S $\rightarrow$ T $\rightarrow$ N $\rightarrow$ U $\rightarrow$ J

S'affranchir du tableau de connexions

Par le tableau de connexions

Avant : S $\leftrightarrow$ G

Après : T $\leftrightarrow$ K

A $\rightarrow$ F $\rightarrow$ W $\rightarrow$ A

B $\rightarrow$ Q $\rightarrow$ Z $\rightarrow$ T $\rightarrow$ V $\rightarrow$ E $\rightarrow$ L $\rightarrow$ R $\rightarrow$ I $\rightarrow$ B

C $\rightarrow$ H $\rightarrow$ S $\rightarrow$ O $\rightarrow$ Y $\rightarrow$ D $\rightarrow$ P $\rightarrow$ C

J $\rightarrow$ M $\rightarrow$ X $\rightarrow$ G $\rightarrow$ K $\rightarrow$ N $\rightarrow$ U $\rightarrow$ J

Le nombre de liens dans chaque chaîne ne dépend que des réglages des rotors !

Recherche de la clé

Nombre total de positions des rotors :

dispositions des rotors $+$ orientations $\longrightarrow 6 \times 26^3 = 105\,456$.

- Répertorier les longueurs des $105\,456$ chaînes (1 an de travail).
- Intercepter des messages-clés chiffrés.
- Dresser le tableau de relations.
- Calculer des chaînes formées des lettres 1-4, 2-5 et 3-6.
- Trouver à quelle clé elles appartiennent (recherche dans le répertoire).

Établir les connexions du tableau

A L L I V E E N B E L R I N

Établir les connexions du tableau

A L L I V E E N B E L R I N

Établir les connexions du tableau

A R R I V E E N B E R L I N

- L $\leftrightarrow$ R
- A, I, V, E, B et N ne sont pas permutées.

Automatisation de l'attaque et ses limites

- Construction des machines, baptisées *bombes* pour automatiser la cryptanalyse.
- Les bombes de Rejewski étaient capables de trouver la clé du jour en 2 heures.

En **1938** les Allemands renforcent la sécurité d'Enigma.

- Ajout de 2 nouveaux rotors.
- Les connections sur le tableau passent de 6 à 10.

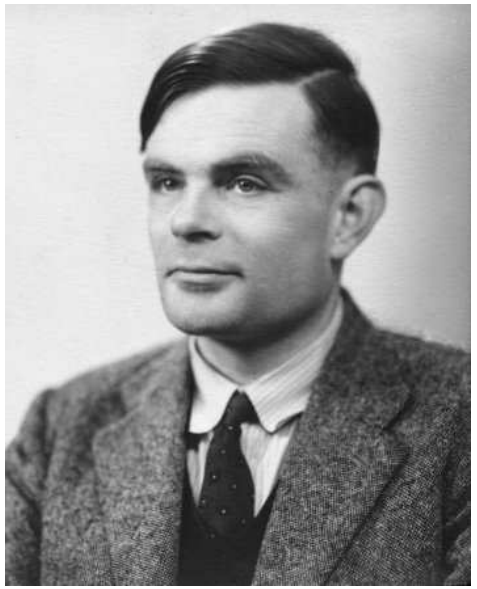
Les cryptanalystes du Bletchley Park

- 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.

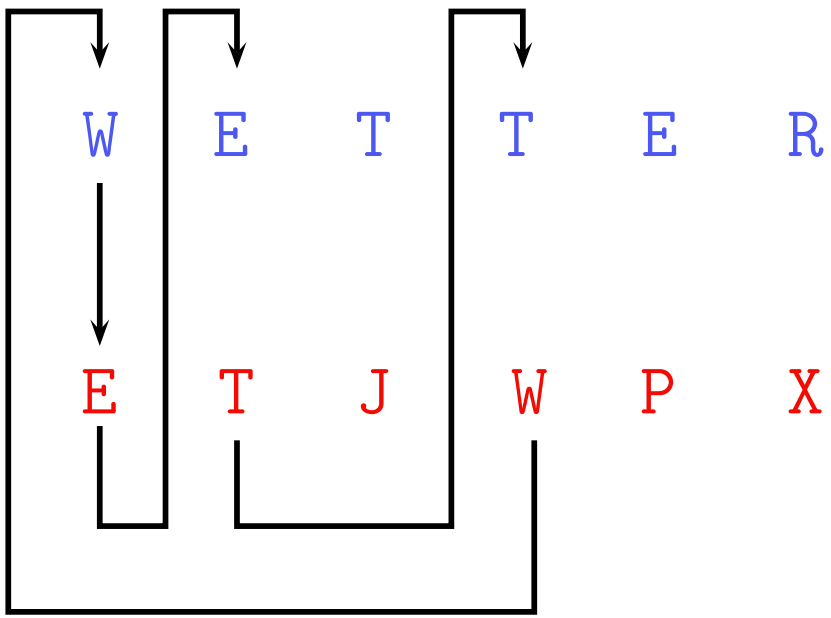
- Méthode des mots probables ("cribs")



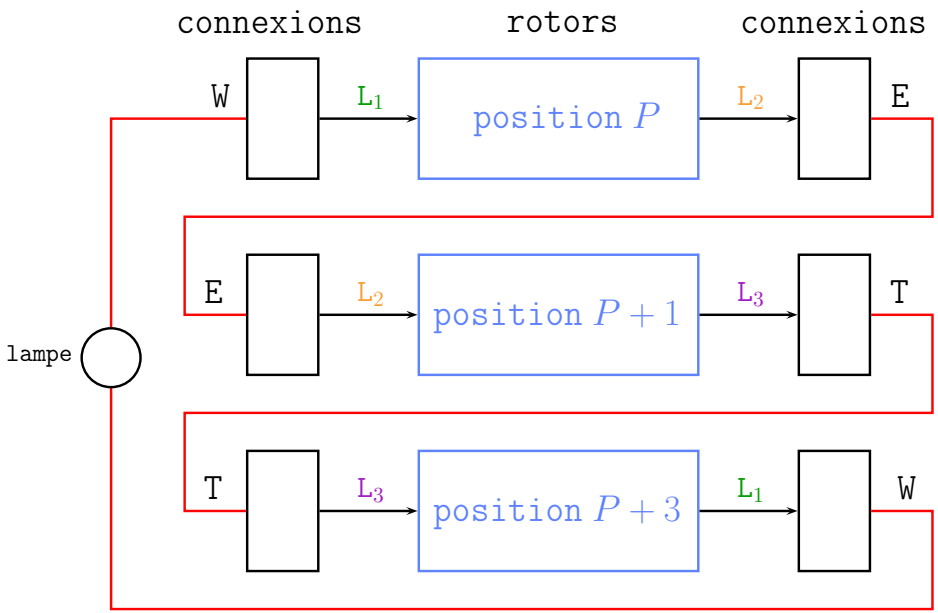
Alan Turing
1912-1954

Méthode des mots probables

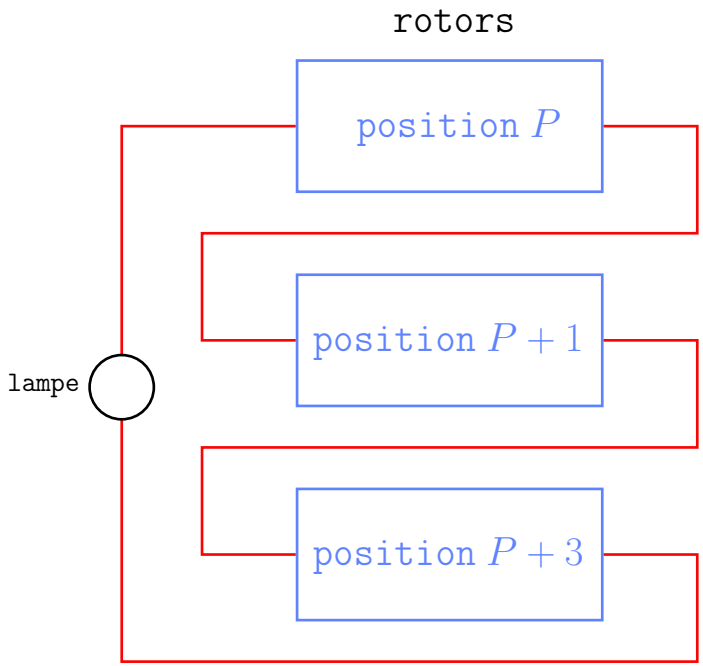
Message Clair : WETTER
Message Chiffré : ETJWPX



Recherche de la position des rotors



S'affranchir du tableau de connexions



Essayer les $26^3 = 17\,576$ positions possibles pour chacun des 60 choix de rotors.

$\rightarrow$ **1 054 560** possibilités.

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).