Journée ISN-EPI — 12 mars 2015

Enigma

Présentation & Éléments de cryptanalyse

Jérémie Detrey

Jeremie.Detrey@loria.fr

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).
- Octobre 1938 : mécanisation de l'attaque polonaise par la bomba kryptologiczna.

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).
- Octobre 1938 : mécanisation de l'attaque polonaise par la bomba kryptologiczna.
- 25 juillet 1939 : début de la seconde guerre mondiale.
  L'armée allemande utilise Enigma pour chiffrer ses communications.

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).
- Octobre 1938 : mécanisation de l'attaque polonaise par la bomba kryptologiczna.
- 25 juillet 1939 : début de la seconde guerre mondiale.
  L'armée allemande utilise Enigma pour chiffrer ses communications.
- Août 1939 : les Polonais communiquent leur cryptanalyse d'Enigma aux Français et aux Anglais.

Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).
- Octobre 1938 : mécanisation de l'attaque polonaise par la bomba kryptologiczna.
- 25 juillet 1939 : début de la seconde guerre mondiale.
  L'armée allemande utilise Enigma pour chiffrer ses communications.
- Août 1939 : les Polonais communiquent leur cryptanalyse d'Enigma aux Français et aux Anglais.
- Fin 1939 : Alan Turing développe la bombe à Bletchley Park, pour contrer les améliorations allemandes apportées à la machine.

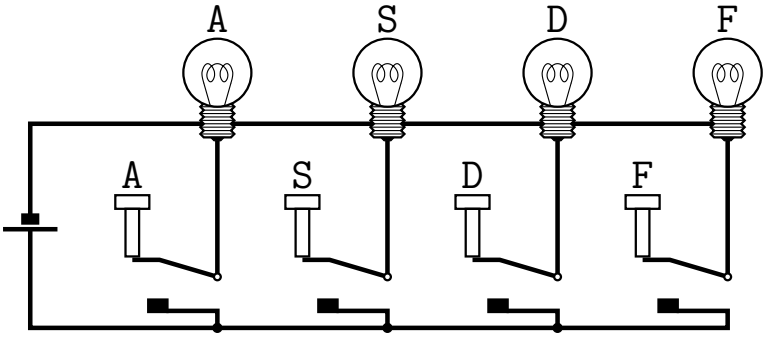
Rapide historique

- 1918 : création de la machine Enigma par l'ingénieur allemand Arthur Scherbius.
- 1925 : première version militaire d'Enigma, utilisée par la marine allemande.
- 1932 : premiers messages décryptés par le Bureau du Chiffre Polonais (Marian Rejewski, Jerzy Różycki et Henryk Zygalski).
- Octobre 1938 : mécanisation de l'attaque polonaise par la bomba kryptologiczna.
- 25 juillet 1939 : début de la seconde guerre mondiale.
  L'armée allemande utilise Enigma pour chiffrer ses communications.
- Août 1939 : les Polonais communiquent leur cryptanalyse d'Enigma aux Français et aux Anglais.
- Fin 1939 : Alan Turing développe la bombe à Bletchley Park, pour contrer les améliorations allemandes apportées à la machine.
- 1944-1945 : 200 à 300 bombes travaillent en permanence pour déchiffrer les communications allemandes (Ultra).

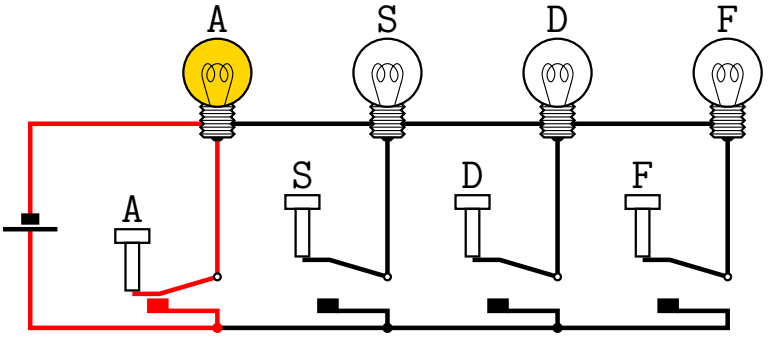
Vue d'ensemble

Photo © Christie's 2013

Clavier et ampoules



Clavier et ampoules



Vue d'ensemble

Photo © Christie's 2013

Rotors

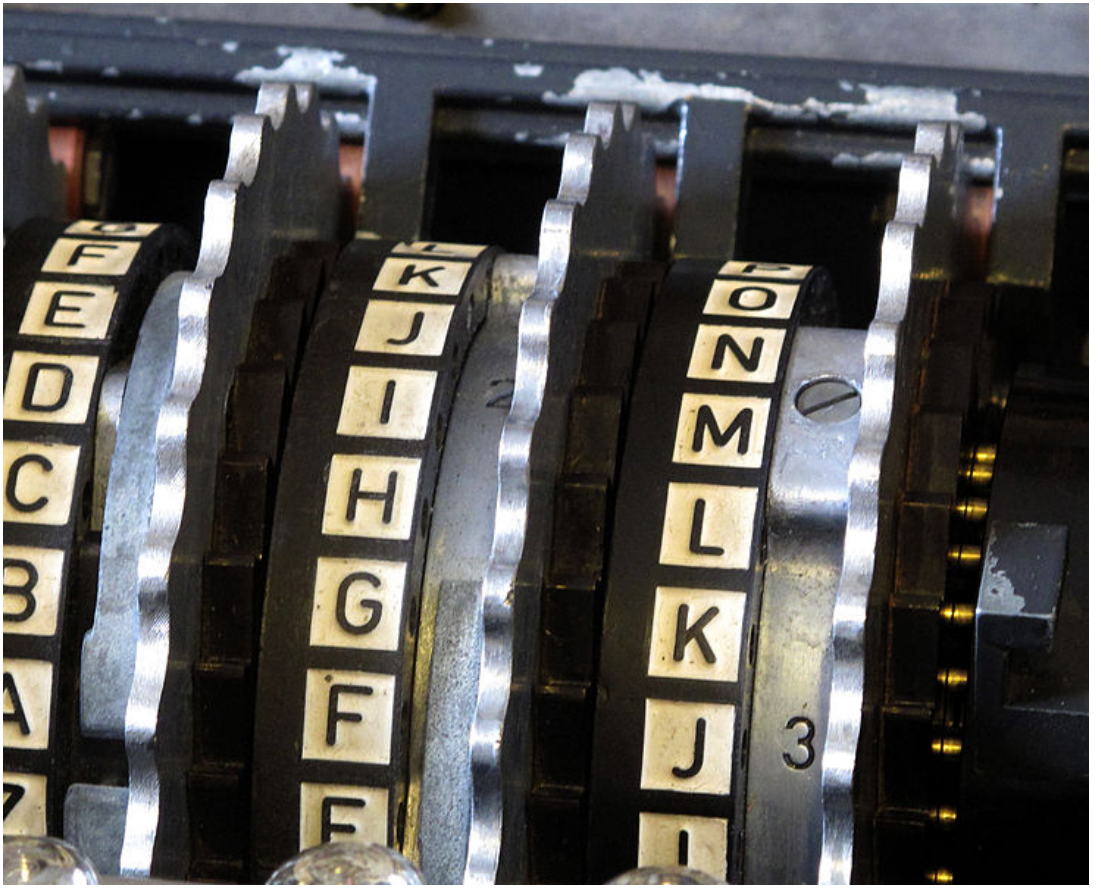
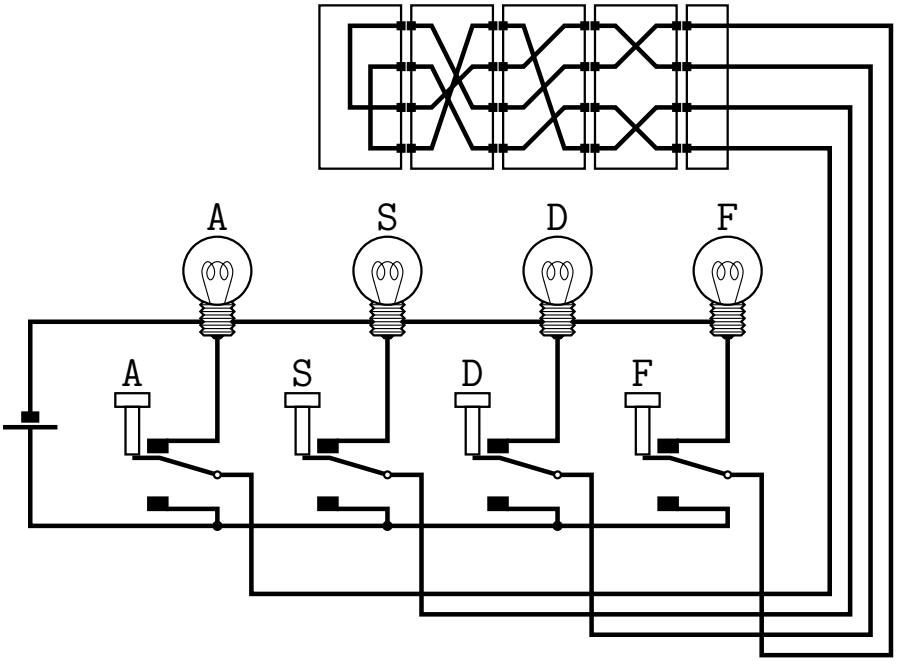
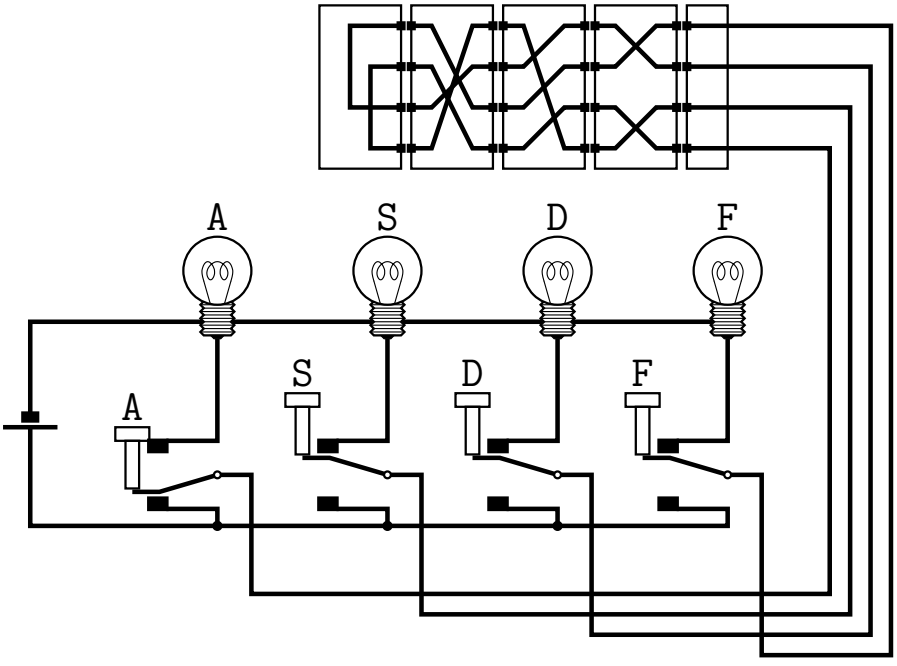


Photo © User:TedColes / Wikimedia Commons

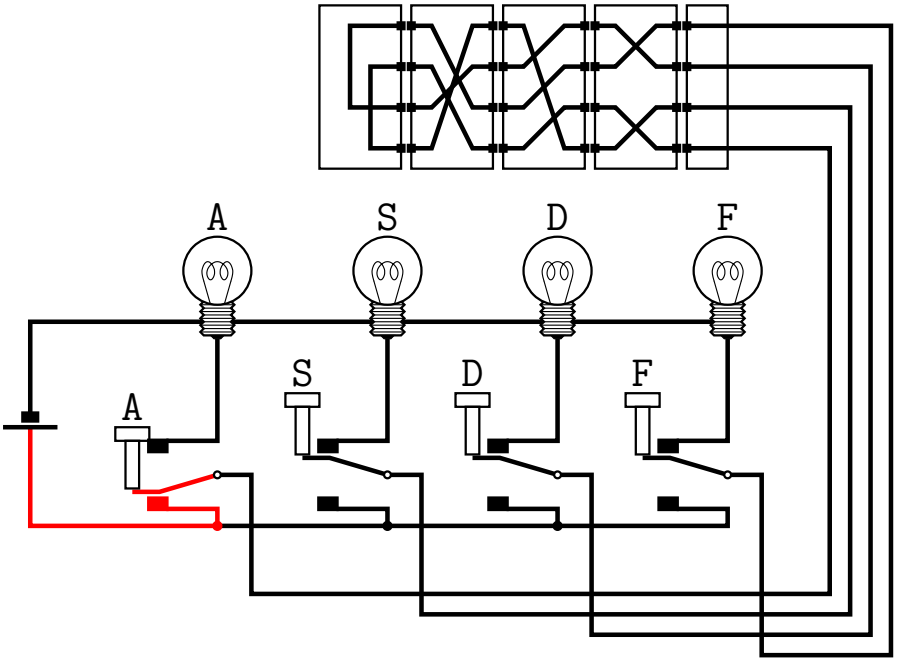
Rotors



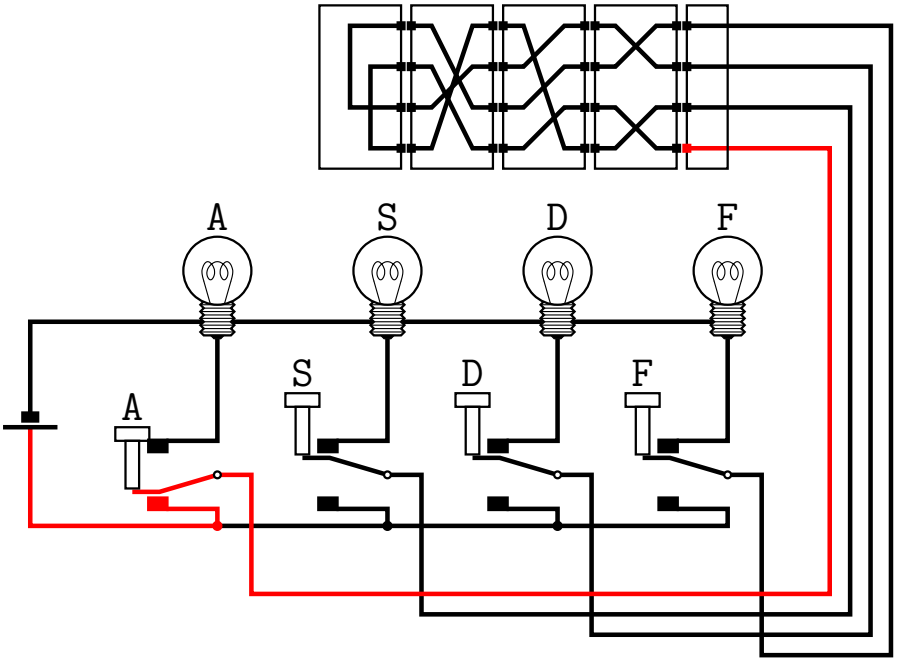
Rotors



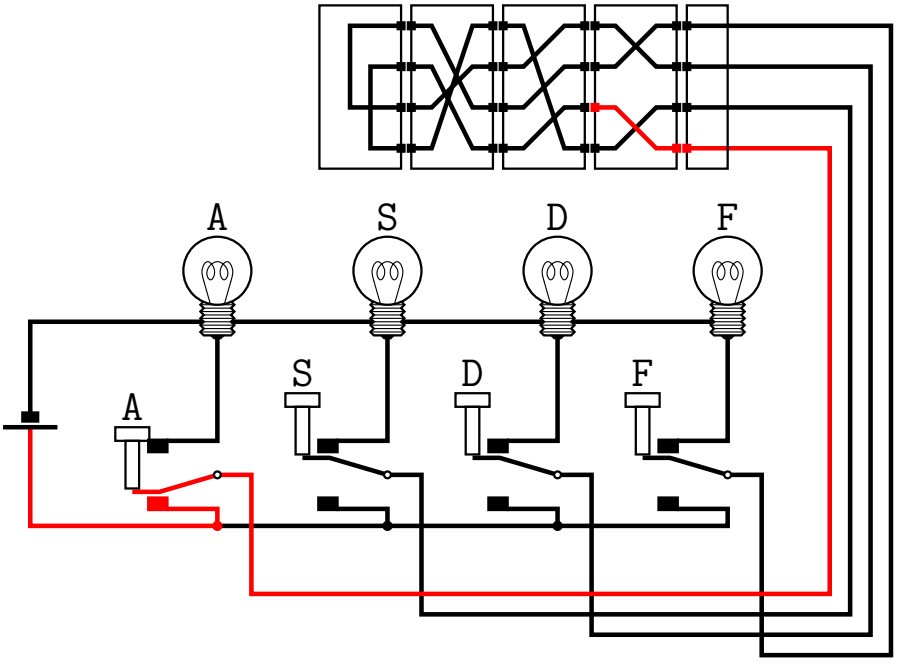
Rotors



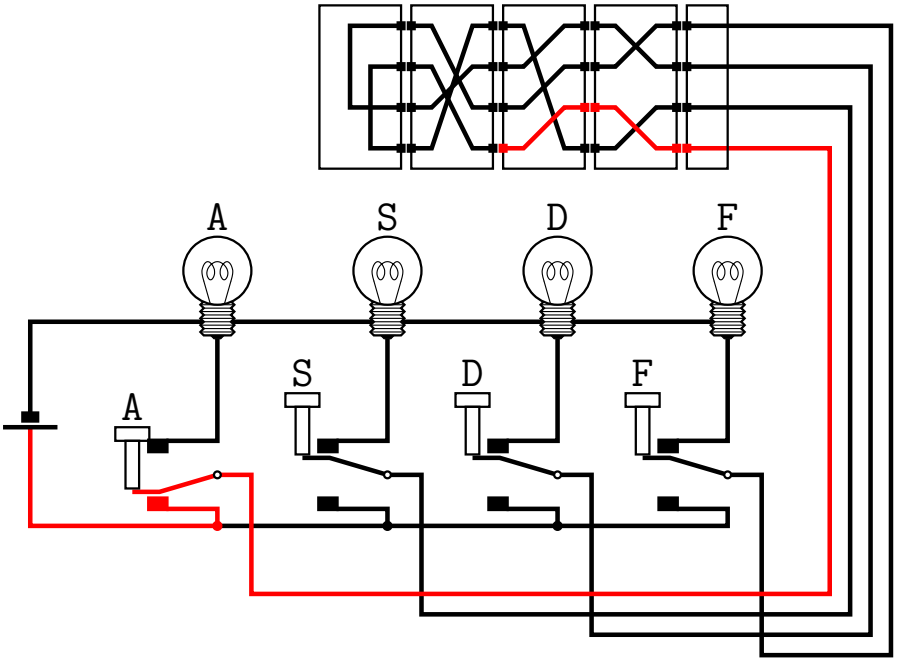
Rotors



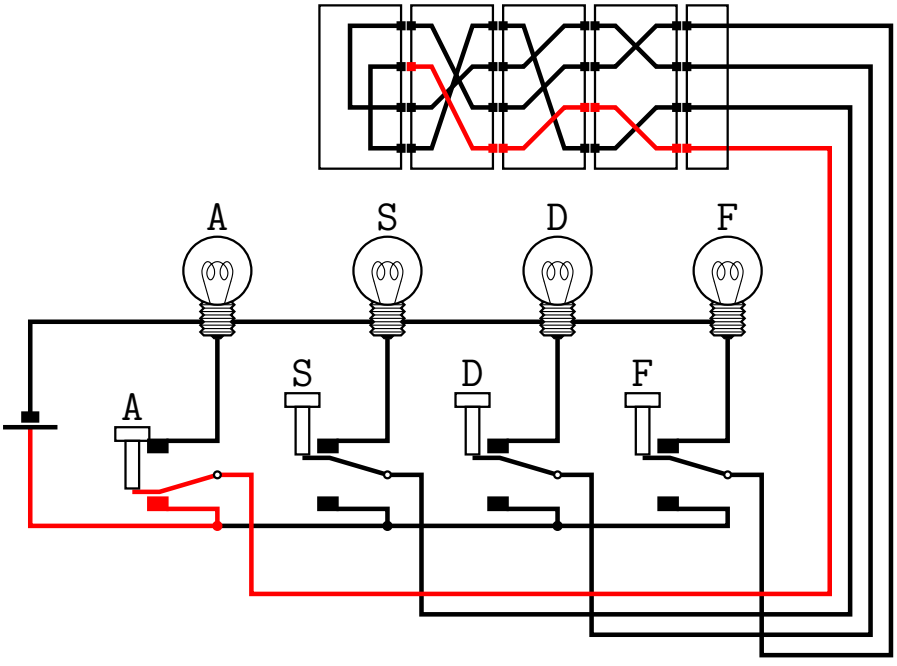
Rotors



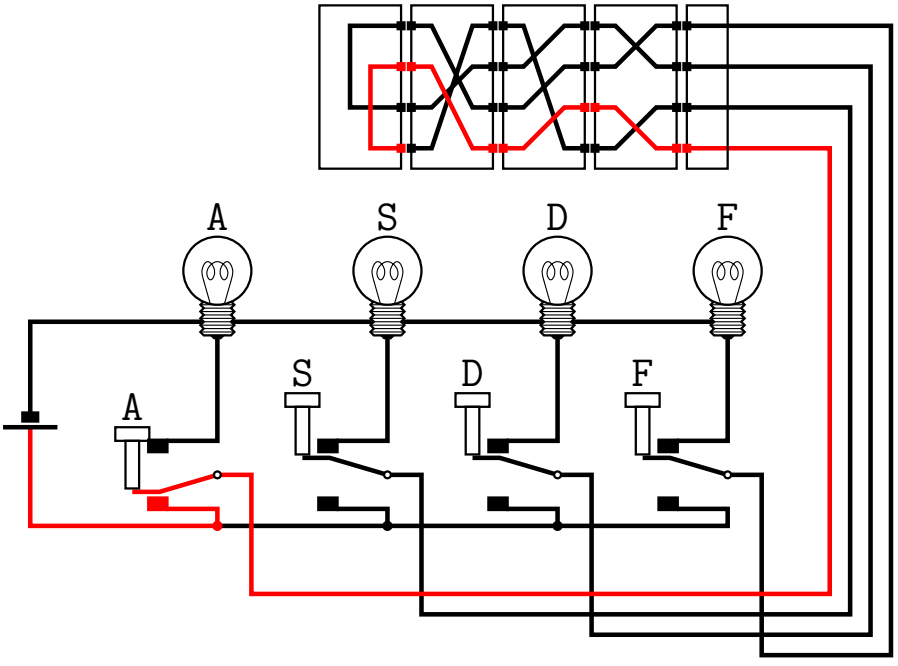
Rotors



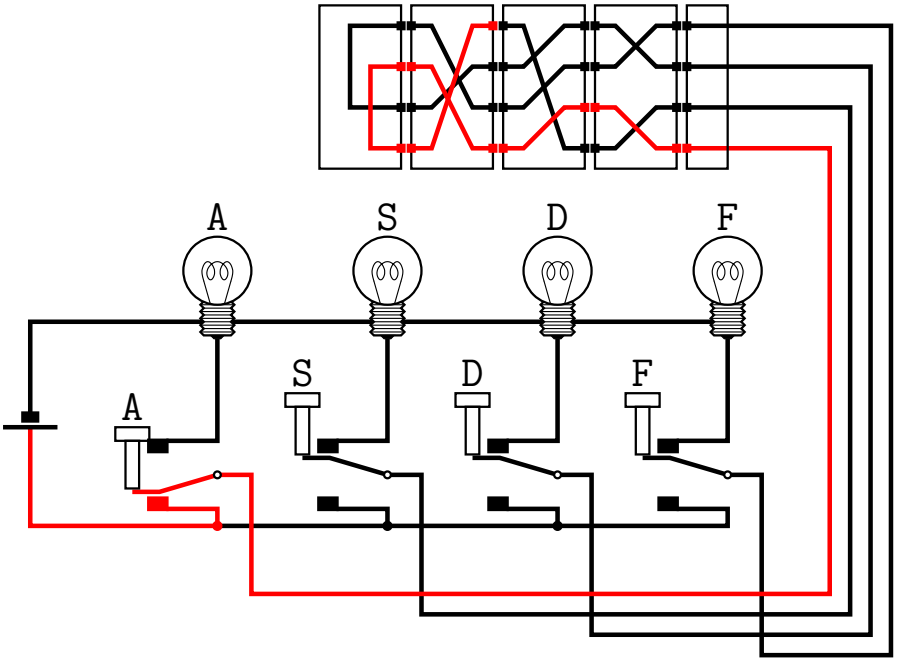
Rotors



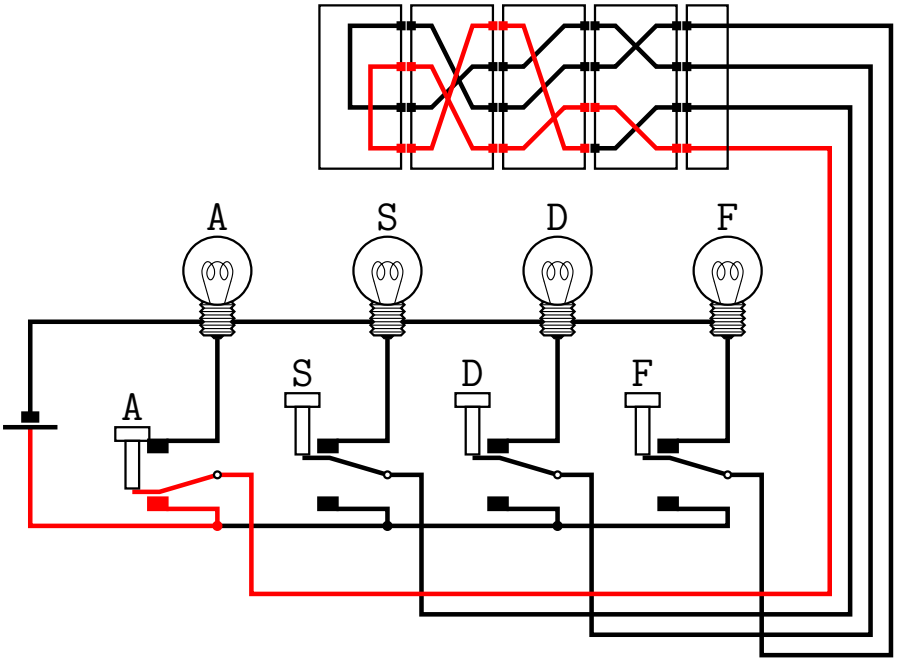
Rotors



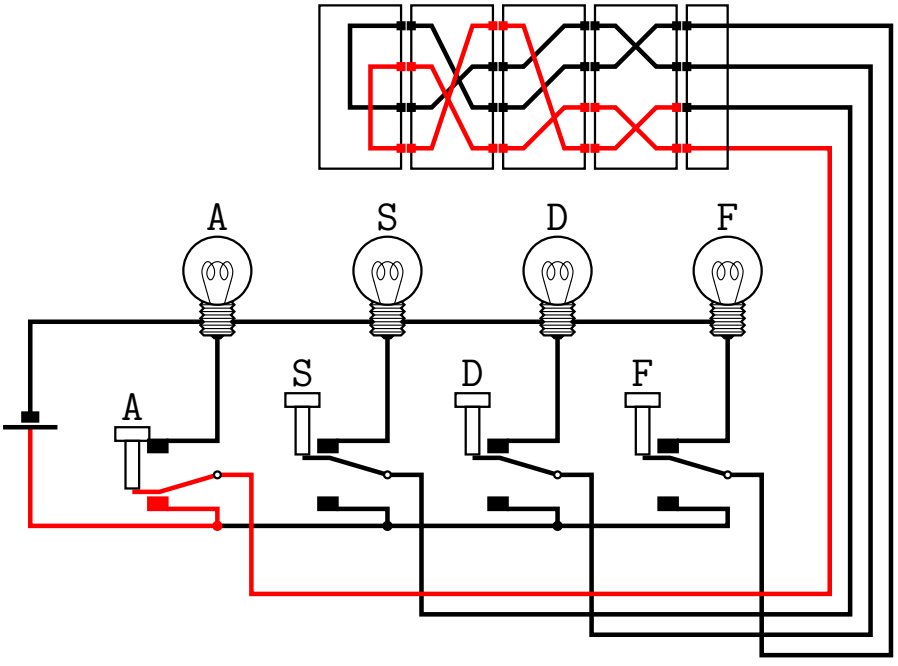
Rotors



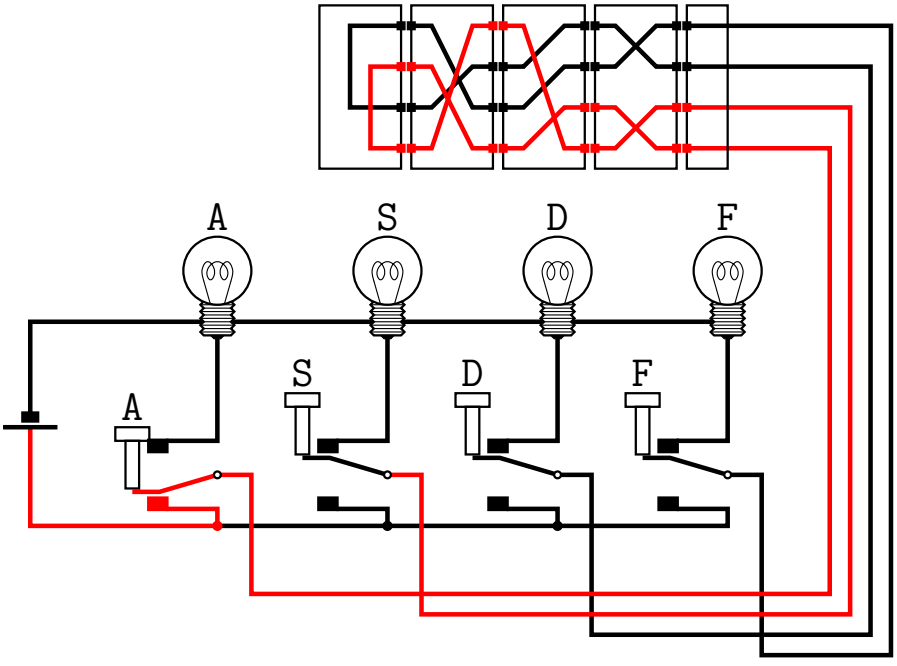
Rotors



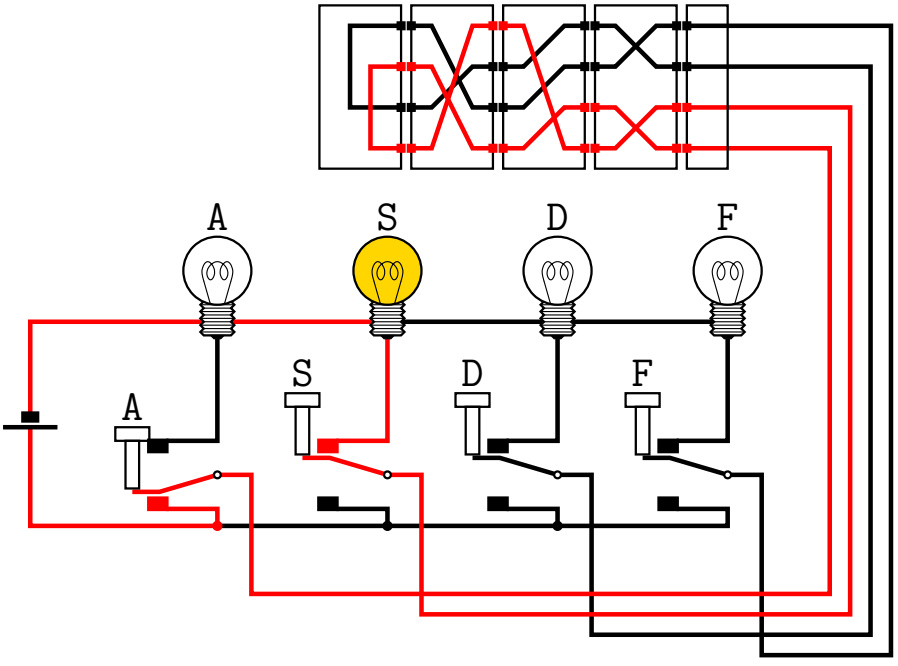
Rotors



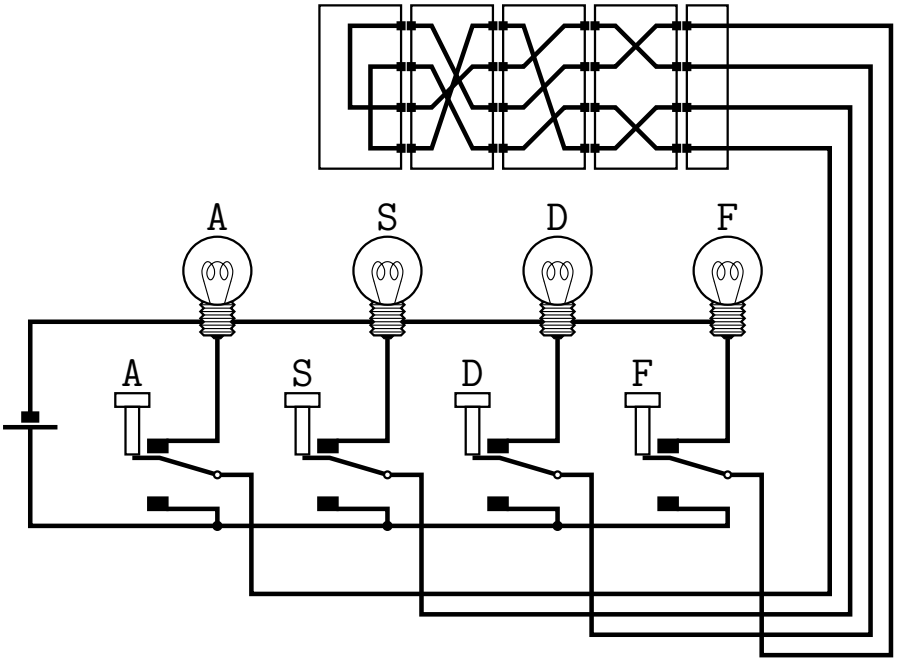
Rotors



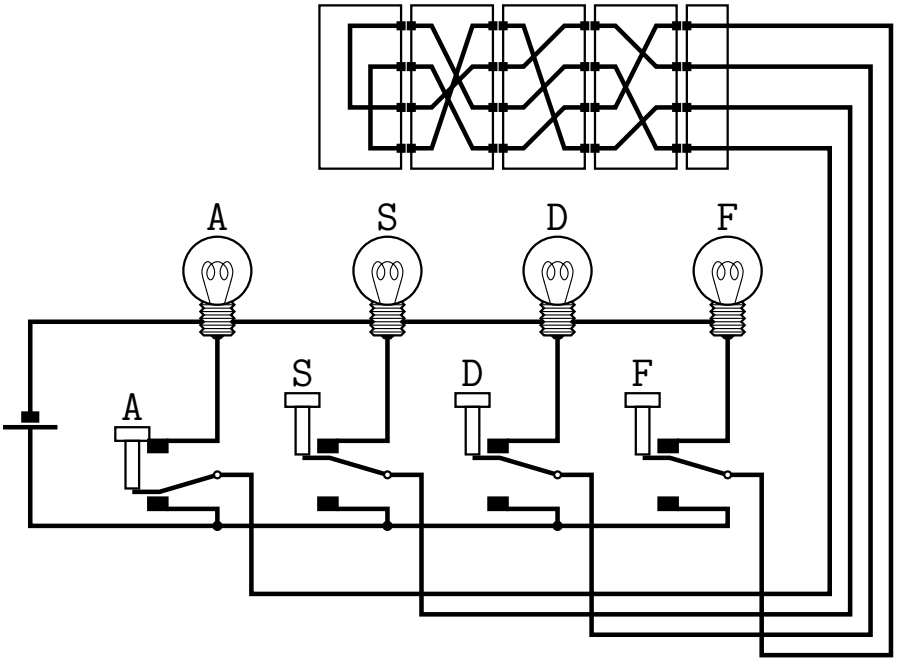
Rotors



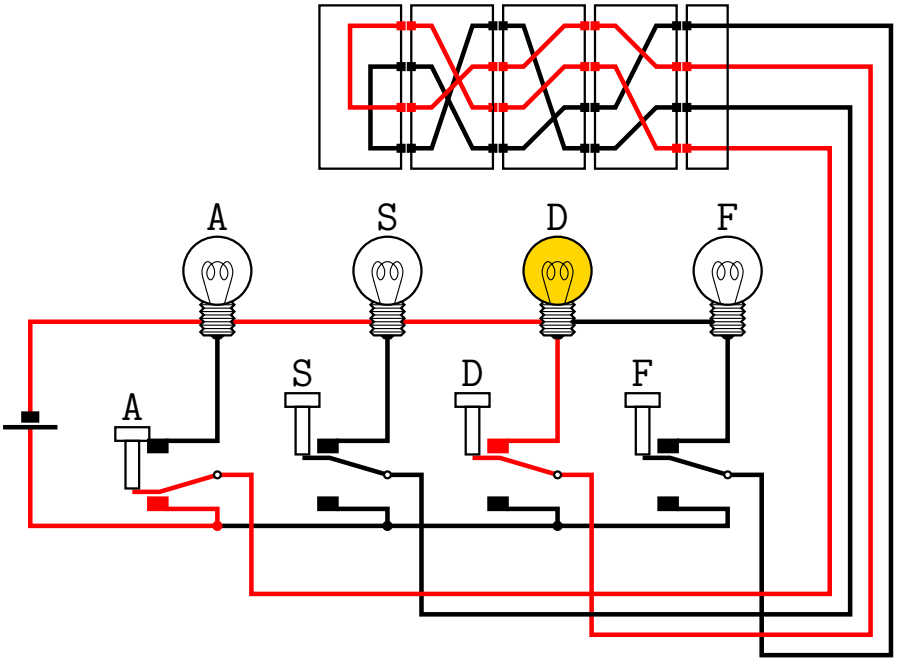
Rotors



Rotors



Rotors



Rotors (détail)

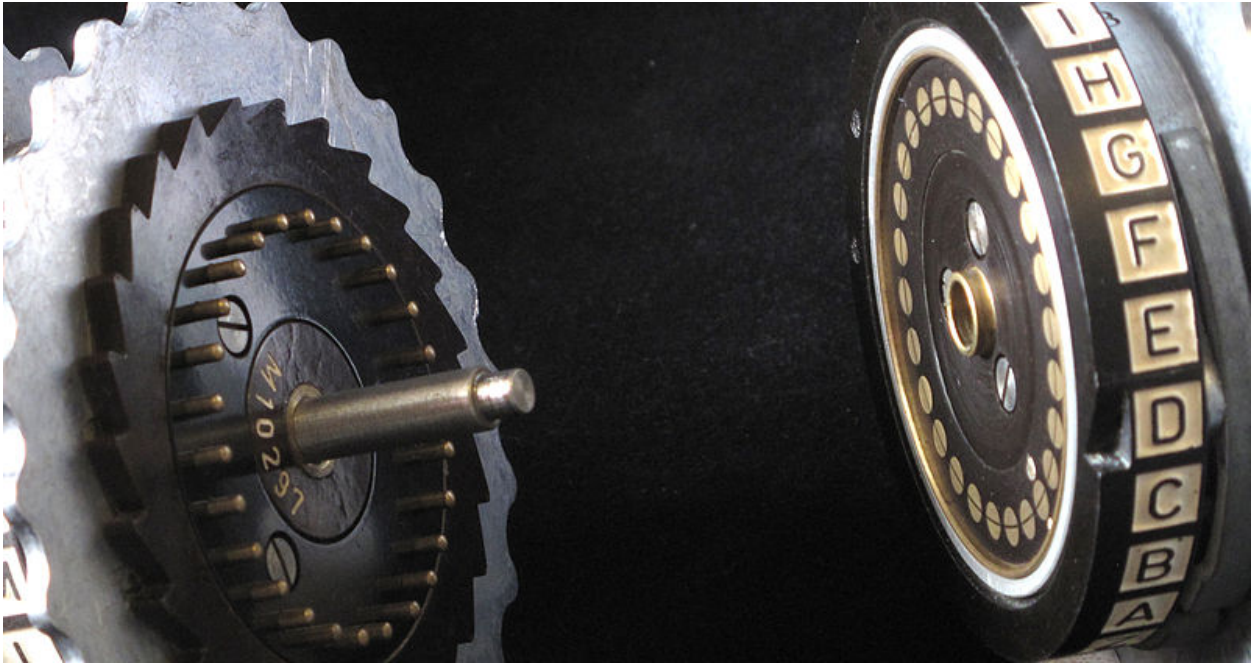
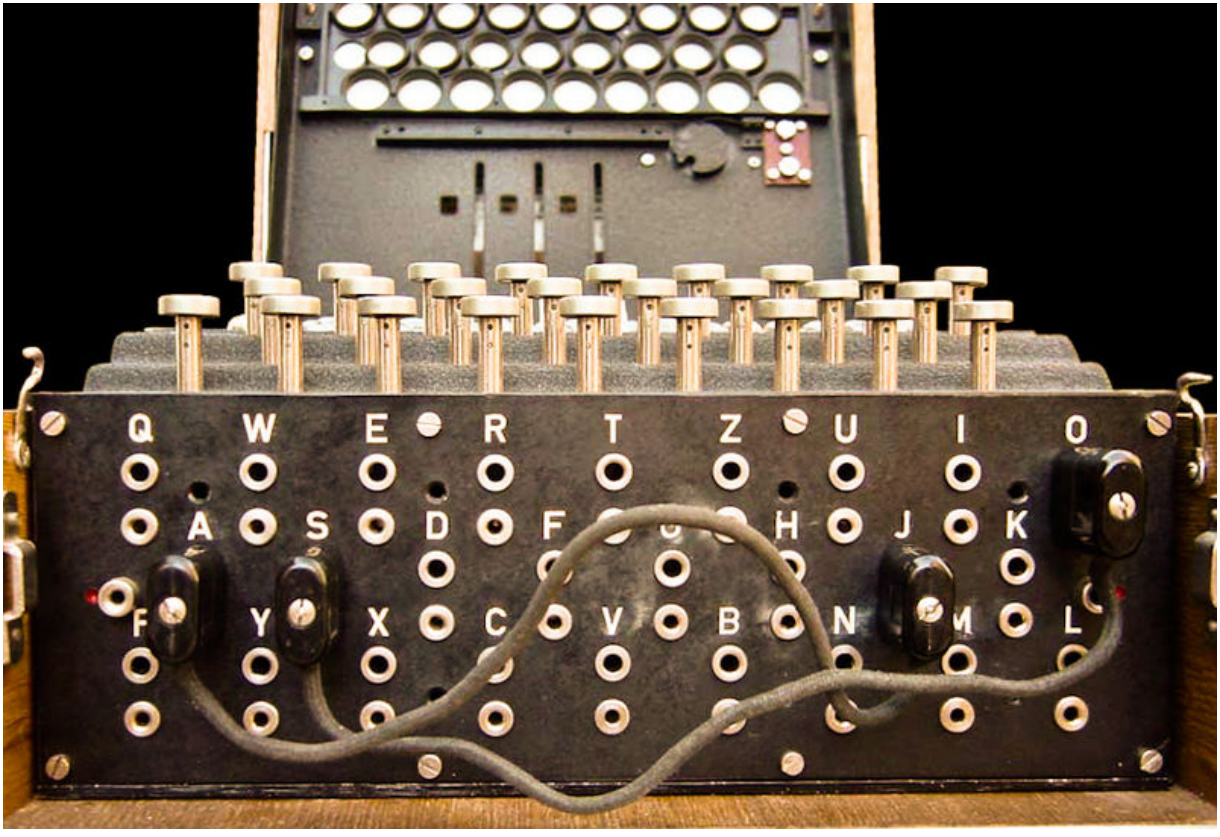


Photo © User:TedColes / Wikimedia Commons

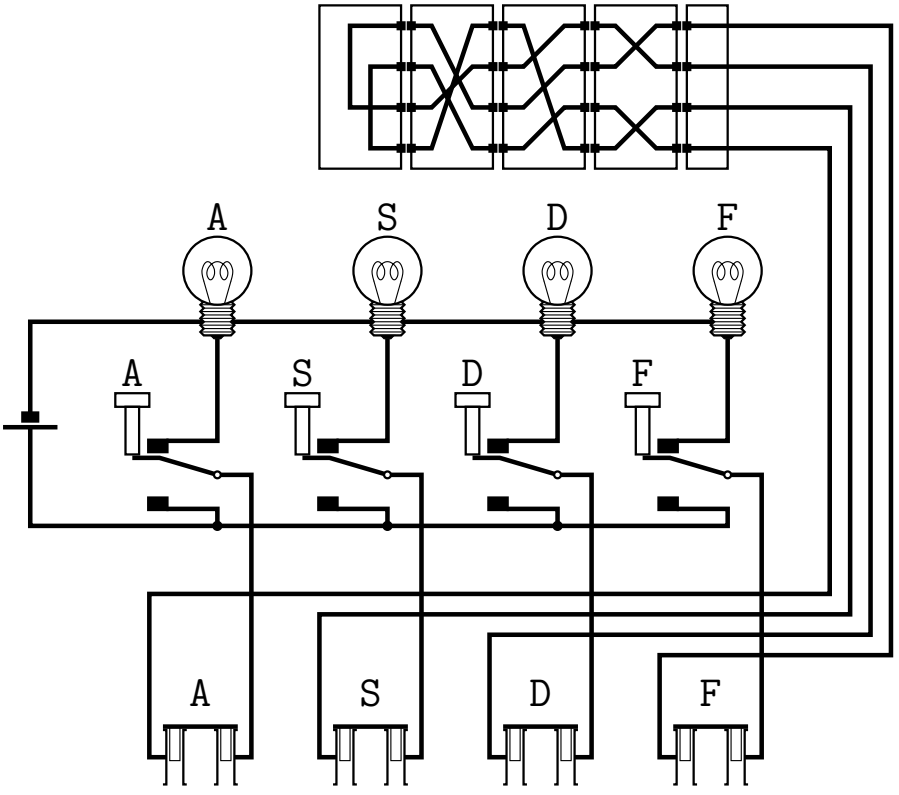
Vue d'ensemble

Photo © Christie's 2013

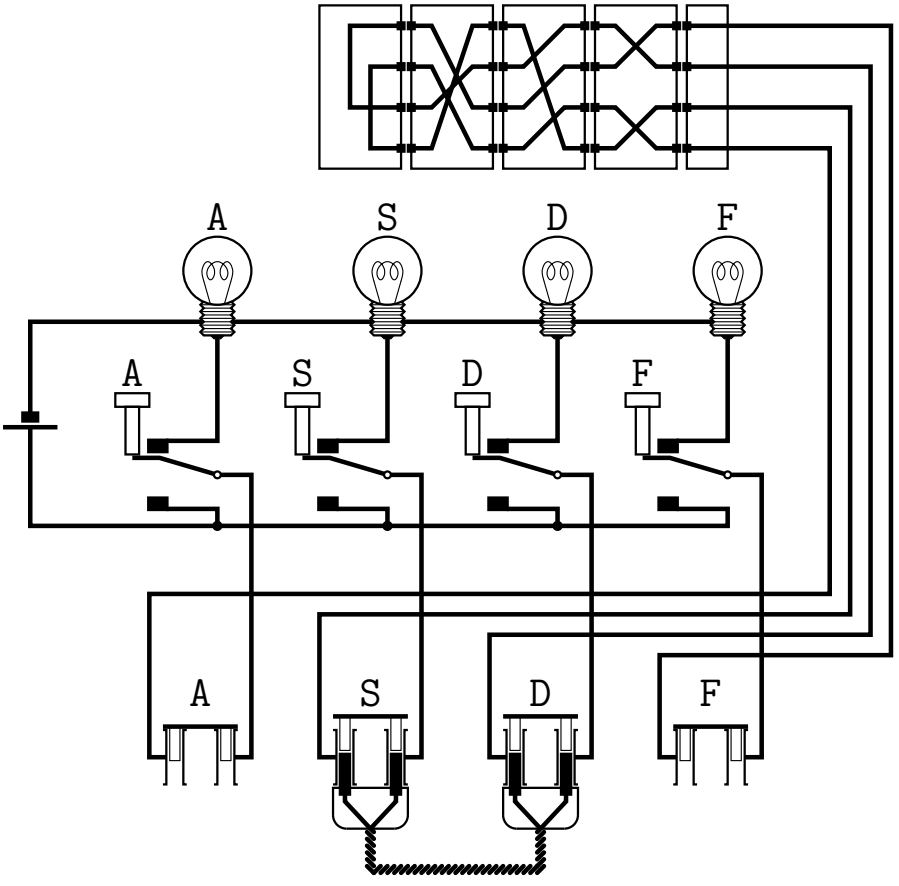
Steckerbrett



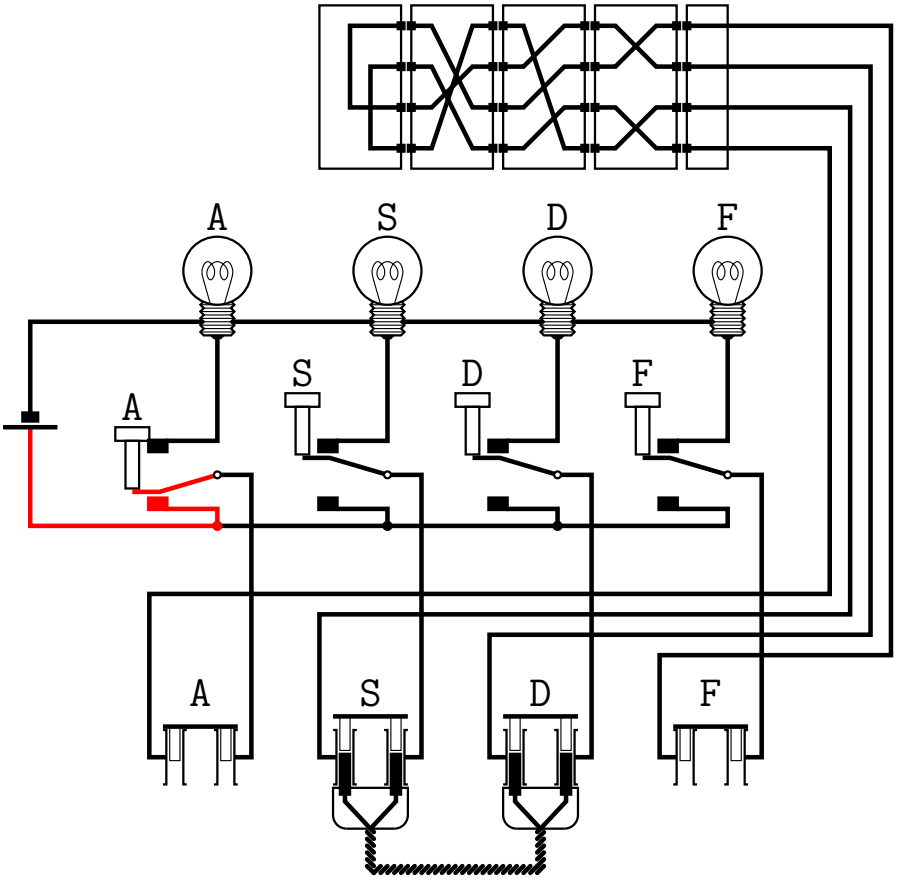
Steckerbrett



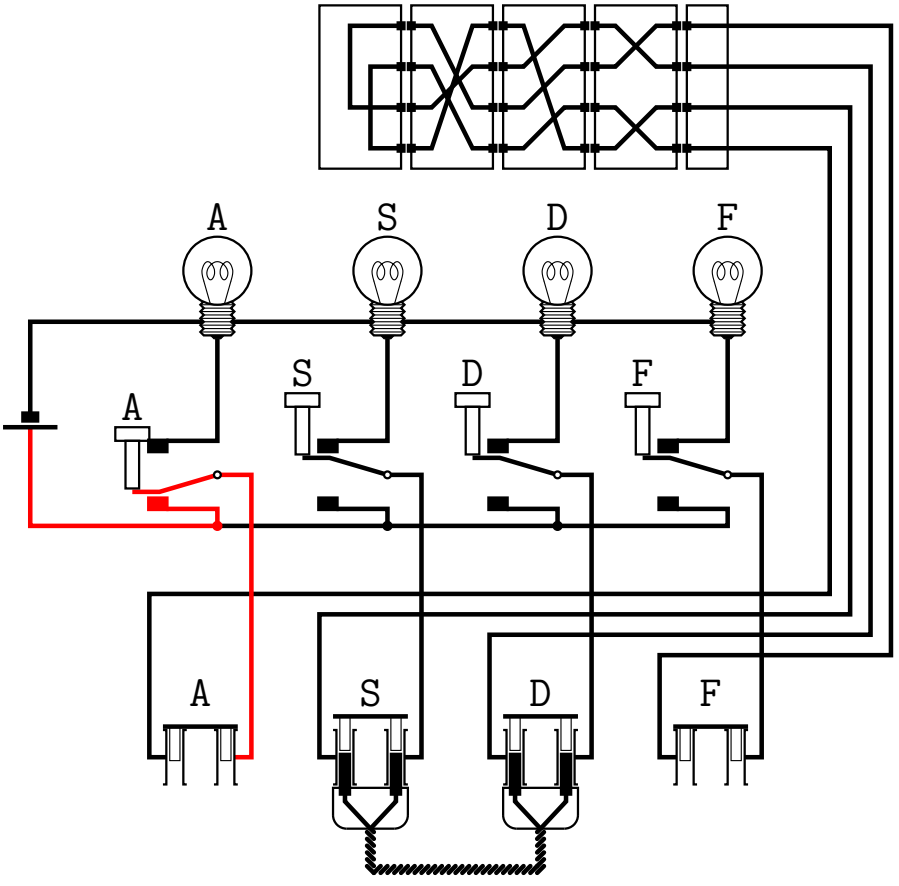
Steckerbrett



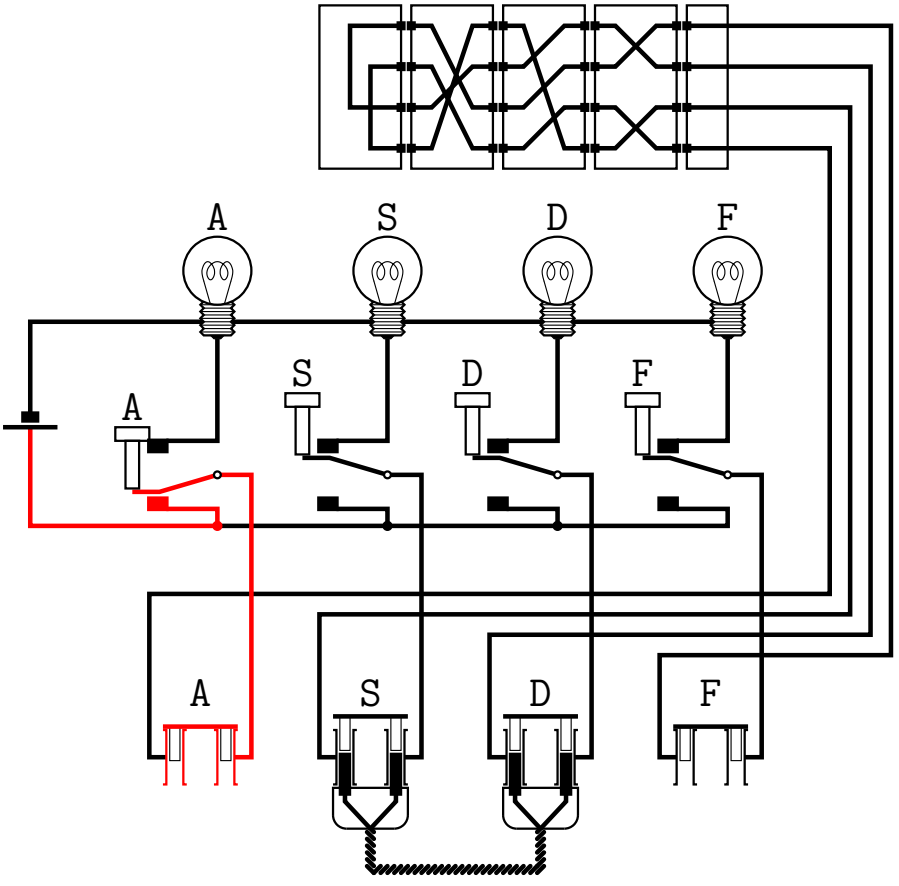
Steckerbrett



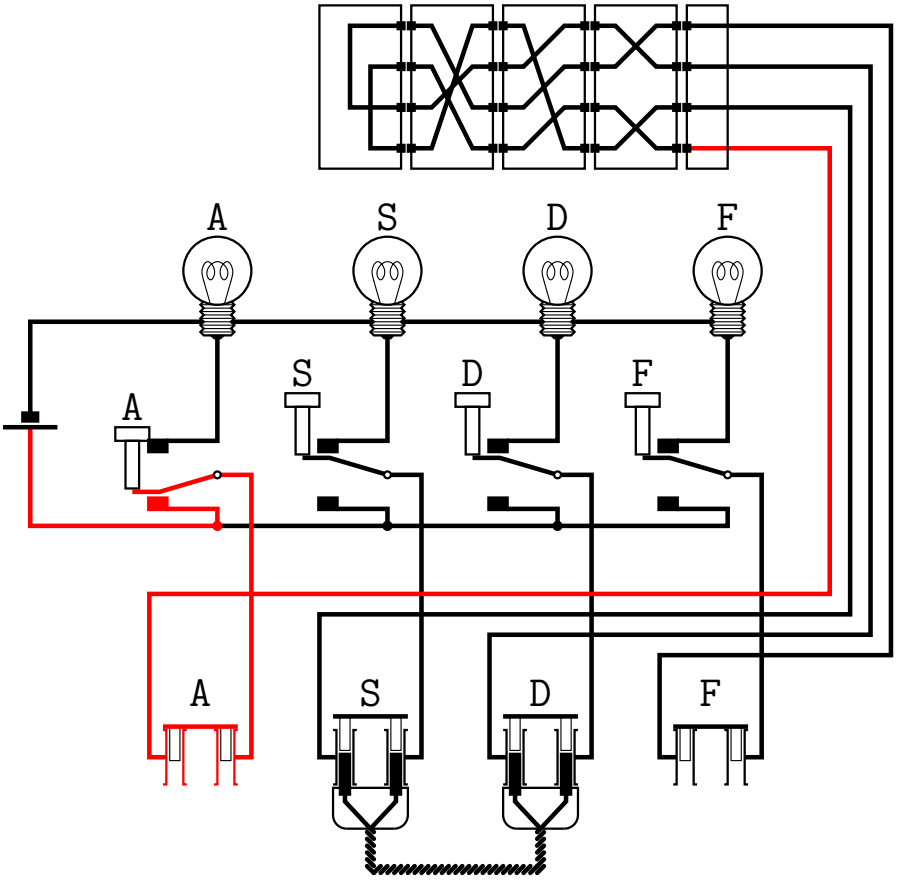
Steckerbrett



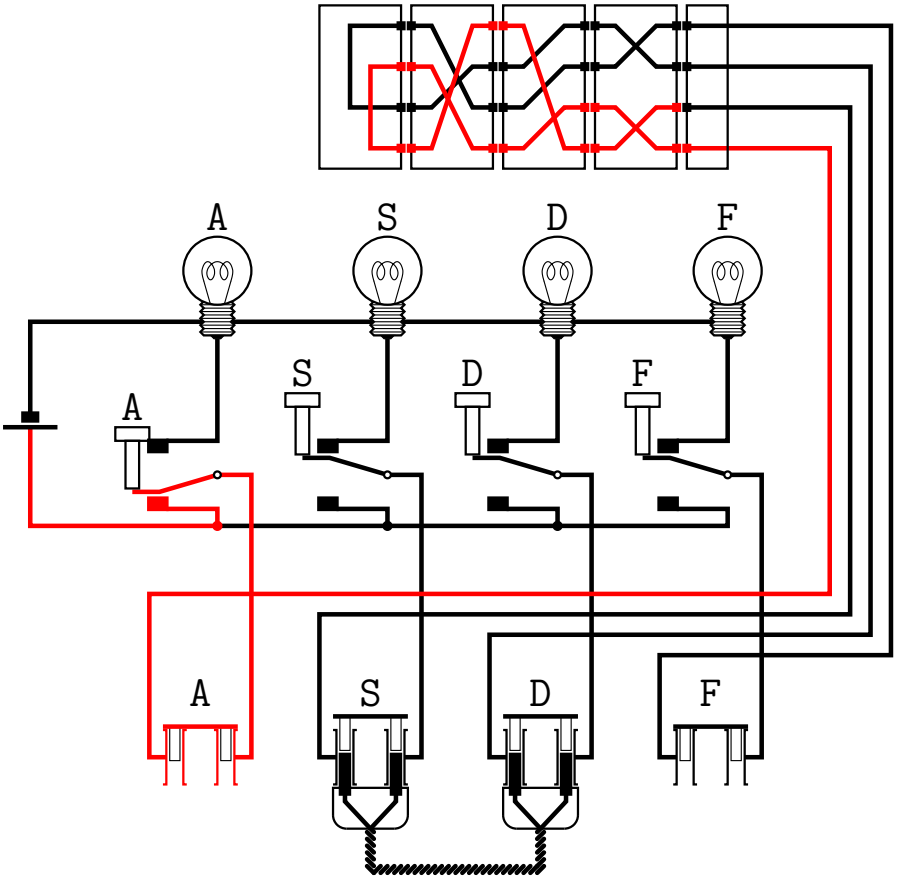
Steckerbrett



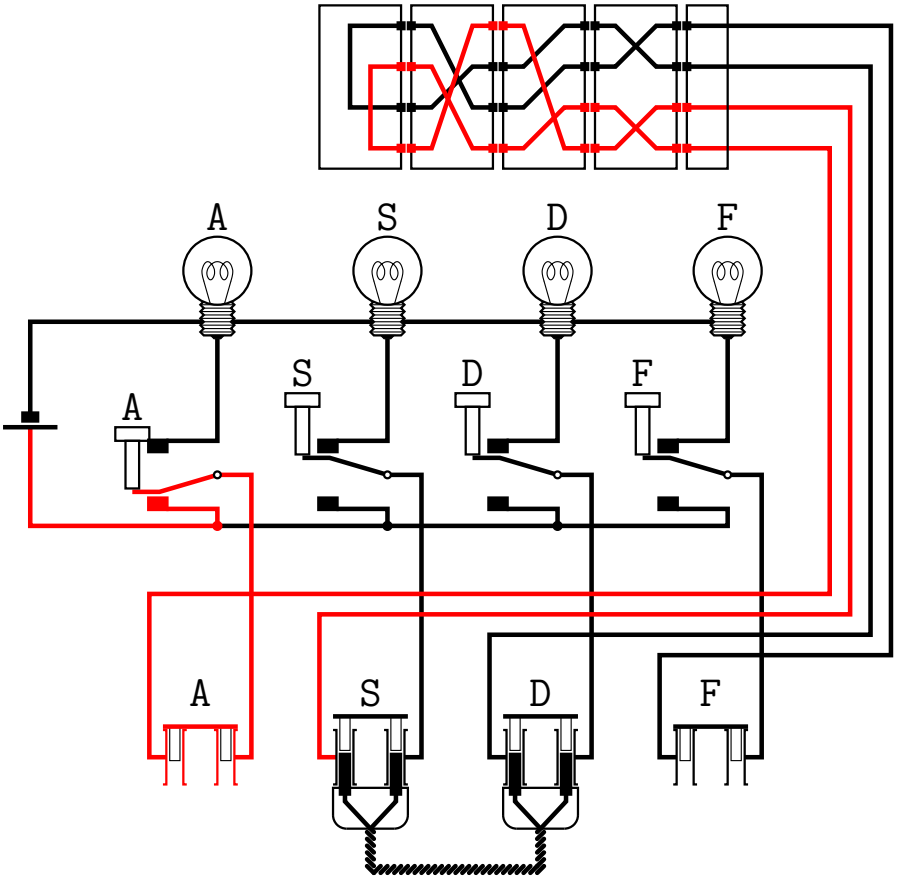
Steckerbrett



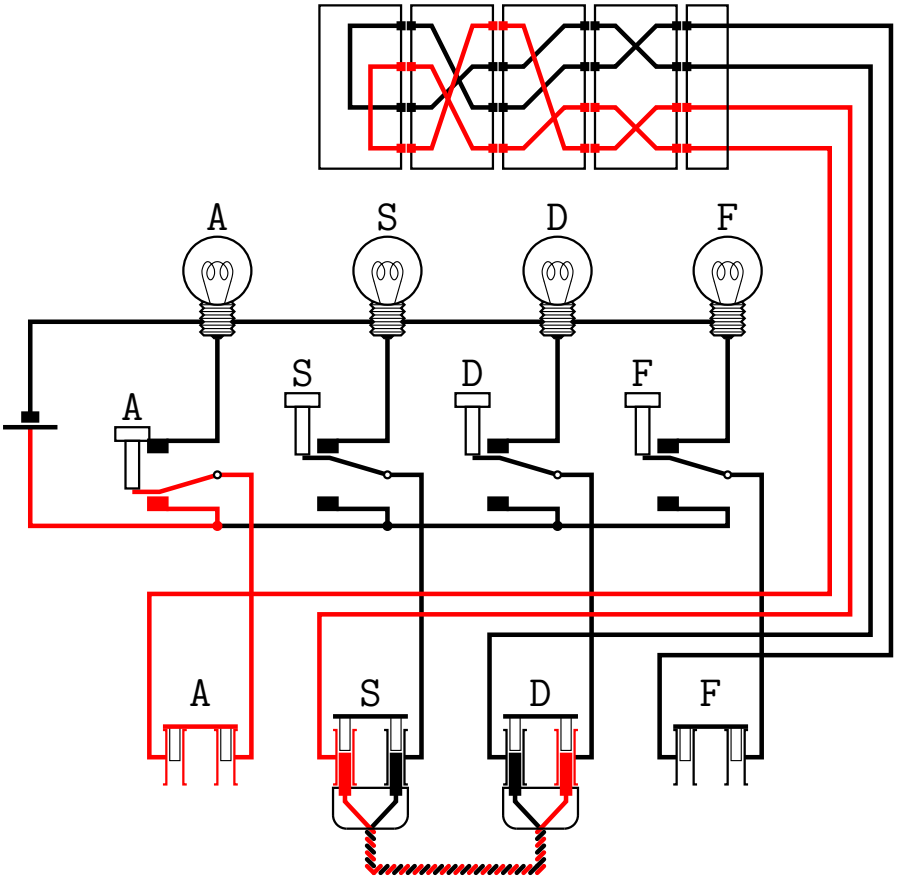
Steckerbrett



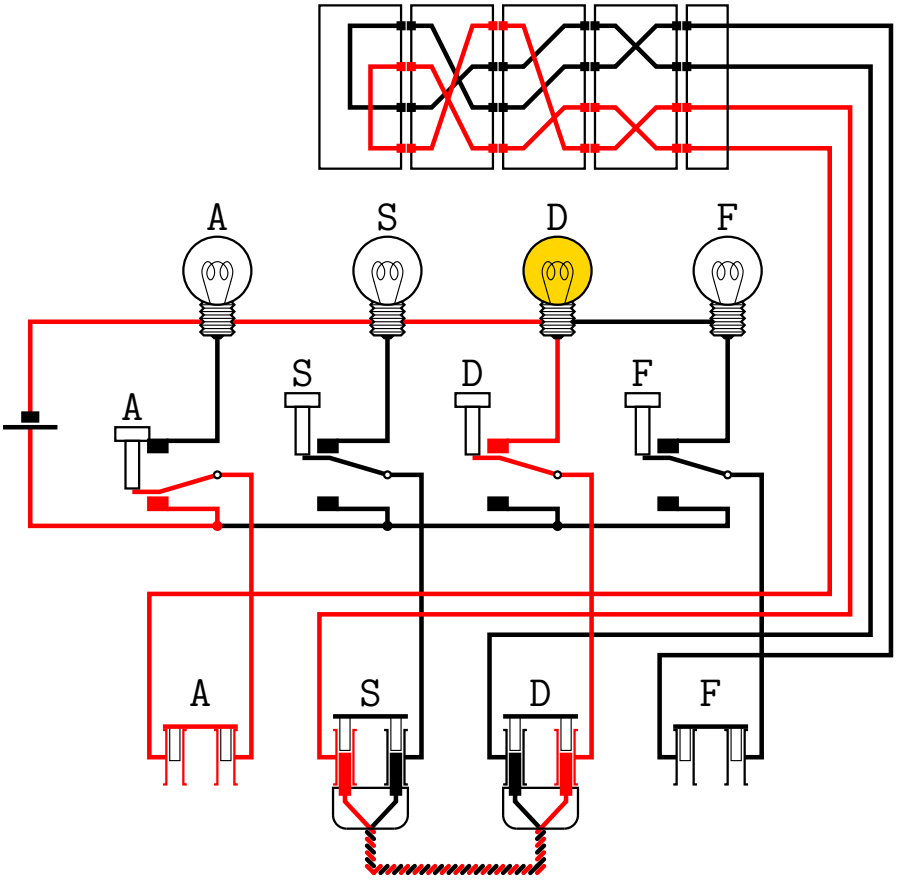
Steckerbrett



Steckerbrett



Steckerbrett



Clés journalières

Geheime Kommandosache
Nicht ins Flugzeug mitnehmen

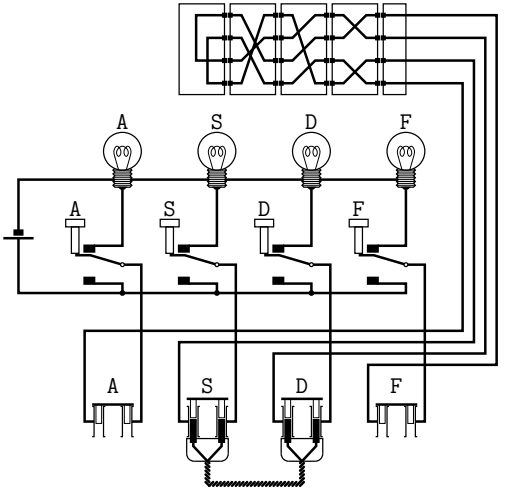
Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

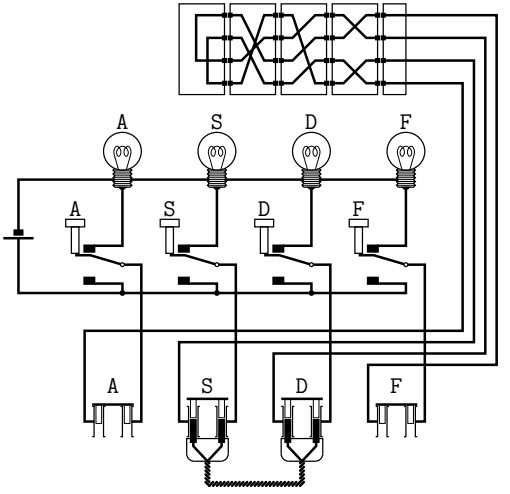
Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	TO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	cid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	ED	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vcx
St	22.	I	II	IV	01	25	02	PZ	SB	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	UD	KP	VO	QS	NW	HL	BM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	ieu	ytc
St	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VJ	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	HY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CA	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upo	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YK	WT	DB	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NP	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lrc	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	XY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DB	VJ	FS	ZK	TU	HX	AQ	GT	YO	EC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	ool	ooi	ywv	sfb

Un peu de combinatoire

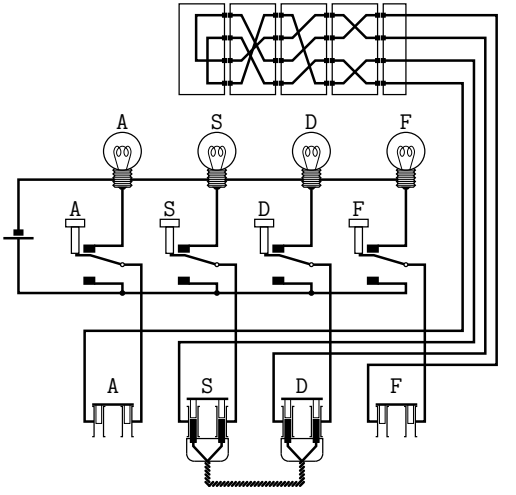


Un peu de combinatoire



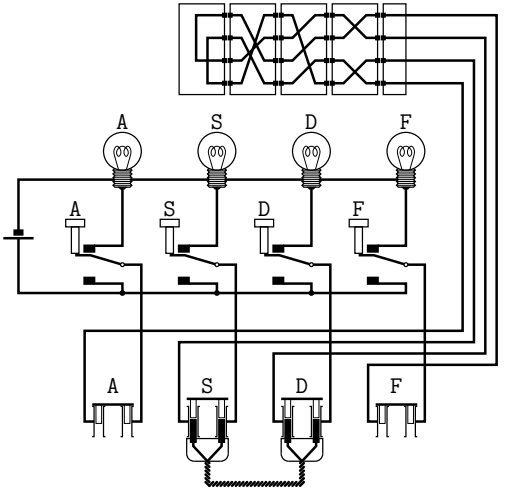
- Combien de combinaisons possibles ?

Un peu de combinatoire



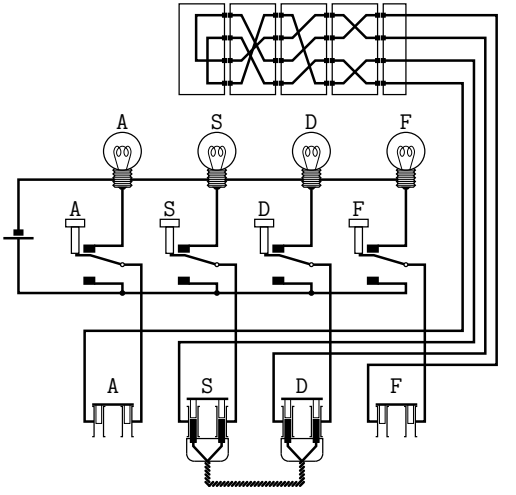
- Combien de combinaisons possibles ?
  - choix (ordonné) de 3 rotors parmi 5

Un peu de combinatoire



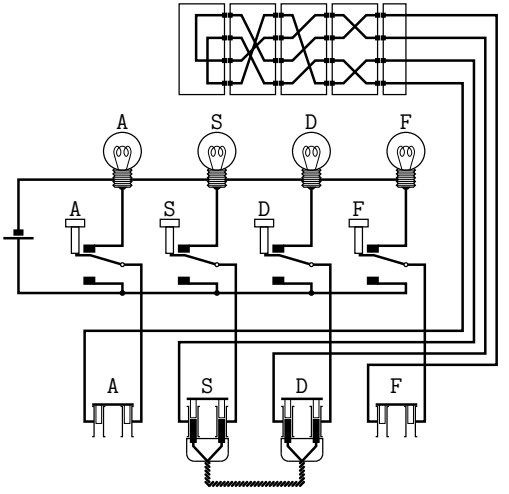
- Combien de combinaisons possibles ?
  - choix (ordonné) de 3 rotors parmi 5
  - 26 positions de départ possibles pour chaque rotor

Un peu de combinatoire



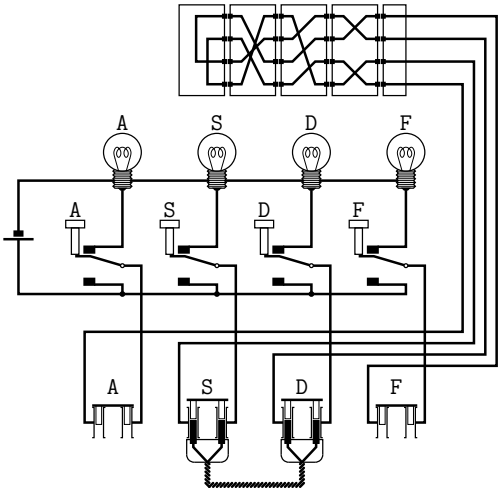
- Combien de combinaisons possibles ?
  - choix (ordonné) de 3 rotors parmi 5
  - 26 positions de départ possibles pour chaque rotor
  - 26 positions possibles pour l'entraînement des rotors de gauche et du milieu

Un peu de combinatoire



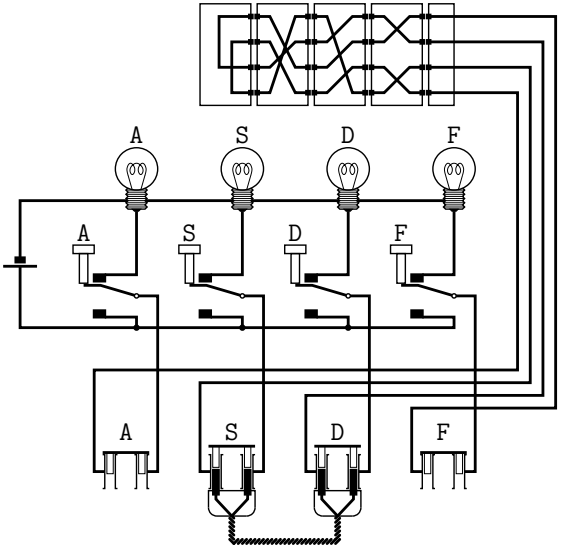
- Combien de combinaisons possibles ?
  - choix (ordonné) de 3 rotors parmi 5
  - 26 positions de départ possibles pour chaque rotor
  - 26 positions possibles pour l'entraînement des rotors de gauche et du milieu
  - choix de 0 à 13 échanges de paires de lettres parmi 26

Un peu de combinatoire



- Combien de combinaisons possibles ?
  - choix (ordonné) de 3 rotors parmi 5
  - 26 positions de départ possibles pour chaque rotor
  - 26 positions possibles pour l'entraînement des rotors de gauche et du milieu
  - choix de 0 à 13 échanges de paires de lettres parmi 26
- $60 \times 17\,576 \times 676 \times 532\,985\,208\,200\,576 = 379\,955\,859\,664\,159\,612\,354\,560$

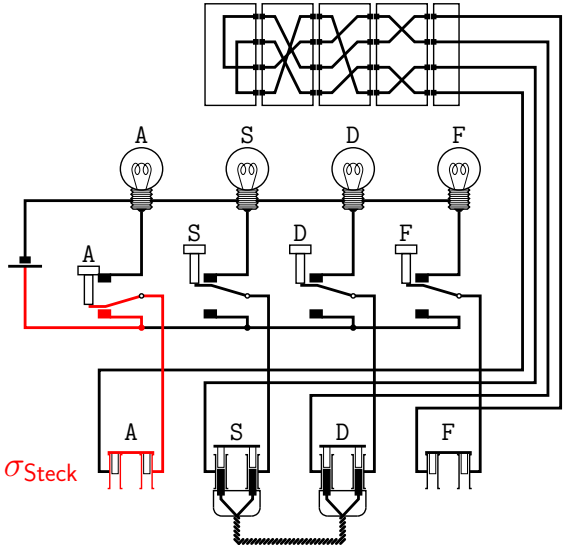
Permutations



σ_{k_0+i}

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :

Permutations



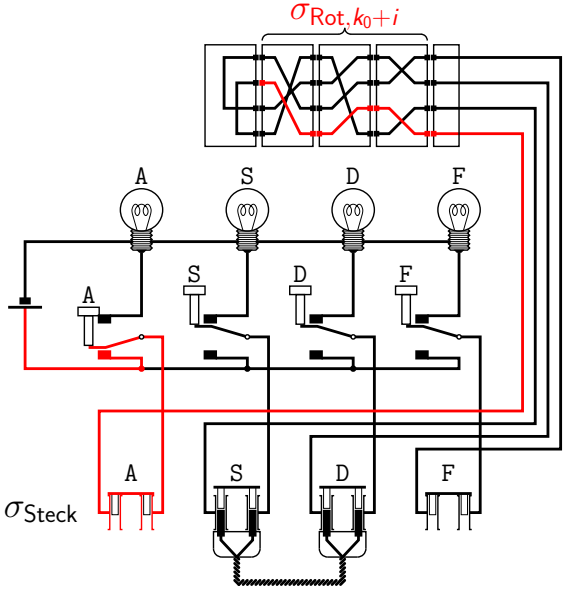
$\sigma_{k_0+i} =$ σ_{Steck}

Par exemple :

$$\sigma_{\text{Steck}}(\texttt{A}) = \texttt{A}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;

Permutations



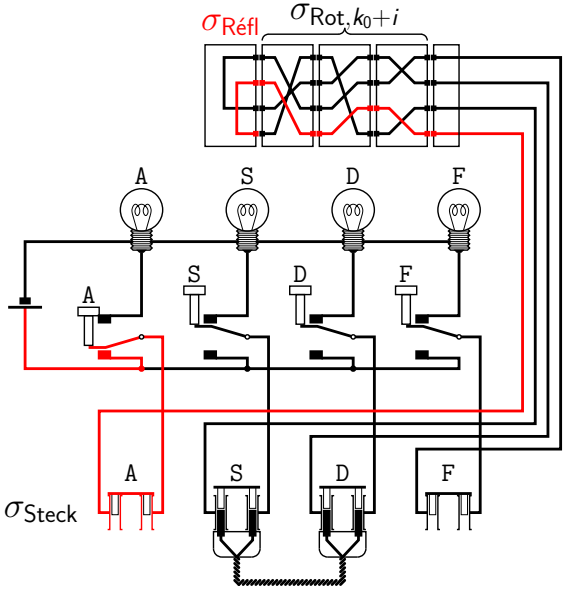
$\sigma_{k_0+i} =$ $\sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$

Par exemple :

$$\sigma_{\text{Steck}}(\mathtt{A}) = \mathtt{A}$$
$$\sigma_{\text{Rot},k_0+i}(\mathtt{A}) = \mathtt{D}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;

Permutations



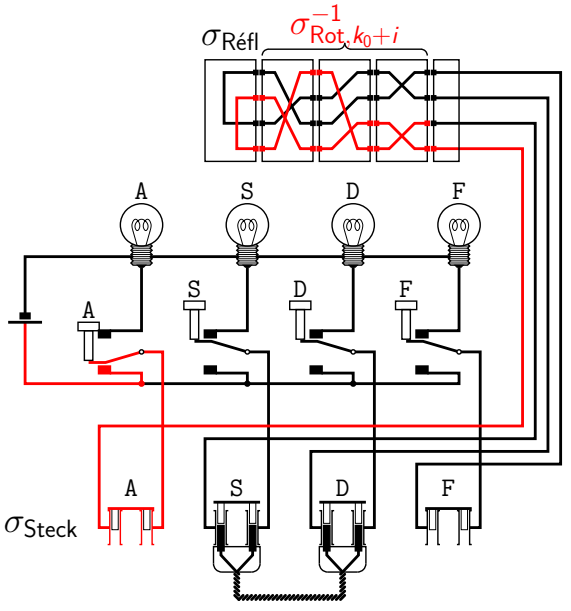
$\sigma_{k_0+i} = \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$

Par exemple :

$$\sigma_{\text{Steck}}(\mathtt{A}) = \mathtt{A}$$
$$\sigma_{\text{Rot},k_0+i}(\mathtt{A}) = \mathtt{D}$$
$$\sigma_{\text{Réfl}}(\mathtt{D}) = \mathtt{A}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\text{Réfl}}$, la permutation réalisée par le réflecteur ;

Permutations



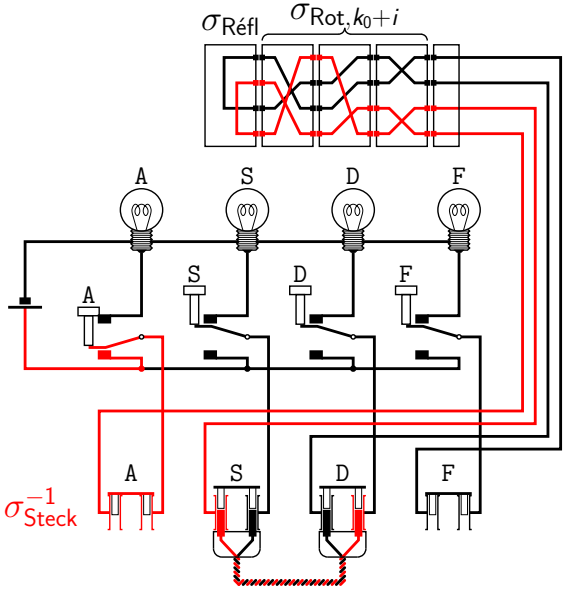
$$\sigma_{k_0+i} = \sigma^{-1}_{\text{Rot},k_0+i} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$$

Par exemple :

$$\begin{aligned} \sigma_{\text{Steck}}(\mathtt{A}) &= \mathtt{A} \\ \sigma_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{D} \\ \sigma_{\text{Réfl}}(\mathtt{D}) &= \mathtt{A} \\ \sigma^{-1}_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{S} \end{aligned}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\text{Réfl}}$, la permutation réalisée par le réflecteur ;
  - puis $\sigma^{-1}_{\text{Rot},k_0+i}$, en repassant dans les rotors au retour ;

Permutations



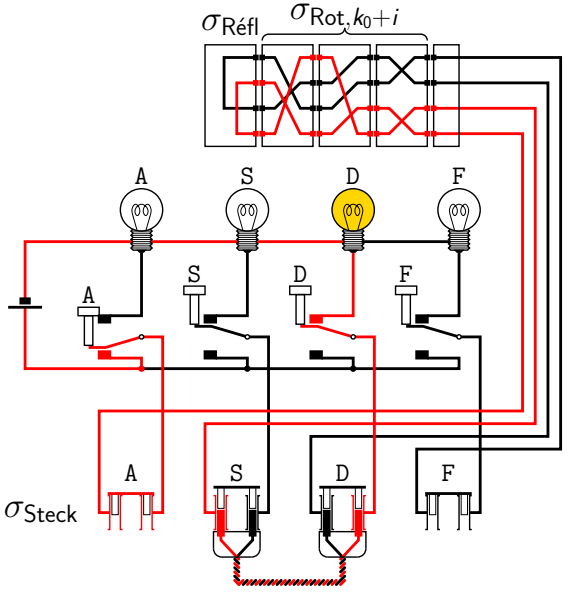
$$\sigma_{k_0+i} = \sigma^{-1}_{\text{Steck}} \circ \sigma^{-1}_{\text{Rot},k_0+i} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$$

Par exemple :

$$\begin{aligned}
\sigma_{\text{Steck}}(\mathtt{A}) &= \mathtt{A} \\
\sigma_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{D} \\
\sigma_{\text{Réfl}}(\mathtt{D}) &= \mathtt{A} \\
\sigma^{-1}_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{S} \\
\sigma^{-1}_{\text{Steck}}(\mathtt{S}) &= \mathtt{D}
\end{aligned}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\text{Réfl}}$, la permutation réalisée par le réflecteur ;
  - puis $\sigma^{-1}_{\text{Rot},k_0+i}$, en repassant dans les rotors au retour ;
  - enfin $\sigma^{-1}_{\text{Steck}}$, en repassant dans le *Steckerbrett* au retour.

Permutations



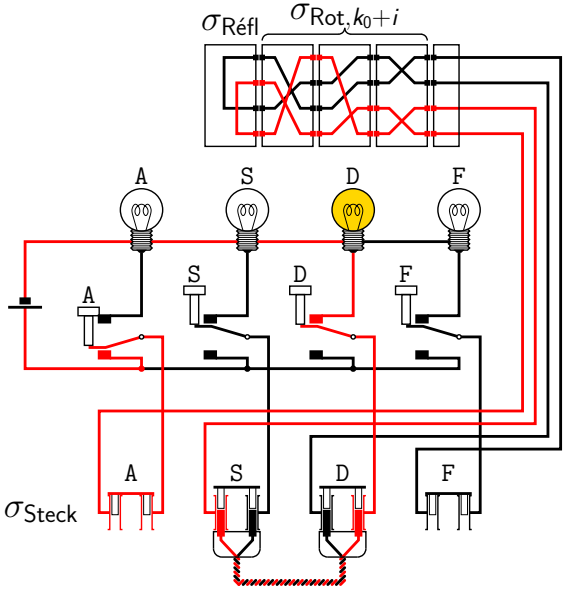
$$\sigma_{k_0+i} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$$

Par exemple :

$$\begin{aligned}
\sigma_{\text{Steck}}(\mathtt{A}) &= \mathtt{A} \\
\sigma_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{D} \\
\sigma_{\text{Réfl}}(\mathtt{D}) &= \mathtt{A} \\
\sigma_{\text{Rot},k_0+i}^{-1}(\mathtt{A}) &= \mathtt{S} \\
\sigma_{\text{Steck}}^{-1}(\mathtt{S}) &= \mathtt{D} \\
\text{d'où } \sigma_{k_0+i}(\mathtt{A}) &= \mathtt{D}
\end{aligned}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\text{Réfl}}$, la permutation réalisée par le réflecteur ;
  - puis $\sigma_{\text{Rot},k_0+i}^{-1}$, en repassant dans les rotors au retour ;
  - enfin $\sigma_{\text{Steck}}^{-1}$, en repassant dans le *Steckerbrett* au retour.

Permutations



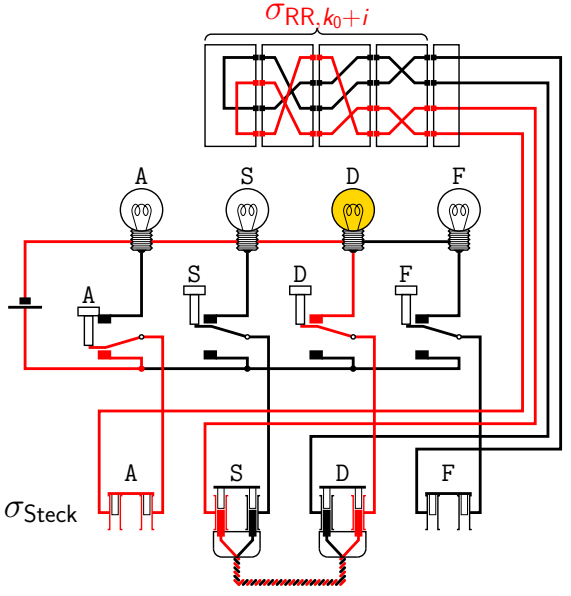
$$\sigma_{k_0+i} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i} \circ \sigma_{\text{Steck}}$$

Par exemple :

$$\begin{aligned}
\sigma_{\text{Steck}}(\mathtt{A}) &= \mathtt{A} \\
\sigma_{\text{Rot},k_0+i}(\mathtt{A}) &= \mathtt{D} \\
\sigma_{\text{Réfl}}(\mathtt{D}) &= \mathtt{A} \\
\sigma_{\text{Rot},k_0+i}^{-1}(\mathtt{A}) &= \mathtt{S} \\
\sigma_{\text{Steck}}^{-1}(\mathtt{S}) &= \mathtt{D} \\
\text{d'où } \sigma_{k_0+i}(\mathtt{A}) &= \mathtt{D}
\end{aligned}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\text{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\text{Réfl}}$, la permutation réalisée par le réflecteur ;
  - puis $\sigma_{\text{Rot},k_0+i}^{-1}$, en repassant dans les rotors au retour ;
  - enfin $\sigma_{\text{Steck}}^{-1}$, en repassant dans le *Steckerbrett* au retour.

Permutations



$$\sigma_{k_0+i} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+i} \circ \sigma_{\mathrm{Steck}}$$

avec $\sigma_{\mathrm{RR},k_0+i} = \sigma_{\mathrm{Rot},k_0+i}^{-1} \circ \sigma_{\mathrm{Réfl}} \circ \sigma_{\mathrm{Rot},k_0+i}$

Par exemple :

$$\sigma_{\mathrm{Steck}}(\mathtt{A}) = \mathtt{A}$$

$$\sigma_{\mathrm{RR},k_0+i}(\mathtt{A}) = \mathtt{S}$$

$$\sigma_{\mathrm{Steck}}^{-1}(\mathtt{S}) = \mathtt{D}$$

$$\text{d'où } \sigma_{k_0+i}(\mathtt{A}) = \mathtt{D}$$

- À partir de la configuration initiale des rotors k_0, lors du chiffrement de la $i^{\text{ième}}$ lettre du message, la machine réalise une permutation de l'alphabet, notée σ_{k_0+i} :
  - d'abord σ_{Steck}, la permutation réalisée par le *Steckerbrett* ;
  - puis $\sigma_{\mathrm{Rot},k_0+i}$, la permutation réalisée par les rotors (différente pour chaque lettre du message) ;
  - puis $\sigma_{\mathrm{Réfl}}$, la permutation réalisée par le réflecteur ;
  - puis $\sigma_{\mathrm{Rot},k_0+i}^{-1}$, en repassant dans les rotors au retour ;
  - enfin $\sigma_{\mathrm{Steck}}^{-1}$, en repassant dans le *Steckerbrett* au retour.

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).
- La permutation du réflecteur est aussi une involution.

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).
- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).
- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.
- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :
  - les cycles de σ_{RR,k_0+i} ont donc la même longueur que ceux de $\sigma_{\text{Réfl}}$, car leurs lettres sont juste permutées par $\sigma_{\text{Rot},k_0+i}$;

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :
  - les cycles de σ_{RR,k_0+i} ont donc la même longueur que ceux de $\sigma_{\text{Réfl}}$, car leurs lettres sont juste permutées par $\sigma_{\text{Rot},k_0+i}$;
  - par conséquent, σ_{RR,k_0+i} est aussi une involution et n'a pas de point fixe.

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :
  - les cycles de σ_{RR,k_0+i} ont donc la même longueur que ceux de $\sigma_{\text{Réfl}}$, car leurs lettres sont juste permutées par $\sigma_{\text{Rot},k_0+i}$;
  - par conséquent, σ_{RR,k_0+i} est aussi une involution et n'a pas de point fixe.

- De même, la permutation complète $\sigma_{k_0+i} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+i} \circ \sigma_{\text{Steck}}$, conjuguée de σ_{RR,k_0+i}, est aussi une involution et n'a pas de point fixe :

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :
  - les cycles de σ_{RR,k_0+i} ont donc la même longueur que ceux de $\sigma_{\text{Réfl}}$, car leurs lettres sont juste permutées par $\sigma_{\text{Rot},k_0+i}$;
  - par conséquent, σ_{RR,k_0+i} est aussi une involution et n'a pas de point fixe.

- De même, la permutation complète $\sigma_{k_0+i} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+i} \circ \sigma_{\text{Steck}}$, conjuguée de σ_{RR,k_0+i}, est aussi une involution et n'a pas de point fixe :
  - chiffrement et déchiffrement sont la même opération ;

Quelques propriétés immédiates

- La permutation du *Steckerbrett* est une involution ($\sigma_{\text{Steck}}^{-1} = \sigma_{\text{Steck}}$ et $\sigma_{\text{Steck}}^{2} = \text{Id}$) :
  - chaque échange de lettres est une transposition (un cycle de longueur 2) ;
  - ces transpositions sont disjointes (chaque lettre n'apparaît au plus que dans une seule transposition).

- La permutation du réflecteur est aussi une involution.
  De plus, elle n'admet pas de point fixe ($\sigma_{\text{Réfl}}(x) \neq x$ pour toute lettre x) car elle est composée d'exactement 13 transpositions disjointes.

- Comme $\sigma_{\text{RR},k_0+i} = \sigma_{\text{Rot},k_0+i}^{-1} \circ \sigma_{\text{Réfl}} \circ \sigma_{\text{Rot},k_0+i}$, les permutations σ_{RR,k_0+i} et $\sigma_{\text{Réfl}}$ sont conjuguées l'une de l'autre :
  - les cycles de σ_{RR,k_0+i} ont donc la même longueur que ceux de $\sigma_{\text{Réfl}}$, car leurs lettres sont juste permutées par $\sigma_{\text{Rot},k_0+i}$;
  - par conséquent, σ_{RR,k_0+i} est aussi une involution et n'a pas de point fixe.

- De même, la permutation complète $\sigma_{k_0+i} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+i} \circ \sigma_{\text{Steck}}$, conjuguée de σ_{RR,k_0+i}, est aussi une involution et n'a pas de point fixe :
  - chiffrement et déchiffrement sont la même opération ;
  - une lettre ne peut jamais être chiffrée en elle-même.

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;
  - tape cette clé deux fois de suite ;

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;
  - tape cette clé deux fois de suite ;
  - met la machine dans la configuration donnée par la clé de message ;

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;
  - tape cette clé deux fois de suite ;
  - met la machine dans la configuration donnée par la clé de message ;
  - tape son message.

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;
  - tape cette clé deux fois de suite ;
  - met la machine dans la configuration donnée par la clé de message ;
  - tape son message.
- Faiblesse : répétition de la clé de message

Méthode des caractéristiques de Rejewski

- Avant chaque nouveau message, l'opérateur :
  - met la machine dans la configuration initiale k_0 donnée par la clé journalière ;
  - choisit une clé de message aléatoire de 3 lettres ;
  - tape cette clé deux fois de suite ;
  - met la machine dans la configuration donnée par la clé de message ;
  - tape son message.

- Faiblesse : répétition de la clé de message

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape $xyzxyz$;

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape $xyzxyz$;
  - le chiffré correspondant est donc $\sigma_{k_0+1}(x)\sigma_{k_0+2}(y)\sigma_{k_0+3}(z)\sigma_{k_0+4}(x)\sigma_{k_0+5}(y)\sigma_{k_0+6}(z)$.

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape $xyzxyz$;
  - le chiffré correspondant est donc $\sigma_{k_0+1}(x)\sigma_{k_0+2}(y)\sigma_{k_0+3}(z)\sigma_{k_0+4}(x)\sigma_{k_0+5}(y)\sigma_{k_0+6}(z)$.
- Étudions le lien entre $\sigma_{k_0+1}(x)$ et $\sigma_{k_0+4}(x)$:

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape *xyzxyz* ;
  - le chiffré correspondant est donc $\sigma_{k_0+1}(x)\sigma_{k_0+2}(y)\sigma_{k_0+3}(z)\sigma_{k_0+4}(x)\sigma_{k_0+5}(y)\sigma_{k_0+6}(z)$.
- Étudions le lien entre $\sigma_{k_0+1}(x)$ et $\sigma_{k_0+4}(x)$:

$$\sigma_{k_0+1}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(x) \text{ et}$$
$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{Steck}})(x)$$

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape $xyzxyz$;
  - le chiffré correspondant est donc $\sigma_{k_0+1}(x)\sigma_{k_0+2}(y)\sigma_{k_0+3}(z)\sigma_{k_0+4}(x)\sigma_{k_0+5}(y)\sigma_{k_0+6}(z)$.
- Étudions le lien entre $\sigma_{k_0+1}(x)$ et $\sigma_{k_0+4}(x)$:

$$\sigma_{k_0+1}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(x) \text{ et}$$
$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{Steck}})(x)$$

- La première équation nous donne

$$x = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

Méthode des caractéristiques de Rejewski

- Notons x, y et z les trois lettres de la clé de message :
  - l'opérateur tape $xyzxyz$;
  - le chiffré correspondant est donc $\sigma_{k_0+1}(x)\sigma_{k_0+2}(y)\sigma_{k_0+3}(z)\sigma_{k_0+4}(x)\sigma_{k_0+5}(y)\sigma_{k_0+6}(z)$.
- Étudions le lien entre $\sigma_{k_0+1}(x)$ et $\sigma_{k_0+4}(x)$:

$$\sigma_{k_0+1}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(x) \text{ et}$$
$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{Steck}})(x)$$

- La première équation nous donne

$$x = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

- D'où $\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M D

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M D C

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S		Y	K	T

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S		Y	K	T

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$\tilde{S}_{k_0+1} =$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M D C J I P G F E Z B H V U L R Q N A W S O Y K T

$$\tilde{S}_{k_0+1} = (\text{AX}$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$$\tilde{S}_{k_0+1} = (\text{AXY}$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M D C J I P G F E Z B H V U L R Q N A W S O Y K T

$$\tilde{S}_{k_0+1} = (\text{AXYK}$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$$\tilde{S}_{k_0+1} = (\text{AXYKZ}$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$$\tilde{S}_{k_0+1} = (\text{AXYKZT}$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$$\tilde{S}_{k_0+1} = (\text{AXYKZT})$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X	M	D	C	J	I	P	G	F	E	Z	B	H	V	U	L	R	Q	N	A	W	S	O	Y	K	T

$$\tilde{S}_{k_0+1} = (\text{AXYKZT})(\text{BMHGPL})$$

Méthode des caractéristiques de Rejewski

$$\sigma_{k_0+4}(x) = (\sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}})(\sigma_{k_0+1}(x))$$

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Tentons de caractériser la permutation $\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$:

$\sigma_{k_0+1}(x)$	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
$\sigma_{k_0+4}(x)$	X M D C J I P G F E Z B H V U L R Q N A W S O Y K T

$$\tilde{S}_{k_0+1} = (\text{AXYKZT})(\text{BMHGPL})(\text{CD})(\text{EJ})(\text{FI})(\text{NVS})(\text{OUW})(\text{QR})$$

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = \ ?$$

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = \ ?$$

- Les permutations S_{k_0+1} et $\tilde{S}_{k_0+1}$ sont conjuguées :

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ S_{k_0+1} \circ \sigma_{\text{Steck}}$$

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = \ ?$$

- Les permutations S_{k_0+1} et $\tilde{S}_{k_0+1}$ sont conjuguées :

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ S_{k_0+1} \circ \sigma_{\text{Steck}}$$

  - les longueurs des cycles de ces permutations sont les mêmes ;

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = \ ?$$

- Les permutations S_{k_0+1} et $\tilde{S}_{k_0+1}$ sont conjuguées :

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ S_{k_0+1} \circ \sigma_{\text{Steck}}$$

  - les longueurs des cycles de ces permutations sont les mêmes ;
  - ces longueurs ne dépendent pas de la lettre x de la clé de message ni de la configuration du *Steckerbrett*, mais uniquement des rotors.

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = (\texttt{??????})(\texttt{??????})(\texttt{??})(\texttt{??})(\texttt{??})(\texttt{???})(\texttt{???})(\texttt{??})$$

- Les permutations S_{k_0+1} et $\tilde{S}_{k_0+1}$ sont conjuguées :

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ S_{k_0+1} \circ \sigma_{\text{Steck}}$$

  - les longueurs des cycles de ces permutations sont les mêmes ;
  - ces longueurs ne dépendent pas de la lettre x de la clé de message ni de la configuration du *Steckerbrett*, mais uniquement des rotors.

Méthode des caractéristiques de Rejewski

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1} \circ \sigma_{\text{Steck}}$$

- Que peut-on dire sur la permutation $S_{k_0+1} = \sigma_{\text{RR},k_0+4} \circ \sigma_{\text{RR},k_0+1}$?

$$\tilde{S}_{k_0+1} = (\texttt{AXYKZT})(\texttt{BMHGPL})(\texttt{CD})(\texttt{EJ})(\texttt{FI})(\texttt{NVS})(\texttt{OUW})(\texttt{QR})$$
$$S_{k_0+1} = (\texttt{??????})(\texttt{??????})(\texttt{??})(\texttt{??})(\texttt{??})(\texttt{???})(\texttt{???})(\texttt{??})$$

- Les permutations S_{k_0+1} et $\tilde{S}_{k_0+1}$ sont conjuguées :

$$\tilde{S}_{k_0+1} = \sigma_{\text{Steck}}^{-1} \circ S_{k_0+1} \circ \sigma_{\text{Steck}}$$

  - les longueurs des cycles de ces permutations sont les mêmes ;
  - ces longueurs ne dépendent pas de la lettre x de la clé de message ni de la configuration du *Steckerbrett*, mais uniquement des rotors.

- Les longueurs de ces cycles forment la caractéristique de la permutation :

$$\text{Carac}(S_{k_0+1}) = \text{Carac}(\tilde{S}_{k_0+1}) = (6, 6, 3, 3, 2, 2, 2, 2)$$

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Il en est de même pour les permutations

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Il en est de même pour les permutations
  - entre les lettres chiffrées $\sigma_{k_0+2}(y)$ et $\sigma_{k_0+5}(y)$:

$$\mathrm{Carac}(\tilde{S}_{k_0+2}) = (13, 13), \qquad \text{où } \tilde{S}_{k_0+2} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \circ \sigma_{\mathrm{Steck}}$$

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Il en est de même pour les permutations
  - entre les lettres chiffrées $\sigma_{k_0+2}(y)$ et $\sigma_{k_0+5}(y)$:

$$\begin{aligned} \mathrm{Carac}(\tilde{S}_{k_0+2}) &= (13,13), && \text{où } \tilde{S}_{k_0+2} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \circ \sigma_{\mathrm{Steck}} \\ &= \mathrm{Carac}(S_{k_0+2}) && \text{où } S_{k_0+2} = \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \end{aligned}$$

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Il en est de même pour les permutations
  - entre les lettres chiffrées $\sigma_{k_0+2}(y)$ et $\sigma_{k_0+5}(y)$:

$$\begin{aligned} \mathrm{Carac}(\tilde{S}_{k_0+2}) &= (13,13), && \text{où } \tilde{S}_{k_0+2} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \circ \sigma_{\mathrm{Steck}} \\ &= \mathrm{Carac}(S_{k_0+2}) && \text{où } S_{k_0+2} = \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \end{aligned}$$

  - entre les lettres chiffrées $\sigma_{k_0+3}(z)$ et $\sigma_{k_0+6}(z)$:

$$\mathrm{Carac}(\tilde{S}_{k_0+3}) = (7,7,4,4,2,2), \text{ où } \tilde{S}_{k_0+3} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+6} \circ \sigma_{\mathrm{RR},k_0+3} \circ \sigma_{\mathrm{Steck}}$$

Méthode des caractéristiques de Rejewski

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

- Il en est de même pour les permutations
  - entre les lettres chiffrées $\sigma_{k_0+2}(y)$ et $\sigma_{k_0+5}(y)$:

$$\begin{aligned} \mathrm{Carac}(\tilde{S}_{k_0+2}) &= (13,13), && \text{où } \tilde{S}_{k_0+2} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \circ \sigma_{\mathrm{Steck}} \\ &= \mathrm{Carac}(S_{k_0+2}) && \text{où } S_{k_0+2} = \sigma_{\mathrm{RR},k_0+5} \circ \sigma_{\mathrm{RR},k_0+2} \end{aligned}$$

  - entre les lettres chiffrées $\sigma_{k_0+3}(z)$ et $\sigma_{k_0+6}(z)$:

$$\begin{aligned} \mathrm{Carac}(\tilde{S}_{k_0+3}) &= (7,7,4,4,2,2), \text{ où } \tilde{S}_{k_0+3} = \sigma_{\mathrm{Steck}}^{-1} \circ \sigma_{\mathrm{RR},k_0+6} \circ \sigma_{\mathrm{RR},k_0+3} \circ \sigma_{\mathrm{Steck}} \\ &= \mathrm{Carac}(S_{k_0+3}) \quad \text{où } S_{k_0+3} = \sigma_{\mathrm{RR},k_0+6} \circ \sigma_{\mathrm{RR},k_0+3} \end{aligned}$$

Méthode des caractéristiques de Rejewski

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :
  - précalculer (une fois pour toutes) une table avec les caractéristiques des permutations $S_k = \sigma_{\mathrm{RR},k+3} \circ \sigma_{\mathrm{RR},k}$, pour toutes les configurations possibles k des rotors :

Configuration k	Carac(S_k)	Permutation (sans *Steckerbrett*)
...	...	...
PFH	$(8, 8, 2, 2, 2, 2, 1, 1)$	(AWROCEUS)(BMYJLTVI)(DF)(HQ)(KP)(XZ)(G)(N)
PFI	$(7, 7, 5, 5, 1, 1)$	(BZEPCRN)(DIHWVGX)(ATYSQ)(FJKUM)(L)(O)
PFJ	$(6, 6, 3, 3, 2, 2, 2, 2)$	(AXYKZT)(BMHGPL)(NVS)(OUW)(CD)(EJ)(FI)(QR)
PFK	$(13, 13)$	(AJPRTFBDSGHCE)(IXUZWLQOVMYKN)
PFL	$(7, 7, 4, 4, 2, 2)$	(BNPTKXD)(ESMGHIZ)(JRLU)(OWQY)(AC)(FV)
PFM	$(8, 8, 4, 4, 1, 1)$	(BDJVRZPM)(COFQKYTL)(ASIN)(EWGU)(H)(X)
PFN	$(11, 11, 1, 1, 1, 1)$	(AQTHDYGOWSJ)(EUNLRMVXFPI)(B)(C)(K)(Z)
...	...	...

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :
  - précalculer (une fois pour toutes) une table avec les caractéristiques des permutations $S_k = \sigma_{\mathrm{RR},k+3} \circ \sigma_{\mathrm{RR},k}$, pour toutes les configurations possibles k des rotors :

Configuration k	Carac(S_k)	Permutation (sans *Steckerbrett*)
...	...	...
PFH	$(8,8,2,2,2,2,1,1)$	(AWROCEUS)(BMYJLTVI)(DF)(HQ)(KP)(XZ)(G)(N)
PFI	$(7,7,5,5,1,1)$	(BZEPCRN)(DIHWVGX)(ATYSQ)(FJKUM)(L)(O)
PFJ	$(6,6,3,3,2,2,2,2)$	(AXYKZT)(BMHGPL)(NVS)(OUW)(CD)(EJ)(FI)(QR)
PFK	$(13,13)$	(AJPRTFBDSGHCE)(IXUZWLQOVMYKN)
PFL	$(7,7,4,4,2,2)$	(BNPTKXD)(ESMGHIZ)(JRLU)(OWQY)(AC)(FV)
PFM	$(8,8,4,4,1,1)$	(BDJVRZPM)(COFQKYTL)(ASIN)(EWGU)(H)(X)
PFN	$(11,11,1,1,1,1)$	(AQTHDYGOWSJ)(EUNLRMVXFPI)(B)(C)(K)(Z)
...	...	...

  - intercepter plusieurs messages chiffrés dans la même journée

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :
  - précalculer (une fois pour toutes) une table avec les caractéristiques des permutations $S_k = \sigma_{\mathrm{RR},k+3} \circ \sigma_{\mathrm{RR},k}$, pour toutes les configurations possibles k des rotors :

Configuration k	Carac(S_k)	Permutation (sans *Steckerbrett*)
...	...	...
PFH	$(8,8,2,2,2,2,1,1)$	(AWROCEUS)(BMYJLTVI)(DF)(HQ)(KP)(XZ)(G)(N)
PFI	$(7,7,5,5,1,1)$	(BZEPCRN)(DIHWVGX)(ATYSQ)(FJKUM)(L)(O)
PFJ	$(6,6,3,3,2,2,2,2)$	(AXYKZT)(BMHGPL)(NVS)(OUW)(CD)(EJ)(FI)(QR)
PFK	$(13,13)$	(AJPRTFBDSGHCE)(IXUZWLQOVMYKN)
PFL	$(7,7,4,4,2,2)$	(BNPTKXD)(ESMGHIZ)(JRLU)(OWQY)(AC)(FV)
PFM	$(8,8,4,4,1,1)$	(BDJVRZPM)(COFQKYTL)(ASIN)(EWGU)(H)(X)
PFN	$(11,11,1,1,1,1)$	(AQTHDYGOWSJ)(EUNLRMVXFPI)(B)(C)(K)(Z)
...	...	...

  - intercepter plusieurs messages chiffrés dans la même journée
  - calculer la caractéristique de chaque permutation $\tilde{S}_{k_0+1}$, $\tilde{S}_{k_0+2}$ et $\tilde{S}_{k_0+3}$:

$$\mathrm{Carac}(\tilde{S}_{k_0+1}) = (6,6,3,3,2,2,2,2)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+2}) = (13,13)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+3}) = (7,7,4,4,2,2)$$

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :
  - précalculer (une fois pour toutes) une table avec les caractéristiques des permutations $S_k = \sigma_{\mathrm{RR},k+3} \circ \sigma_{\mathrm{RR},k}$, pour toutes les configurations possibles k des rotors :

Configuration k	Carac(S_k)	Permutation (sans *Steckerbrett*)
...	...	...
PFH	$(8,8,2,2,2,2,1,1)$	(AWROCEUS)(BMYJLTVI)(DF)(HQ)(KP)(XZ)(G)(N)
PFI	$(7,7,5,5,1,1)$	(BZEPCRN)(DIHWVGX)(ATYSQ)(FJKUM)(L)(O)
PFJ	$(6,6,3,3,2,2,2,2)$	(AXYKZT)(BMHGPL)(NVS)(OUW)(CD)(EJ)(FI)(QR)
PFK	$(13,13)$	(AJPRTFBDSGHCE)(IXUZWLQOVMYKN)
PFL	$(7,7,4,4,2,2)$	(BNPTKXD)(ESMGHIZ)(JRLU)(OWQY)(AC)(FV)
PFM	$(8,8,4,4,1,1)$	(BDJVRZPM)(COFQKYTL)(ASIN)(EWGU)(H)(X)
PFN	$(11,11,1,1,1,1)$	(AQTHDYGOWSJ)(EUNLRMVXFPI)(B)(C)(K)(Z)
...	...	...

  - intercepter plusieurs messages chiffrés dans la même journée
  - calculer la caractéristique de chaque permutation $\tilde{S}_{k_0+1}$, $\tilde{S}_{k_0+2}$ et $\tilde{S}_{k_0+3}$:

$$\mathrm{Carac}(\tilde{S}_{k_0+1}) = (6,6,3,3,2,2,2,2)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+2}) = (13,13)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+3}) = (7,7,4,4,2,2)$$

Méthode des caractéristiques de Rejewski

- Idée de Rejewski :
  - précalculer (une fois pour toutes) une table avec les caractéristiques des permutations $S_k = \sigma_{\mathrm{RR},k+3} \circ \sigma_{\mathrm{RR},k}$, pour toutes les configurations possibles k des rotors :

Configuration k	Carac(S_k)	Permutation (sans *Steckerbrett*)
...	...	...
PFH	$(8,8,2,2,2,2,1,1)$	(AWROCEUS)(BMYJLTVI)(DF)(HQ)(KP)(XZ)(G)(N)
PFI	$(7,7,5,5,1,1)$	(BZEPCRN)(DIHWVGX)(ATYSQ)(FJKUM)(L)(O)
PFJ	$(6,6,3,3,2,2,2,2)$	(AXYKZT)(BMHGPL)(NVS)(OUW)(CD)(EJ)(FI)(QR)
PFK	$(13,13)$	(AJPRTFBDSGHCE)(IXUZWLQOVMYKN)
PFL	$(7,7,4,4,2,2)$	(BNPTKXD)(ESMGHIZ)(JRLU)(OWQY)(AC)(FV)
PFM	$(8,8,4,4,1,1)$	(BDJVRZPM)(COFQKYTL)(ASIN)(EWGU)(H)(X)
PFN	$(11,11,1,1,1,1)$	(AQTHDYGOWSJ)(EUNLRMVXFPI)(B)(C)(K)(Z)
...	...	...

  - intercepter plusieurs messages chiffrés dans la même journée
  - calculer la caractéristique de chaque permutation $\tilde{S}_{k_0+1}$, $\tilde{S}_{k_0+2}$ et $\tilde{S}_{k_0+3}$:

$$\mathrm{Carac}(\tilde{S}_{k_0+1}) = (6,6,3,3,2,2,2,2)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+2}) = (13,13)$$
$$\mathrm{Carac}(\tilde{S}_{k_0+3}) = (7,7,4,4,2,2)$$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : `OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC`

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : `OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC`
  - crib supposé : `OBERKOMMANDO`

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : `OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC`
  - crib supposé : `OBERKOMMANDO`
- Rappel : une lettre ne peut jamais être chiffrée en elle-même

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
..OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : `OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC`
  - crib supposé : `OBERKOMMANDO`
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}\,(\mathrm{O}) = \mathrm{L}$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathrm{O}) = \mathrm{L}$ et $\sigma_{k_0+6}(\mathrm{L}) = \mathrm{O}$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathtt{O}) = \mathtt{L}$ et $\sigma_{k_0+6}(\mathtt{L}) = \mathtt{O}$
  - $\sigma_{k_0+13}(\mathtt{M}) = \mathtt{O}$ et $\sigma_{k_0+13}(\mathtt{O}) = \mathtt{M}$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathtt{O}) = \mathtt{L}$ et $\sigma_{k_0+6}(\mathtt{L}) = \mathtt{O}$
  - $\sigma_{k_0+13}(\mathtt{M}) = \mathtt{O}$ et $\sigma_{k_0+13}(\mathtt{O}) = \mathtt{M}$
  - $\sigma_{k_0+12}(\mathtt{M}) = \mathtt{N}$ et $\sigma_{k_0+12}(\mathtt{N}) = \mathtt{M}$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathtt{O}) = \mathtt{L}$ et $\sigma_{k_0+6}(\mathtt{L}) = \mathtt{O}$
  - $\sigma_{k_0+13}(\mathtt{M}) = \mathtt{O}$ et $\sigma_{k_0+13}(\mathtt{O}) = \mathtt{M}$
  - $\sigma_{k_0+12}(\mathtt{M}) = \mathtt{N}$ et $\sigma_{k_0+12}(\mathtt{N}) = \mathtt{M}$
  - $\sigma_{k_0+17}(\mathtt{O}) = \mathtt{N}$ et $\sigma_{k_0+17}(\mathtt{N}) = \mathtt{O}$

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathtt{O}) = \mathtt{L}$ et $\sigma_{k_0+6}(\mathtt{L}) = \mathtt{O}$
  - $\sigma_{k_0+13}(\mathtt{M}) = \mathtt{O}$ et $\sigma_{k_0+13}(\mathtt{O}) = \mathtt{M}$
  - $\sigma_{k_0+12}(\mathtt{M}) = \mathtt{N}$ et $\sigma_{k_0+12}(\mathtt{N}) = \mathtt{M}$
  - $\sigma_{k_0+17}(\mathtt{O}) = \mathtt{N}$ et $\sigma_{k_0+17}(\mathtt{N}) = \mathtt{O}$
  - ...

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{k_0+6}(\mathtt{O}) = \mathtt{L}$ et $\sigma_{k_0+6}(\mathtt{L}) = \mathtt{O}$
  - $\sigma_{k_0+13}(\mathtt{M}) = \mathtt{O}$ et $\sigma_{k_0+13}(\mathtt{O}) = \mathtt{M}$
  - $\sigma_{k_0+12}(\mathtt{M}) = \mathtt{N}$ et $\sigma_{k_0+12}(\mathtt{N}) = \mathtt{M}$
  - $\sigma_{k_0+17}(\mathtt{O}) = \mathtt{N}$ et $\sigma_{k_0+17}(\mathtt{N}) = \mathtt{O}$
  - ...

Cryptanalyse britannique : crib et menus

- Suppose la connaissance d'un *crib* : un morceau du message clair
  - message chiffré : OLOEY LXMYA SNOOK TNEWS OMZFX TPQBE ATORW FQTFA FDC
  - crib supposé : OBERKOMMANDO
- Rappel : une lettre ne peut jamais être chiffrée en elle-même
- On peut utiliser cette propriété pour aligner message chiffré et crib :

```
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
OLOEYLXMYASNOOKTNEWSOMZFXTPQBEATORWFQTFAFDC
.....OBERKOMMANDO
```

- On regarde alors les liens entre les différentes lettres en clair et les chiffrés correspondants :
  - $\sigma_{\mathrm{RR},k_0+6}\left(\sigma_{\mathrm{Steck}}(\mathtt{O})\right) = \sigma_{\mathrm{Steck}}(\mathtt{L})$ et $\sigma_{\mathrm{RR},k_0+6}\left(\sigma_{\mathrm{Steck}}(\mathtt{L})\right) = \sigma_{\mathrm{Steck}}(\mathtt{O})$
  - $\sigma_{\mathrm{RR},k_0+13}(\sigma_{\mathrm{Steck}}(\mathtt{M})) = \sigma_{\mathrm{Steck}}(\mathtt{O})$ et $\sigma_{\mathrm{RR},k_0+13}(\sigma_{\mathrm{Steck}}(\mathtt{O})) = \sigma_{\mathrm{Steck}}(\mathtt{M})$
  - $\sigma_{\mathrm{RR},k_0+12}(\sigma_{\mathrm{Steck}}(\mathtt{M})) = \sigma_{\mathrm{Steck}}(\mathtt{N})$ et $\sigma_{\mathrm{RR},k_0+12}(\sigma_{\mathrm{Steck}}(\mathtt{N})) = \sigma_{\mathrm{Steck}}(\mathtt{M})$
  - $\sigma_{\mathrm{RR},k_0+17}(\sigma_{\mathrm{Steck}}(\mathtt{O})) = \sigma_{\mathrm{Steck}}(\mathtt{N})$ et $\sigma_{\mathrm{RR},k_0+17}(\sigma_{\mathrm{Steck}}(\mathtt{N})) = \sigma_{\mathrm{Steck}}(\mathtt{O})$
  - ...

Pour en savoir plus

- https://en.wikipedia.org/wiki/Enigma_machine
- http://www.matematiksider.dk/enigma_eng.html
- http://www.ellsbury.com/enigmabombe.htm
- http://users.telenet.be/d.rijmenants/en/enigmamenu.htm

Vue d'ensemble