Enigma: decifrare una vittoria

I polacchi (e la matematica) al servizio dell'Europa

La matematica di Enigma

Permutazioni

Una permutazione di un insieme X è una funzione bigettiva (biettiva, iniettiva e suriettiva) da X in X.

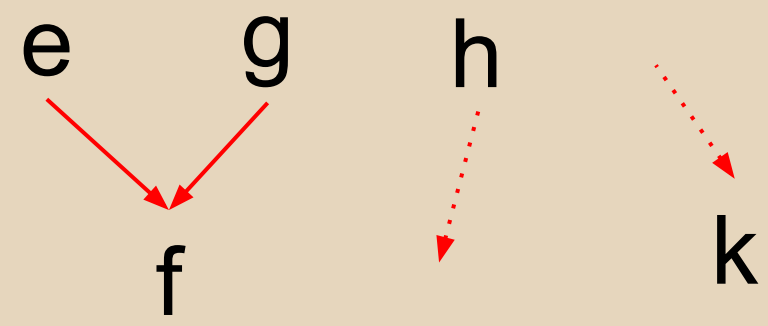
Noi siamo interessati al caso

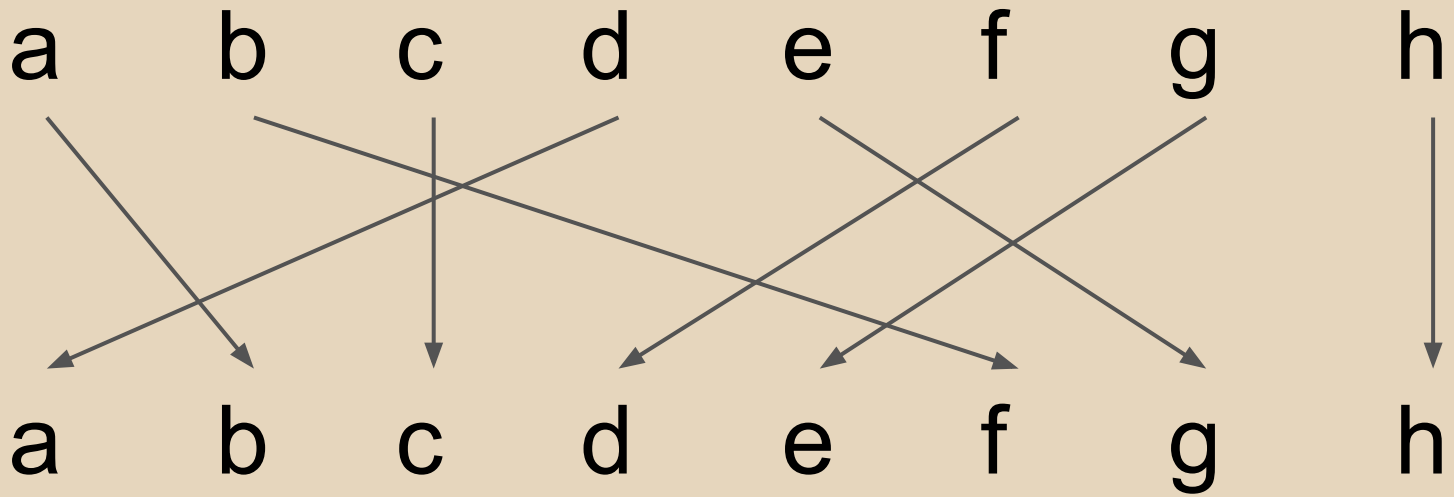
X={a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}

Scriveremo **I** per la permutazione identica, cioè quella che manda ogni elemento in sè stesso.

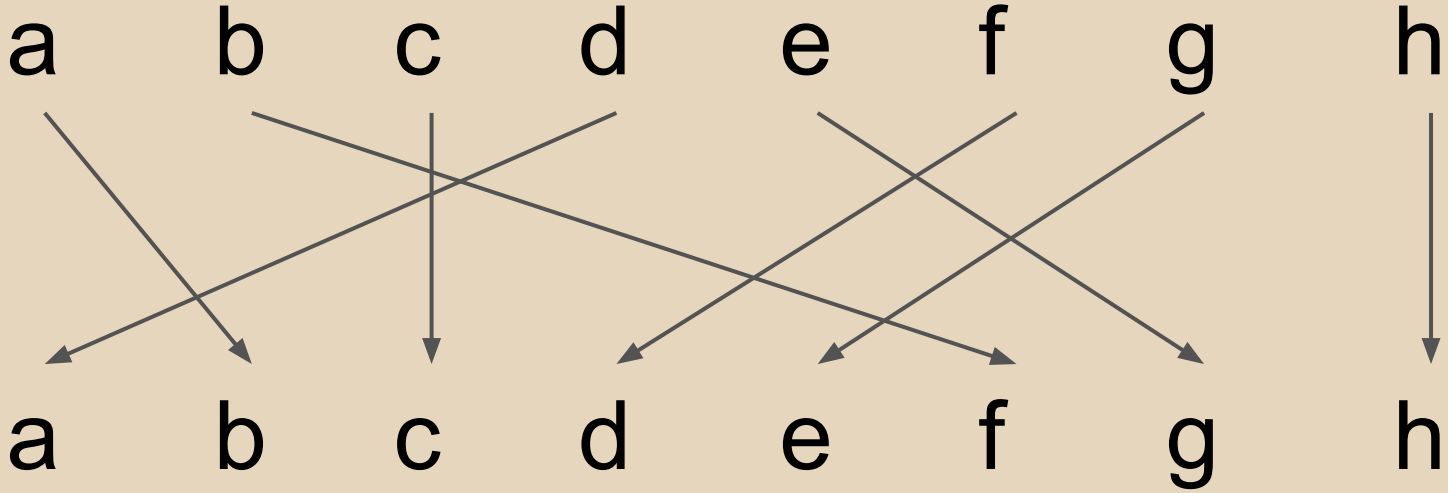
Permutazioni

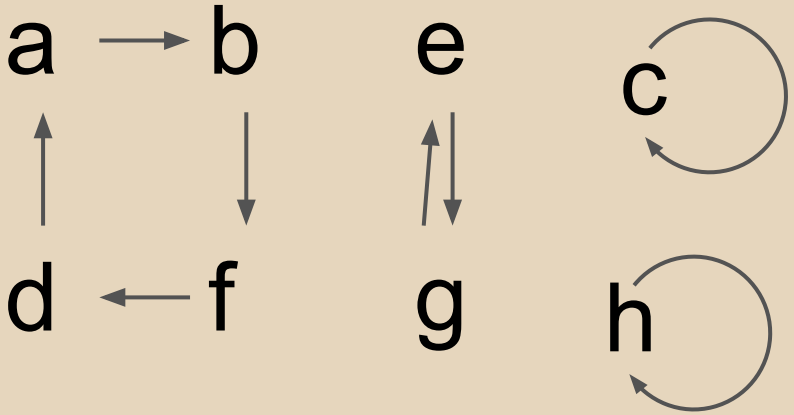
Vietato:





Decomposizione in cicli





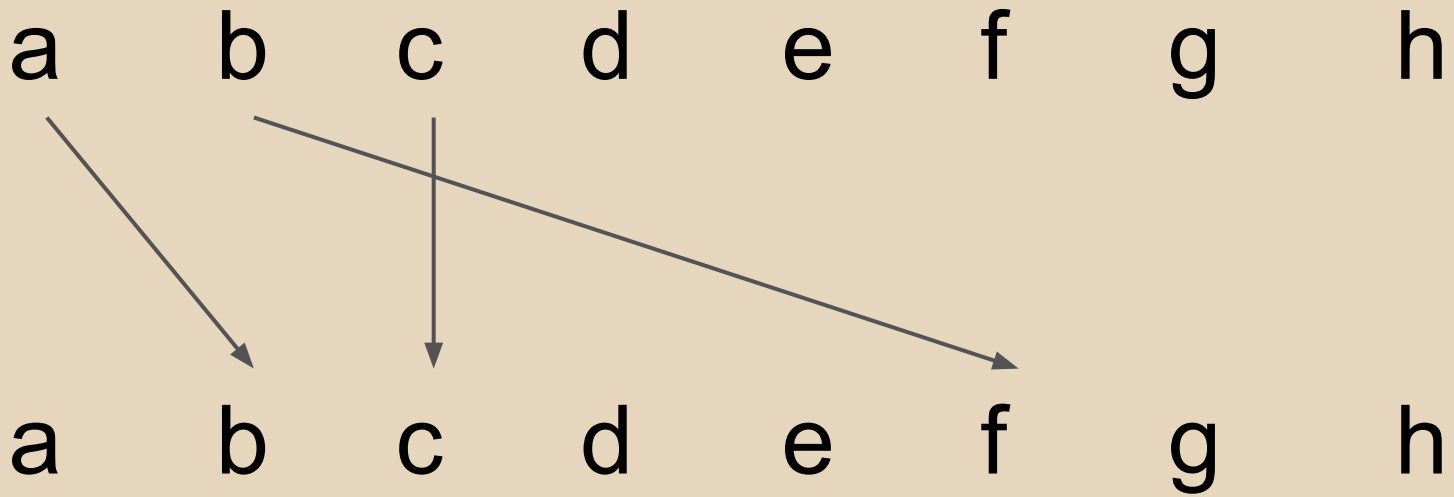
A=(abfd)(eg)(c)(h)
=(abfd)(eg)
=(fdab)(ge)

Quante sono le permutazioni di 26 lettere?

Per a ho 26 scelte, per b 25, per c 24, etc.

In totale, 26*25*24*...*2*1=26!

26! è circa $4*10^{26}$ cioè circa 4 centinaia di milioni di miliardi di miliardi.

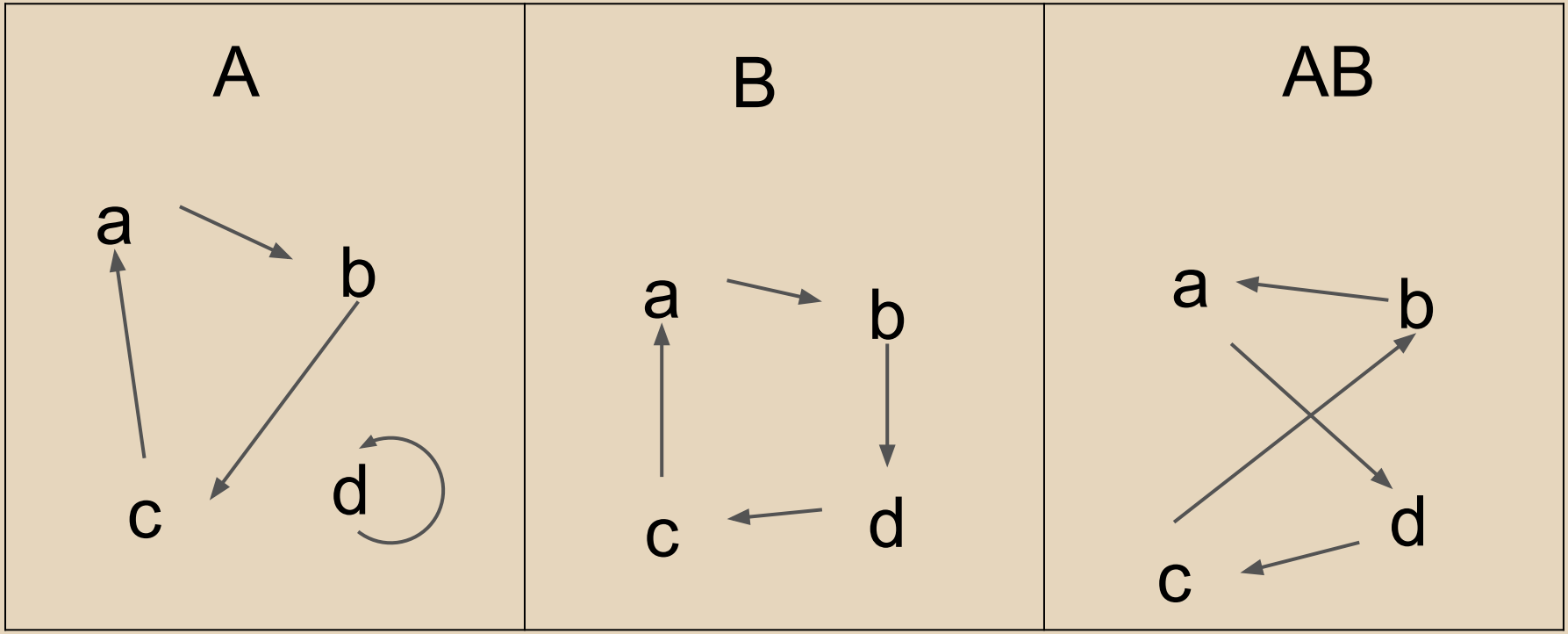


Composizione di permutazioni

Siano A e B due permutazioni. Scriveremo AB per la permutazione che si ottiene facendo prima A e poi B.

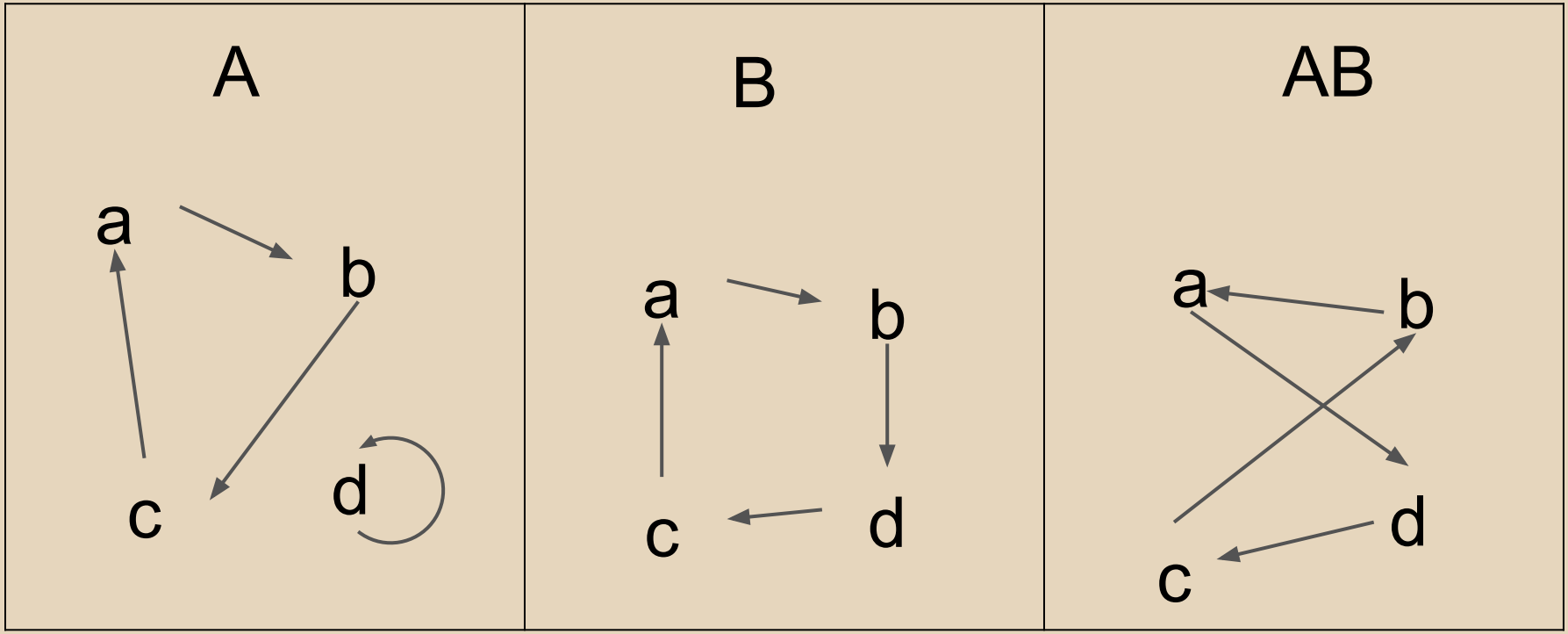
Composizione di permutazioni

Siano A e B due permutazioni. Scriveremo AB per la permutazione che si ottiene facendo prima A e poi B.



Composizione di permutazioni

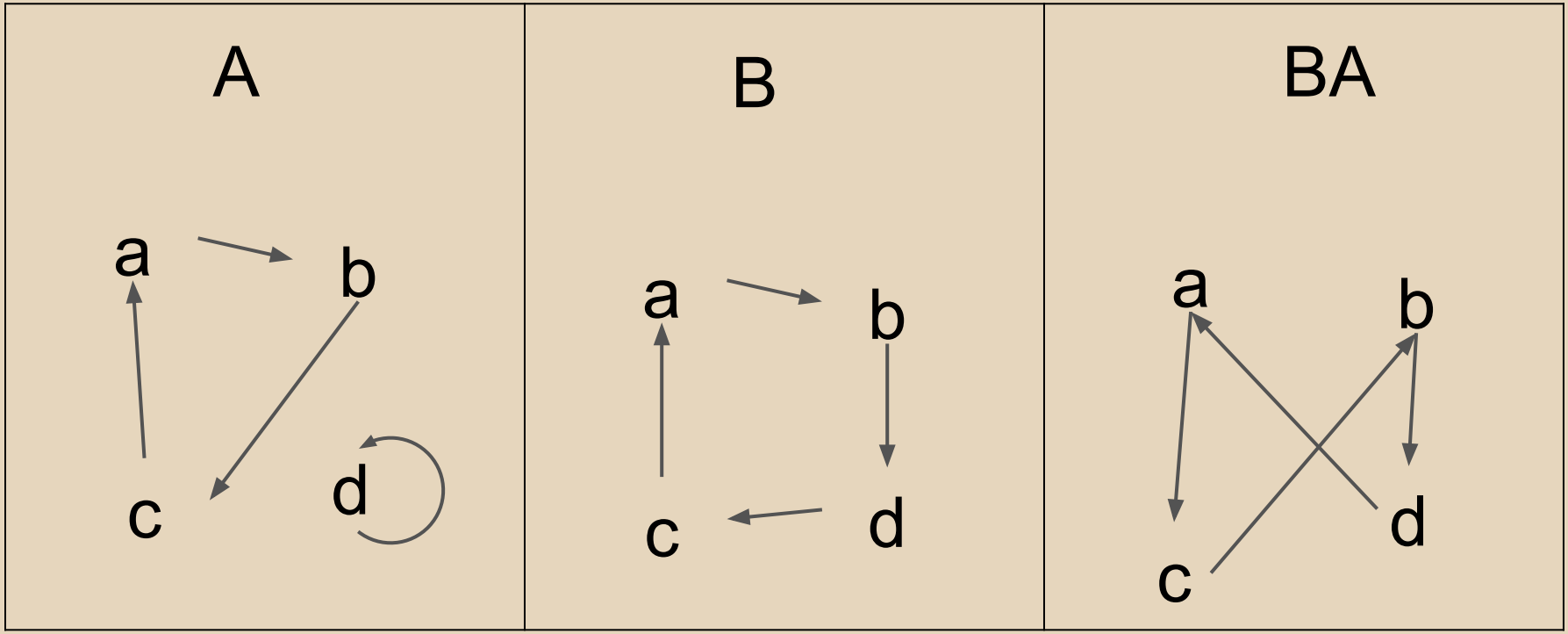
Quindi A=(abc)(d) B=(abdc) AB=(adcb).



L'ordine è importante!

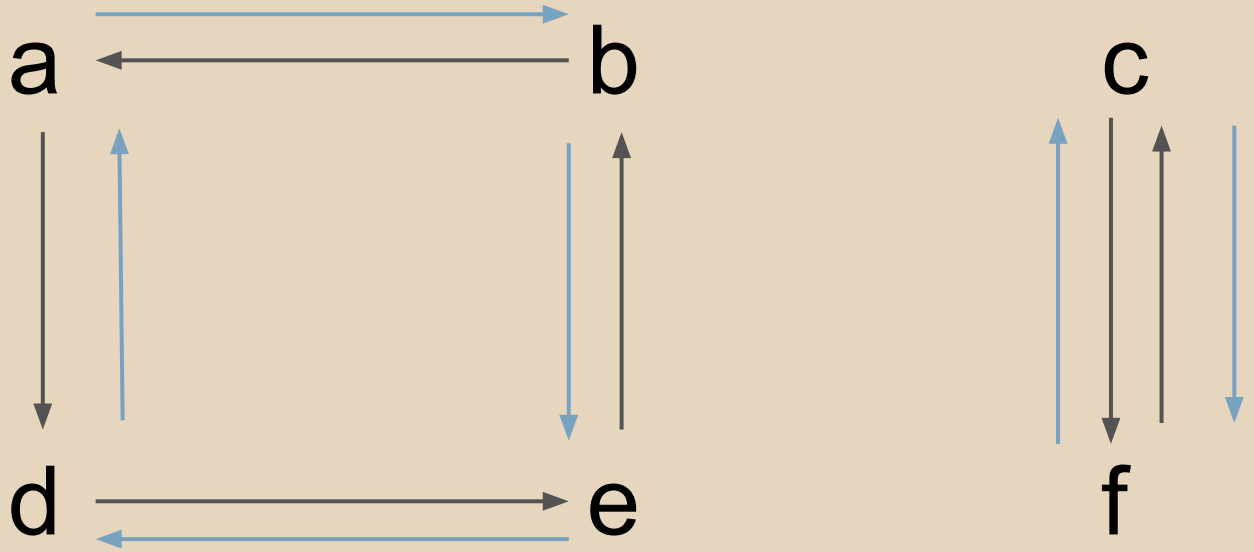
In generale AB è diversa da BA.

Se A=(abc)(d) B=(abdc), allora AB=(adcb) ma BA=(acbd)



Permutazione inversa

Sia A una permutazione. Scriviamo A^{-1} per la sua inversa, cioè quella con le frecce al contrario. Abbiamo $AA^{-1}=I$ e $A^{-1}A=I$. In questo caso $A=(adeb)(cf)$ $A^{-1}=(abed)(cf)$



Gruppo

Le permutazioni di un insieme formano un gruppo.

In un gruppo possiamo risolvere equazioni:

$AX=B \qquad A^{-1}AX=A^{-1}B \qquad X=A^{-1}B$

oppure

$XA=B \qquad XAA^{-1}=BA^{-1} \qquad X=BA^{-1}$

oppure

$AXB=C \qquad X=A^{-1}CB^{-1}$

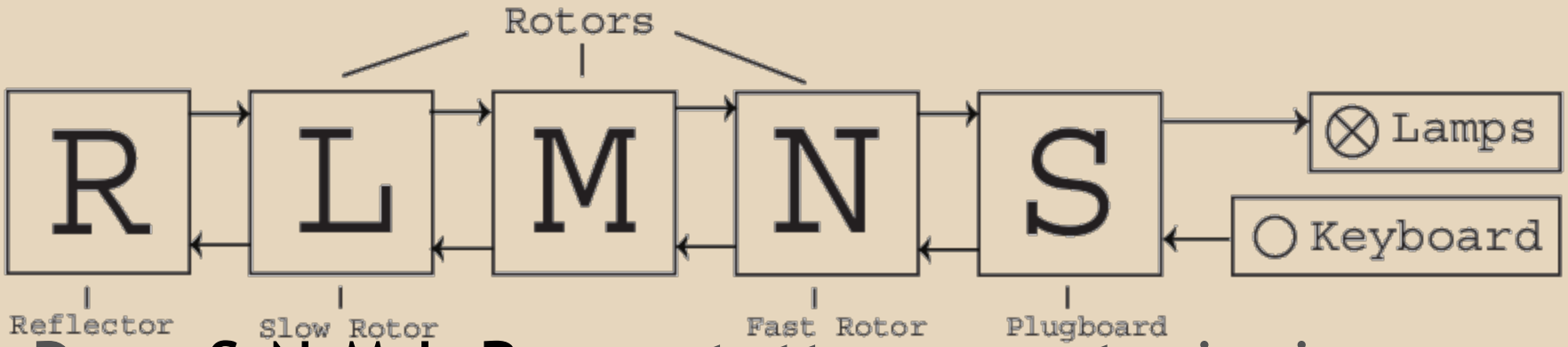
Permutazioni di Enigma

Ma si voleva che se schiacciando X si illumina Y, allora schiacciando Y si illuminasse X, quindi tutte le permutazioni A di Enigma sono inverse di se stesse, cioè $A=A^{-1}$ e quindi $AA=I$.

Allora tutte le permutazioni possono essere fatte di cicli con al più due elementi, e queste sono circa $7*10^{12}$, cioè molte meno di $4*10^{26}$.

Le permutazioni di enigma

Ecco il diagramma funzionale:



Dove S,N,M,L,R sono tutte permutazioni.
Quindi la permutazione totale sarà

$$SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$$

I rotori girano...

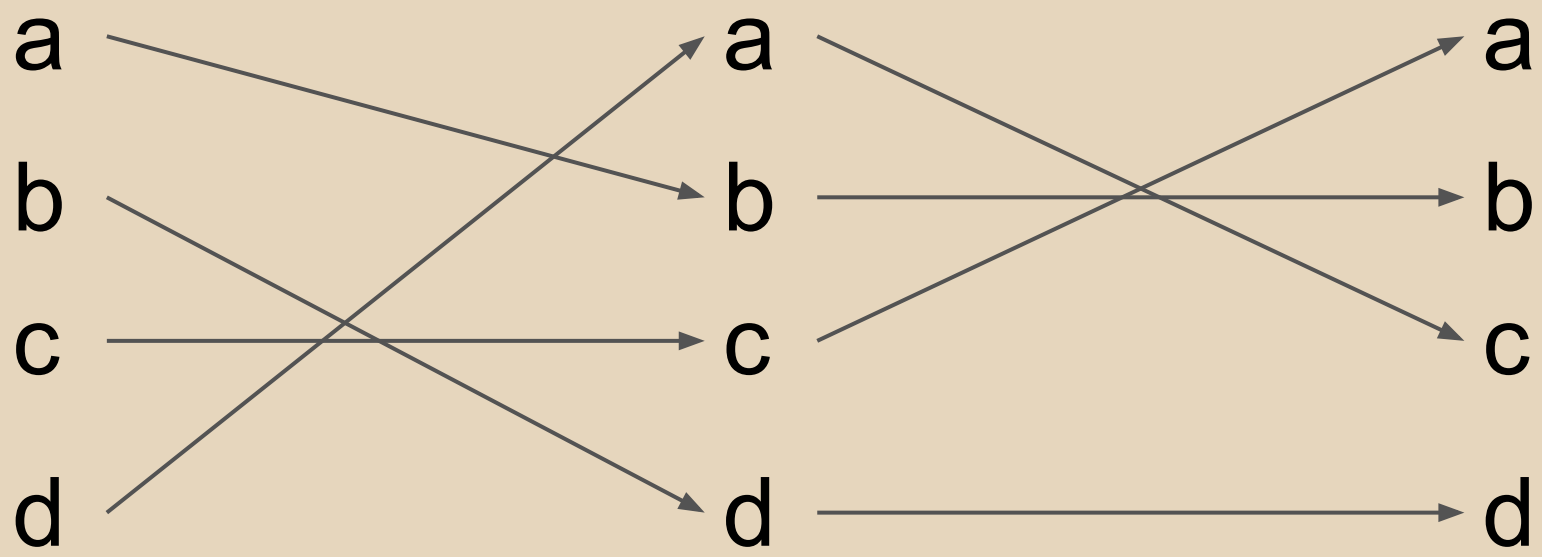
Cosa succede ad N quando gira di uno scatto?

N diventa PN dove P è la permutazione che corrisponde all'avanzamento di uno scatto.

P=(abdcefghijklmnopqrstuvwxyz)

Composizione e inverse

Siano A e B due permutazioni, con relative inverse A^{-1} e B^{-1}. Com'è fatta l'inversa di AB?



Quindi $(AB)^{-1}=B^{-1}A^{-1}$

I rotori girano...

La prima lettera è soggetta alla permutazione

$A=SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$

La seconda, N diventa PN e $(PN)^{-1}=P^{-1}N^{-1}$

$B=SPNMLRL^{-1}M^{-1}N^{-1}P^{-1}S^{-1}=(SPNML)R(SPNML)^{-1}$

Quindi

$C=SPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}S^{-1}=(SP^2NML)R(SP^2NM)^{-1}$

$D=(SPPPNML)R(SPPPNML)^{-1}$

$E=(SPPPPNML)R(SPPPPNML)^{-1}$

$F=(SPPPPNML)R(SPPPPNML)^{-1}$

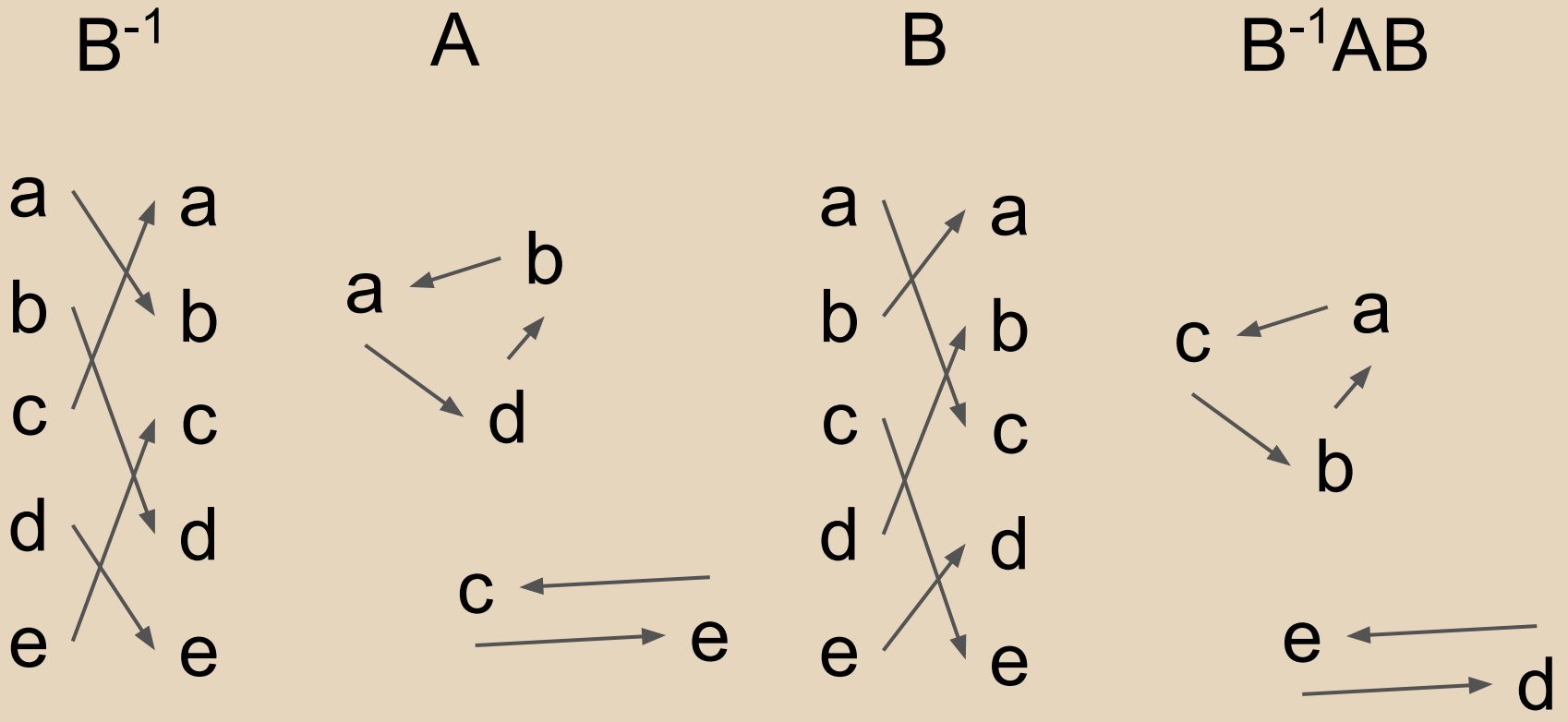
Coniugato

Sia A e B due permutazioni, allora il coniugio di A rispetto a B è la permutazione $B^{-1}AB$.

Cosa succede ai cicli dentro A?

Restano uguali in forma e dimensione.

"Dimostrazione"



Il riflettore

Il riflettore è una permutazione particolare, infatti per costruzione R scambia tutte le lettere a due a due, cioè è fatta solo da cicli con due elementi. Per esempio

$$R=(ab)(cd)(ef)(gh)(ij)(kl)(mn)(op)(qr)(st)(uv)(wx)(yz)$$

Notiamo che $RR=I$ quindi $R=R^{-1}$.

Conseguenze

Dalle equazioni

$A=(SNML)R(SNML)^{-1}$ $B=(SPNML)R(SPNML)^{-1}$

$C=(SPPNML)R(SPPNM)^{-1}$ $D=(SPPPNML)R(SPPPNML)^{-1}$

$E=(SPPPPNML)R(SPPPPNML)^{-1}$

$F=(SPPPPNML)R(SPPPPNML)^{-1}$

vediamo che tutte le permutazini sono coniugate al riflettore, quindi sono tutte composte da 13 cicli con due elementi.

Cosa sappiamo

AUQ	AMN	IND	JHU	PVJ	FEG	SJM	SPO	WTM	RAO
BNH	CHL	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
BCT	CGJ	JWF	MIC	QGA	LYB	SJM	SPO	WTM	RAO
CIK	BZT	KHB	XJV	RJL	WPX	SUG	SMF	WKI	RKK
DDB	VDV	KHB	XJV	RJL	WPX	SUG	SMF	XRS	GNM
EJP	IPS	LDR	HDE	RJL	WPX	TMN	EBY	XRS	GNM
FBR	KLE	LDR	HDE	RJL	WPX	TMN	EBY	XOI	GUK
GPB	ZSV	MAW	UXP	RFC	WQQ	TAA	EXB	XYW	GCP
HNO	THD	MAW	UXP	SYX	SCW	USE	NWH	YPC	OSQ
HNO	THD	NXD	QTU	SYX	SCW	VII	PZK	YPC	OSQ
HXV	TTI	NXD	QTU	SYX	SCW	VII	PZK	ZZY	YRA
IKG	JKF	NLU	QFZ	SYX	SCW	VQZ	PVR	ZEF	YOC
IKG	JKF	OBU	DLZ	SYZ	SCW	VQZ	PVR	ZSJ	YWG

Sappiamo che la prima lettera è mandata da A in A e da D in A. Quindi AD^{-1} manda A in A. Ma DD=I e quindi AD^{-1}=AD.

Equazioni

Come visto, possiamo scorrere e trovare le composizioni:

AD=(a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s)
BE=(axt)(blfqveoum)(cgy)(d)(hjpswizrn)(k)
CF=(abviktjgfcqny)(duzrehlxwpsmo)

Abbiamo, tre equazioni e sei incognite.

Ma $A=SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$ e

$D=SPPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1}S^{-1}$

$AD=$

$SNMLRL^{-1}M^{-1}N^{-1}S^{-1}SPPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1}S^{-1}=$

$S(NMLRL^{-1}M^{-1}N^{-1})S^{-1}S(PPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1})S^{-1}$

Ma $A=SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$ e

$D=SPPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1}S^{-1}$

$AD=$

$SNMLRL^{-1}M^{-1}N^{-1}S^{-1}SPPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1}S^{-1}=$

$S(NMLRL^{-1}M^{-1}N^{-1})S^{-1}S(PPPNMLRL^{-1}M^{-1}N^{-1}P^{-1}P^{-1}P^{-1})S^{-1}$

E le due permutazioni fra parentesi non includono S. Ma allora posso dimenticare S per trovare la struttura ciclica di AD. Fattorizzando, si trovano A,B,C,D,E,F.

Ritorniamo alle equazioni originali.

Per brevità, scriviamo $Q=MLRL^{-1}M^{-1}$ quindi

$A=SNQN^{-1}S^{-1}$

$B=SPNP^{-1}QPN^{-1}P^{-1}S^{-1}$

$C=SP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}S^{-1}$

$D=SP^{3}NP^{-3}QP^{3}N^{-1}P^{-3}S^{-1}$

$E=SP^{4}NP^{-4}QP^{4}N^{-1}P^{-4}S^{-1}$

$F=SP^{5}NP^{-5}QP^{5}N^{-1}P^{-5}S^{-1}$

Ora i membri a sinistra sono conosciuti.

Nel dicembre del 1932, furono recuperati delle chiavi, per cui S era conosciuta.

$S^{-1}AS=NQN^{-1}$

$S^{-1}BS=PNP^{-1}QPN^{-1}P^{-1}$

$S^{-1}CS=P^{2}NP^{-2}QP^{2}N^{-1}P^{-2}$

$S^{-1}DS=P^{3}NP^{-3}QP^{3}N^{-1}P^{-3}$

$S^{-1}ES=P^{4}NP^{-4}QP^{4}N^{-1}P^{-4}$

$S^{-1}FS=P^{5}NP^{-5}QP^{5}N^{-1}P^{-5}$

Ma anche P è conosciuta, quindi:

$S^{-1}AS=NQN^{-1}$

$P^{-1}S^{-1}BSP=NP^{-1}QPN^{-1}$

$P^{-2}S^{-1}CSP^{2}=NP^{-2}QP^{2}N^{-1}$

$P^{-3}S^{-1}DSP^{3}=NP^{-3}QP^{3}N^{-1}$

$P^{-4}S^{-1}ESP^{4}=NP^{-4}QP^{4}N^{-1}$

$P^{-5}S^{-1}FSP^{5}=NP^{-5}QP^{5}N^{-1}$

Facendo dei prodotti incrociati:

$S^{-1}ASP^{-1}S^{-1}BSP=NQN^{-1}NP^{-1}QPN^{-1}=N(QP^{-1}QP)N^{-1}$

$P^{-2}S^{-1}CSP^{2}P^{-3}S^{-1}DSP^{3}=NP^{-2}QP^{2}N^{-1}NP^{-3}QP^{3}N^{-1}=$
$NP^{-2}(QP^{-1}QP)P^{2}N^{-1}$

$P^{-4}S^{-1}ESP^{4}P^{-5}S^{-1}FSP^{5}=NP^{-4}QP^{4}N^{-1}NP^{-5}QP^{5}N^{-1}=$
$NP^{-4}(QP^{-1}QP)P^{4}N^{-1}$

Facendo dei prodotti incrociati:

$N^{-1}S^{-1}ASP^{-1}S^{-1}BSPN=QP^{-1}QP$

$P^{-2}S^{-1}CSP^{2}P^{-3}S^{-1}DSP^{3}=NP^{-2}(QP^{-1}QP)P^{2}N^{-1}=$
$NP^{-2}N^{-1}S^{-1}ASP^{-1}S^{-1}BSPNP^{2}N^{-1}=$
$(NP^{-2}N^{-1})S^{-1}ASP^{-1}S^{-1}BSP(NP^{-2}N^{-1})^{-1}$

Ma ora $B=XAX^{-1}$ è risolvibile.

Fine

Grazie a tutti!

Bibliografia

Riferimenti bibliografici:

- Christensen, Chris "Polish mathematicians finding patterns in Enigma messages", Mathematics Magazine 80 (2007) n. 4, pp. 247-273
- Rejewski, Marian "How Polish mathematicians deciphered `Enigma' (translation)" Annals of the History of Computing vol. 3 n. 3 (July 1982) pp.213-234

Slide aggiuntive

Le sguenti slide erano state preparate in caso di domande specifiche ma non sono state utilizzate

Evoluzione

Macchina	Possibilità della macchina	Quanti zeri
Enigma (senza sapere come funziona)	26!=26*25*...*2*1	26
Enigma (coniugato del riflettore)	(26 2)(24 2)...(2 2) /13!	12
Enigma (con 3 rotori e 6 scambi)	100391791600*6*67 6*17576	18
Enigma (con 4 rotori e 10 scambi)	150738274937250* 24*17576*456976	25

Variabilità e entropia

settaggio	variabilità	entropia	lettera	enigma 2.0
dalla tastiera alla plugboard	nessuna	nessuna		nessuna
plugboard	giornaliera	100,391,791,500	S	150,738,274,937,250
rotore I II e III	tre mesi	6	N, M, L	24
setting rotore	giornaliera	676		17576
groundsetting	giornaliera	17576		456976
riflettore	nessuna	nessuna	R	
message key	per messaggio	676		17576