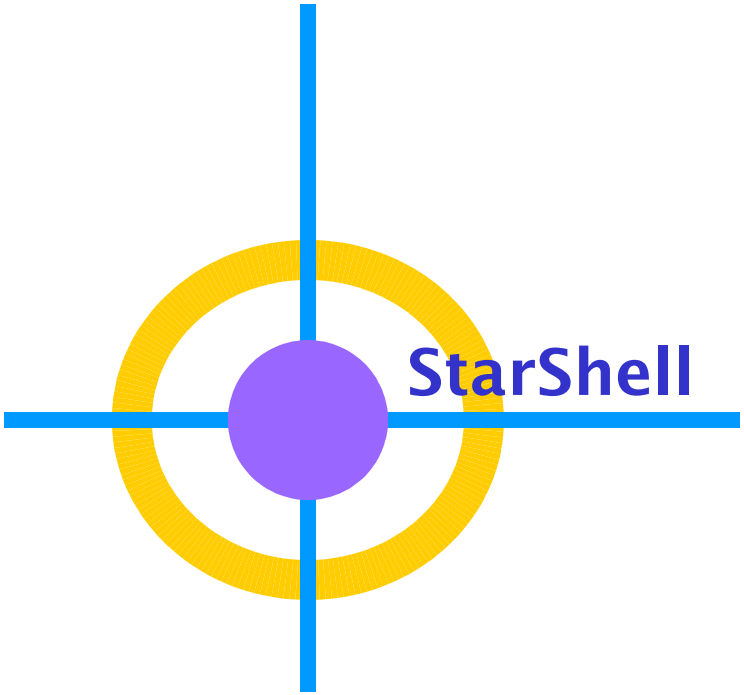


Crittografia Classica

Il Disco di Festo

Località Pre-Minoica
Isola di Creta
Lingua sconosciuta
Forse simboli magici o propiziatori?

Crittografia nei Testi Sacri

- Bibbia
  - Tre tecniche di cifratura:
    - **Atbash - alfabeto rovesciato**
      - **aleph, taw, beth, shin, ...**
      - **cifra di Babilonia nel libro di Geremia**
    - **Albam - alfabeto diviso in due metà**
    - **Atbah - relazione numerica**
      - **per le prime nove:**
      - **lettera da sostituire + lettera sostituente = 10**
      - **per le successive:**
      - **lettera da sostituire + lettera sostituente = 28**

cf. "Il Codice Da Vinci" di Dan Brown

Termini di Crittografia

- A: Vocabolario e set di caratteri **V** in chiaro
- B: Testo cifrato, codice o testo crittato e insieme di caratteri **W**
  - **Possono essere diversi, sovrapposti o identici**
  - **Set di caratteri del computer: sequenze di bit**
- Crittazione: mappa da A a B (iniettiva - A può generare uno o più B) **V -> W**
- Decrittazione: mappa inversa da B ad A **W -> V**
- La Crittazione è complessa: insieme finito di mappaggi - passi della crittografazione
  - **possono essere specificati da una tabella di crittazione**
- Somma di passi di crittazione = sistema di crittazione
- Sistema di crittazione + sistema di decrittazione = sistema crittografico

Termini di Crittografia

- **Omofoni** (varianti): un carattere in chiaro crittografato con più caratteri crittati
- **Nulli** (dummy): aggiunti al testo in chiaro prima della crittografazione (ε)
- **Crittografia monoalfabetica**: corrispondenza 1 a 1 tra caratteri in chiaro e crittati
- **Polialfabetica**: corrispondenza n a n
  - **non trivialmente periodica - requisito di base**
- **Chiave**: sequenza di caratteri usata in un passo di crittografazione con un algoritmo appropriato
  - **Occorre cambiare le chiavi per evitare periodicità**
  - **La chiave ottimale è lunga come il messaggio da crittografare**
- **Blocchi**: unità di crittografazione di più caratteri

Sostituzioni Semplici

- **V^1 -> W**
  - **crittografazione eterogenea con o senza omofoni e nulli**
- **V -> V**
  - **Permutazioni**
  - **Caso speciale: permutazioni autoreciproche**
- Riflessioni
  - **sottoinsieme di permutazioni reciproche (solo alcune lettere)**
  - **Chiamata anche 'a connessioni incrociate' (Enigma)**
- Alfabeti misti e cicli

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

(a s n h y x w v q l f i) (b e r m g t o j) (c) (d u p k) (z)
```

Cifrario a Rotore

Cifrario di Cesare

Svetonio (Vitae Cesarorum): lettera di Cesare a Cicerone

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	25	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

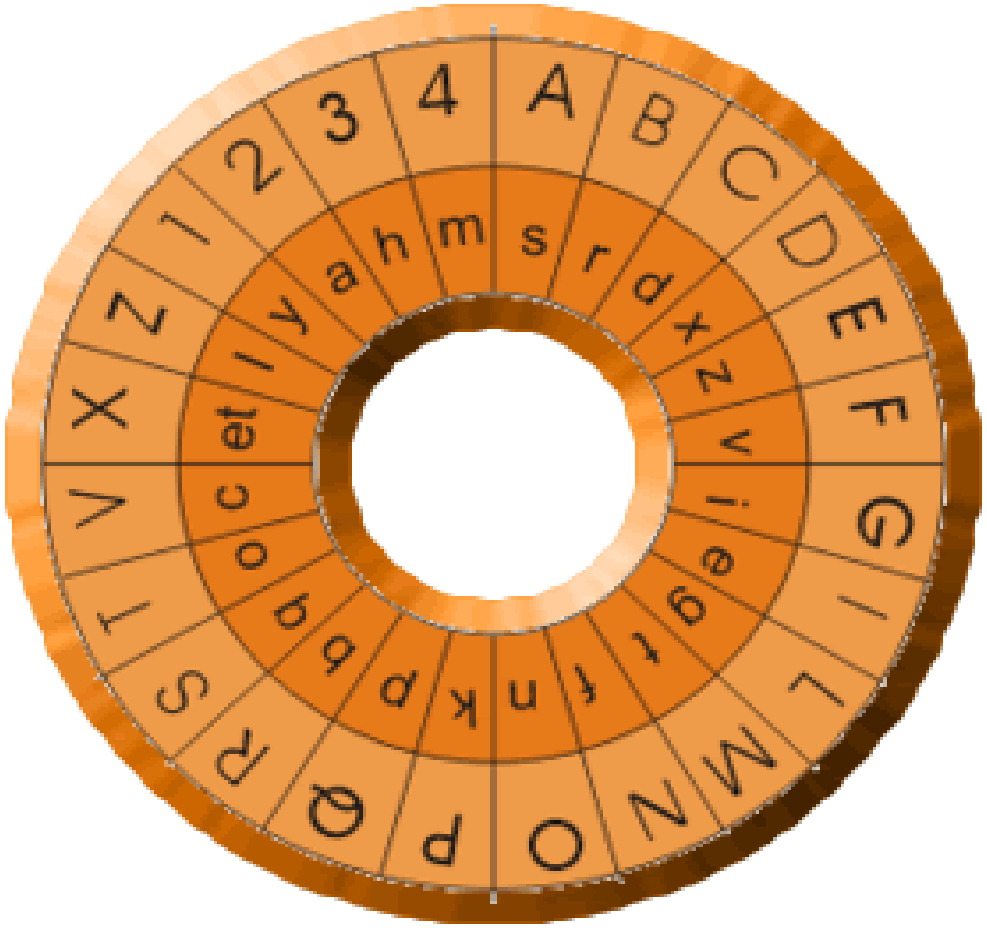
$$X \longleftarrow \mod 26 (M + 13)$$

```
GALLIA OMNES DIVISA EST IN PARTES TRES
TNYYVN BZARF QVIVFN RFG VA CNEGRF GERF
```

In generale:

$$X \longleftarrow \mod 26 (M + K), \qquad K = \{0,...,25\}$$

Disco di Alberti

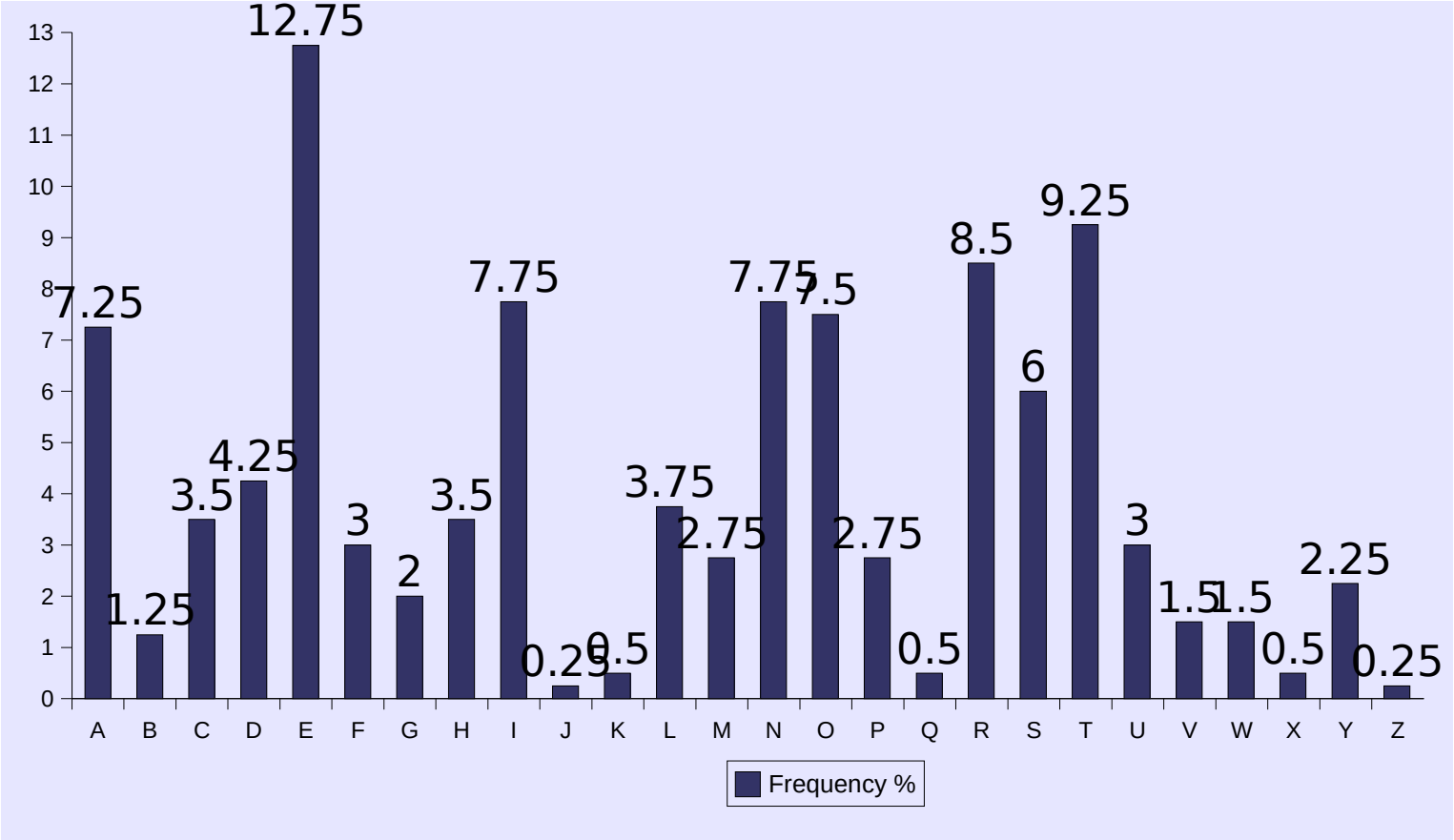


Leon Battista Alberti
XV sec.

Rotazione data:

ALBERTI ⟶ sgrzboe

Frequenza delle Lettere in Inglese



Lingue diverse hanno frequenze diverse.
Il crittanalista determina facilmente sia la lingua che il messaggio.

Contrasto a Frequenza Lettere

- Omofoni
  - Più simboli per i caratteri più frequenti
    - **p. es. anche ƒØ§ž per E**
    - **si abbassa la frequenza di E**
- Nulle
  - Simboli meno frequenti aggiunti al testo in modo da non alterare il significato
    - **p. es. NELQMEZZZZOQDELKCAMMINWDIKNOSQTRA**
    - **aumento delle frequenze dei simboli nulli**

Cifrario di Porta

Giovan Battista Porta, 1563

	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
A	0	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
B	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
C	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77
D	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103
E	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129
F	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
G	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181
H	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
I	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233
J	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259
K	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285
L	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311
M	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337
N	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363
O	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389
P	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415
Q	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441
R	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467
S	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493
T	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519
U	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545
V	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571
W	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597
X	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623
Y	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649
Z	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675

Testo in chiaro: QUESTOQEZUNKSEGRETOQ (con lettere nulle)

Testo cifrato: 436 122 508 420 670 348 472 173 123 380

Cifrari a Trasposizione

i	c	h	b	i	n
d	e	r	d	o	k
t	o	r	e	i	s
e	n	b	a	r	t

Rettangolare: idteceonhrrbbdeaioirnkst

Diagonale: ieracrerhditbosiknetndob

Bustrofelica: idtenoechrrbaedbioirtskn

Spirale: tsknibhcidtenbariodreore

i				i				r				t				i				b			
	c		b		n		e		d		k		o		e		s		n		a		t
		h				d				o				r				e				r	

Rail fence: iirtibcbnedkoesnathdorer

	c			n			d			o			s			a	
i		h	i		d	r		o	t		r	i		e	b		r
	b			e			k			e			n			t	

Croix Grecque: cndosaihidrotriebrbekent

Trasposizione Colonnare

Permutazione P: 2 1 4 3

1 2 3 4	*2 1 4 3*
e s w a	S E A W
r s c h	S R H C
o n d u	N O U D
n k e l	K N L E

Trasposizione semplice a chiave:

SSNKERONAHULWCDE

Variante di Richelieu:

SEAWSRHCNOUDKNLE

Trasposizione doppia

	2 4 1 3	*1 2 3 4*
1 e s w a	*2* r s c h	S R H C
2 r s c h	*4* n k e l	K N L E
3 o n d u	*1* e s w a	S E A W
4 n k e l	*3* o n d u	N O U D

Permutazioni P1: 2 4 1 3 P2: 2 4 1 3

Per colonne:

SKSNRNEOHLAUCEWD

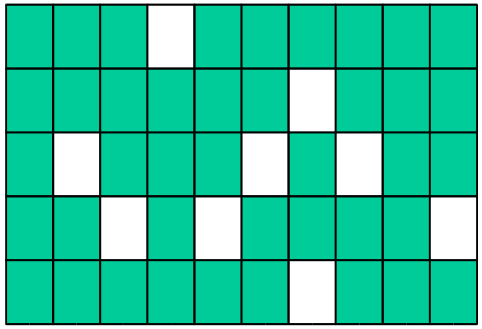
Per righe:

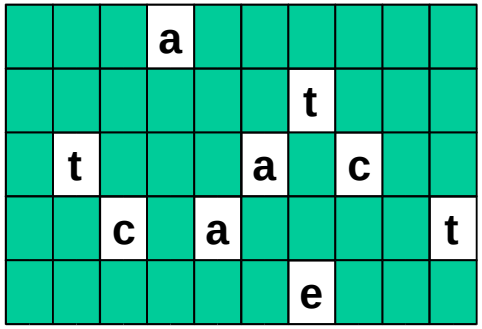
SRHCKNLESEAWNOUD

Griglie

Griglie semplici o di Cardano:

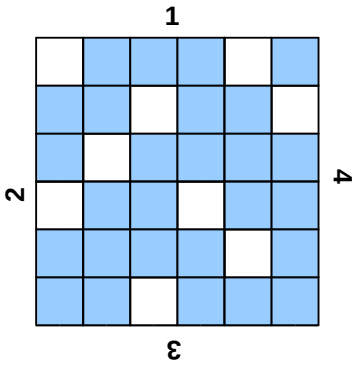
s f v a y j x r a v
q e k u e e t f g t
x t f m c a d c e t
o y c h a i a e c t
o g t z e d e i l i

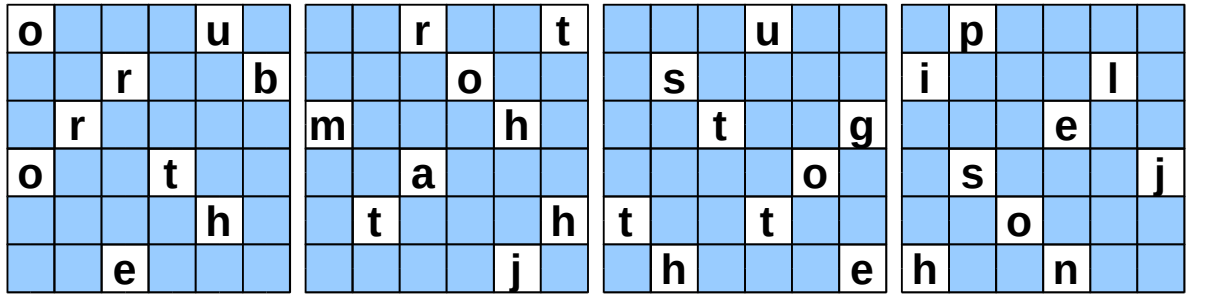




Griglie a rotazione o di Fleissner:

o p r u u t
i s r o l b
m r t e h g
o s a t o j
t t o t h h
h h e n j e





StarShell

Sostituzioni Multipartite Semplici

$V^1 \rightarrow W^m$

Cifratura di Polibio

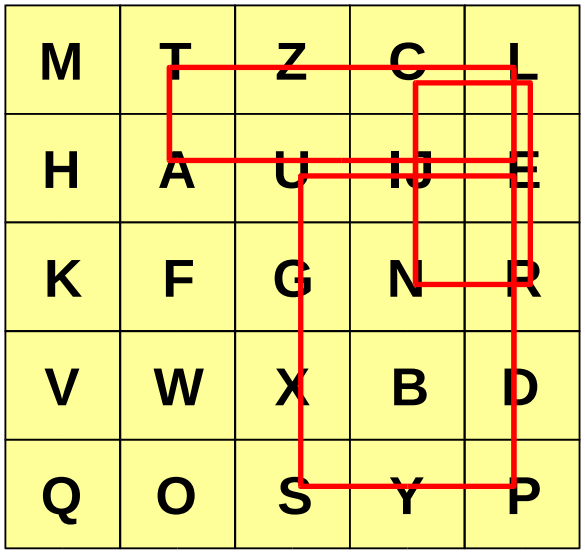
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Testo in chiaro: S E G R E T O

Testo cifrato: (4,3) (1,5) (2,2) (4,2) (1,5) (4,4) (3,4)

Cifrario di Playfair

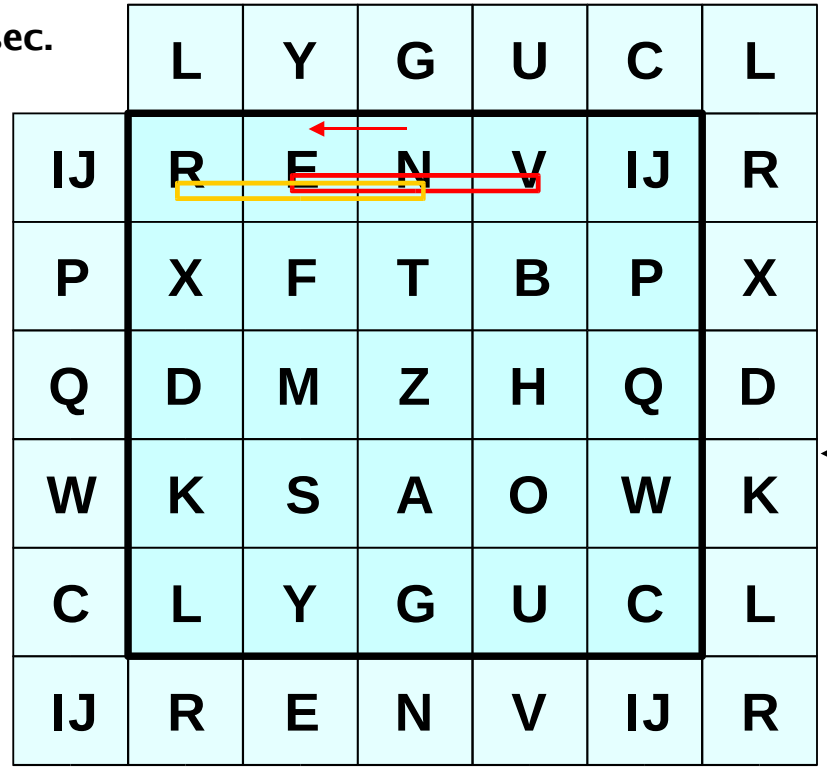
Charles Wheatstone, XIX sec.



SE CR ET

UP LN AL

Rotazione in senso orario - angoli opposti del rettangolo



Generazione di quadrato magico con algoritmo del cavallo

'Ombre'

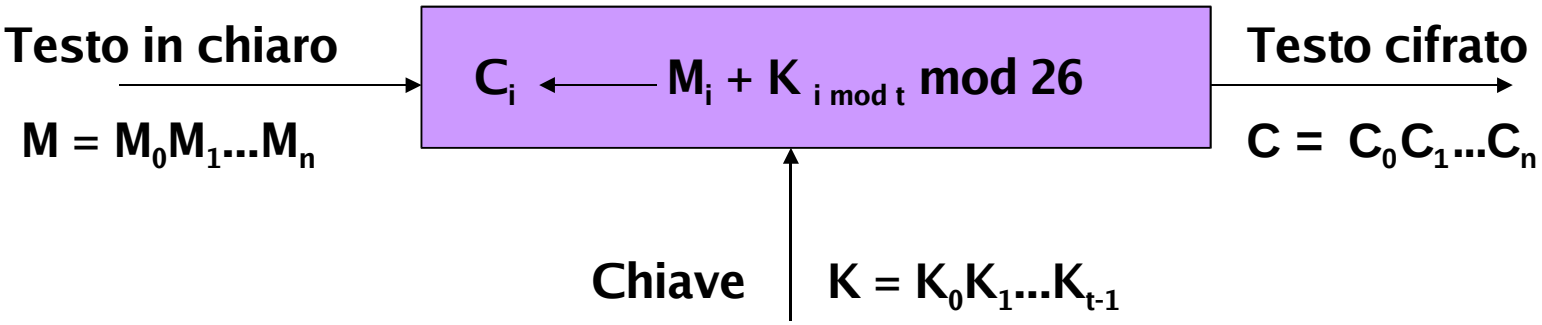
VE NI RE

NR VR EN

Shiftato di un passo nella direzione dalla prima alla seconda lettera, con eventuale uso delle ombre

Cifrari a Sostituzione Polialfabetica

Cifrario di Vigenère, 1586



CODIC EMOLT OSICU RO	Testo in chiaro
REBUS REBUS REBUS RE	Chiave
TSECU VQFPL FWJWM IS	Testo cifrato

Numero possibile di chiavi: 26^t

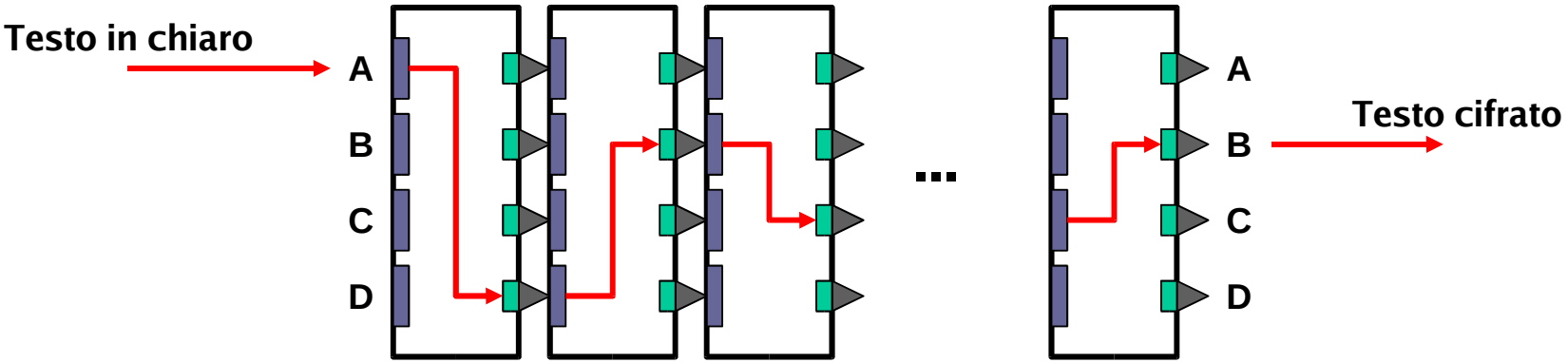
Considerato inviolabile per molto tempo

Possibili penetrazioni con *indici di coincidenza*

Quadrato di Vigenère

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

Rotori



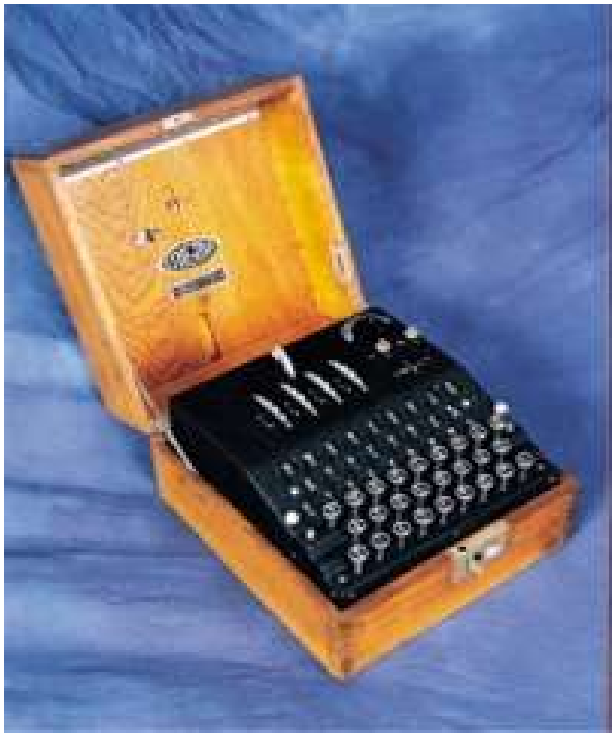
E. H. Hebern (1918)

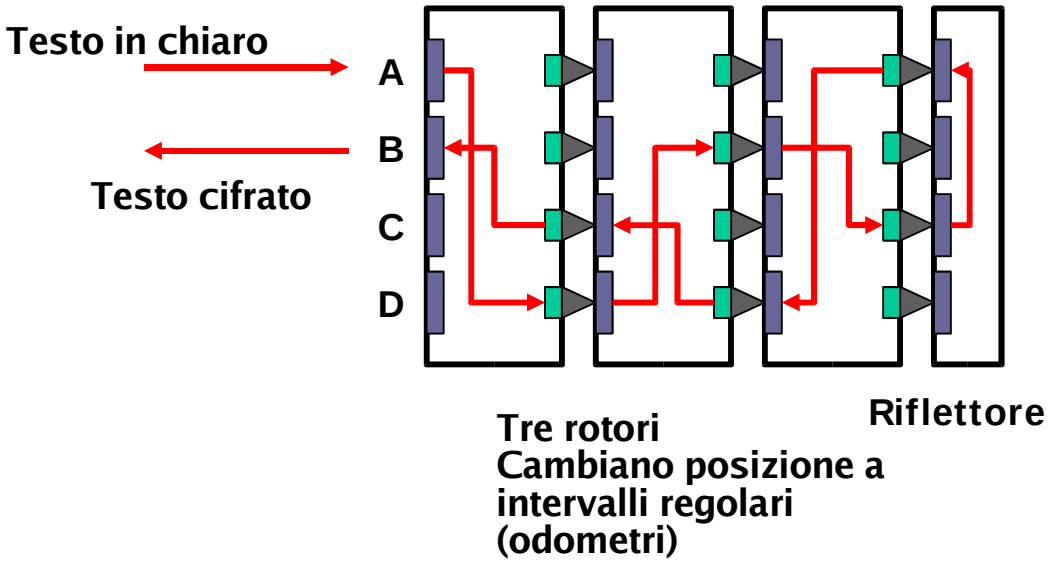
Adottati da molti eserciti

Rotori

Hagelin “Cryptographer” C-36
Boris Hagelin
Aktiebolaget Cryptoteknik
Stockholm, 1936

Enigma





Tre rotori
Cambiano posizione a intervalli regolari (odometri)

Wehrmacht (1937): scelta di 3 rotori tra 5
Kriegsmarine (1943): 4 rotori tra 8

Debolezze:
Nessuna lettera cifra se stessa
Cifratura riflessiva: A->B => B->A
Posizione iniziale rotori trasmessa

Decrittografato a Bletchley Park (G.B.) da Alan Turing et al.

Sicurezza della Crittografazione

- Incondizionatamente Sicura
  - Il testo cifrato non contiene abbastanza informazioni per determinare univocamente il testo in chiaro corrispondente, per qualsiasi quantità di testo in chiaro
    - **Solo One-Time-Pads**
    - **Normalmente i testi lunghi crittografati con la stessa chiave aumentano la probabilità di successo di crittanalisi**
- Computazionalmente Sicura
  - Il costo della decrittografazione è superiore al valore dell'informazione crittografata
  - Il tempo richiesto per la decrittografazione supera la vita utile dell'informazione

Problemi di Crittografazione

- E' gestita da esseri umani

  The Enigma machine, as it was, would have been impregnable, if it had been used properly. (Gordon Welchmann, 1982)

  - **Errori di crittografazione**
    - **richiedono la ritrasmissione del messaggio**
  - **Ripetere un messaggio crittografato in chiaro**
    - **compromette chiave e metodo selezione chiavi**
  - **Inviare un messaggio noto in forma cifrata**
  - **Usare parole o frasi probabili**
    - **Liberty, Gloire, Vaterland, Führer**
  - **Inviare messaggi solo quando necessario**
    - **analisi del traffico**
  - **Mescolare messaggi personali ad ufficiali**
    - **effetto mutande**

Principio di Kerckhoffs

- Legge di base della crittologia
  - ***"il faut qu'il puisse sans inconvénient tomber entre les mains de l'ennemi"***

    Auguste Kerckhoffs (1835-1903), fiammingo (*La cryptographie militaire*, 1883)
  - ***"the enemy knows the system being used"***

    Shannon, 1949

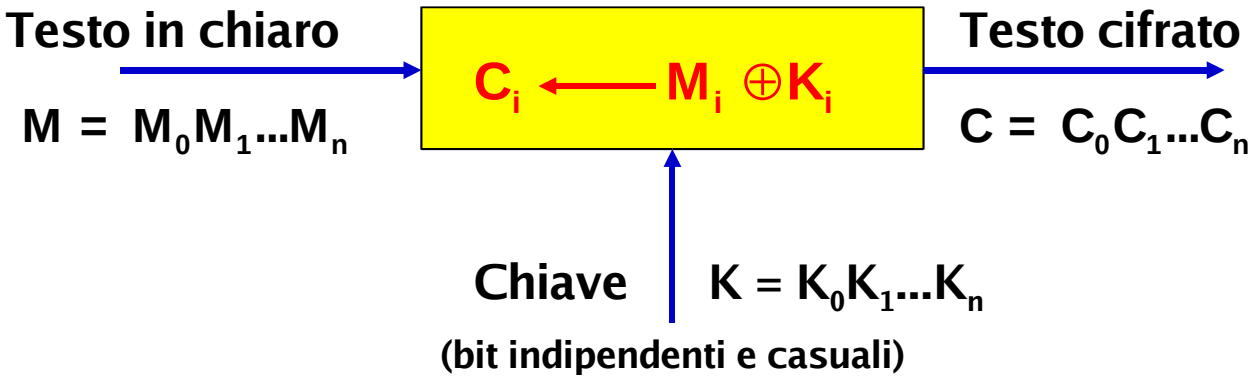
- Assumere che il nemico conosca gli algoritmi usati
- Contrario di: **Security through Obscurity**

Attacchi di Crittanalisi

Type of Attack	Known to Cryptanalyst
Ciphertext only	Encryption algorithm
	Ciphertext to be decoded
Known plaintext	Encryption algorithm
	Ciphertext to be decoded
	One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	Encryption algorithm
	Ciphertext to be decoded
	Plaintext message chosen by cryptanalist, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	Encryption algorithm
	Ciphertext to be decoded
	Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	Encryption algorithm
	Ciphertext to be decoded
	Plaintext message chosen by cryptanalist, together with its corresponding ciphertext generated with the secret key
	Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

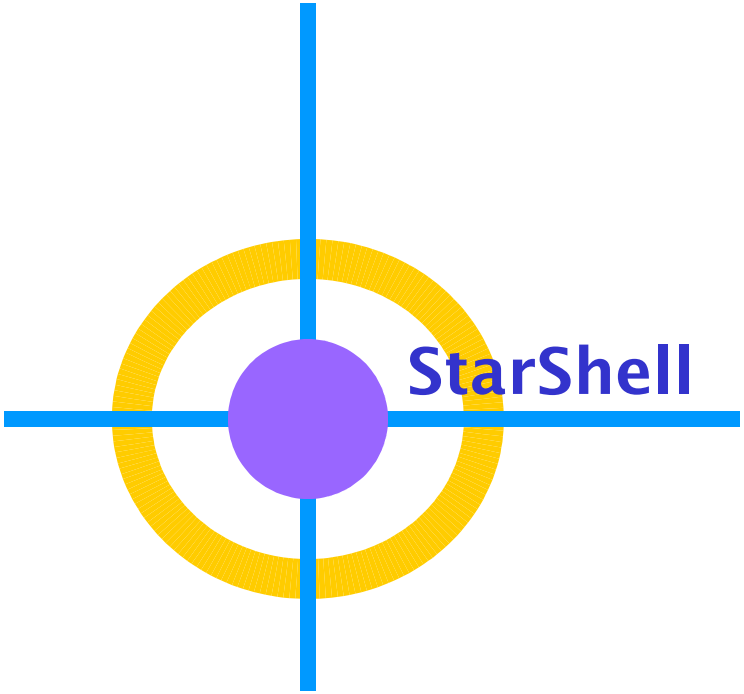
Cifrario Perfetto

One-time pad



Cifrario perfetto se M e C sono indipendenti
Prob (M=M') = Prob (M=M' | C=C')

Lunghezza chiave ≥ Lunghezza testo in chiaro


StarShell