Crittografia classica

Barbara Masucci

Dipartimento di Informatica ed Applicazioni
Università di Salerno

masucci@dia.unisa.it
http://www.dia.unisa.it/professori/masucci

Steganografia

Occultamento del messaggio

Steganografia

Steganos = coperto **Grafien = scrittura**

Steganografia: Esempi

Erodoto (*Histories*):
Demerato in esilio avvisa gli spartani del progetto di invasione da parte di Serse, re dei Persiani

Espediente della tavoletta di cera

Gorgo, sorella di Cleomenes e moglie di Leonidas (re spartano) scoprì la presenza del messaggio ...

Steganografia: Esempi

Erodoto (*Histories*):
Istieo incoraggia Aristagora di Mileto a ribellarsi a Serse

Espediente dello schiavo, sul cui capo rasato è stato tatuato un messaggio

Dopo la crescita dei capelli, il corriere viene inviato da Aristagora

Steganografia: Esempi

- Cina
  - Messaggi dipinti su striscioline di seta, appallottolate, ricoperte di cera e inghiottite dal corriere
- Plinio il vecchio
  - Comunicazione mediante inchiostro simpatico ottenuto dal lattice di titimabo
- Gian Battista Porta
  - Comunicazione mediante uovo sodo e una sorta di "inchiostro simpatico"

Steganografia: Problemi

- Se il corriere è attentamente perquisito il messaggio può essere scoperto
  - Raschiando tavolette di cera
  - Rasando il capo al corriere
  - Sbucciando le uova
  - …

La segretezza è perduta al momento dell'intercettazione

Crittografia

Trasformazione

+

Segretezza

Crittografia

Cryptos = segreto **Grafien = scrittura**

Crittografia

Dall'antichità fino a pochi anni fa:

- Essenzialmente comunicazioni private
- Usi Militari e Diplomatici

χρυπτοσ γραφια λογοσ

Oggi: studio di tecniche ed applicazioni che dipendono dall'esistenza di problemi difficili

Scritture segrete

Trasformazione delle parole per renderne incomprensibile il significato

Città di Menet Khufu (Nilo), 4000 anni fa

Incisione funebre (geroglifico)
scopo trasformazione:
conferire *dignità* e
onoreficenza al defunto

Altre trasformazioni, scopo:

- **mistero**
- senso dell'**arcano**
- conferire potere **magico** alle parole

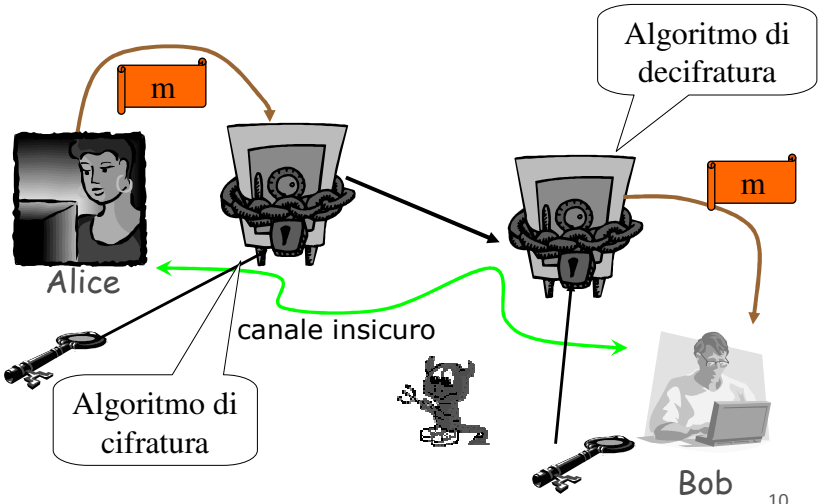
Cifrari simmetrici

Alice

canale insicuro

Bob

Cifrari simmetrici



Metodi antichi di cifratura

- Erodoto
- **Scytala** spartana, 500 a.C. (Plutarco in *Vite parallele*)
- Polibio, 118 a.C. *(Libro X delle Storie)*

	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: C A S A

testo cifrato: (1,3) (1,1) (4,3) (1,1)

Metodi antichi di cifratura

Bibbia: tre tipi di cifratura

- **Atbash**: alfabeto rovesciato (**A**leph, **t**aw, **b**eth, **sh**in)
  cifratura 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 rimanenti:
  lettera da sostituire + lettera sostituente = 28

Cifrario di Cesare

100-44 a.C.

Svetonio (Vitae Caesarorum): 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	24	25

$X \leftarrow M+3 \bmod 26$

testo in chiaro

OMNIA GALLIA EST DIVISA IN PARTES TRES
RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

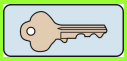
testo cifrato

Cifrari con shift

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	24	25

Cifrari con shift

Chiave K



$X \leftarrow M+K \bmod 26 \qquad K \in \{0,1,\ldots,25\}$

Quante chiavi sono possibili?

Cifrari a sostituzione monoalfabetica

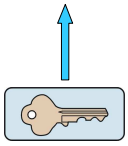
Alfabeto in chiaro

Alfabeto cifrante

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

testo in chiaro: C A S A

testo cifrato: T O P O



- Numero di chiavi da provare: $26! = 4 \times 10^{26}$

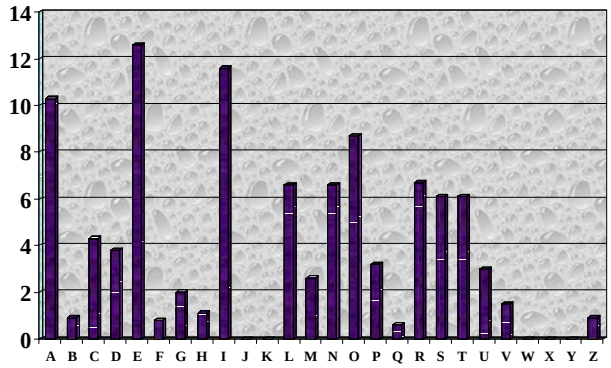
  Con 10^6 computer, ognuno che prova 10^9 chiavi al secondo, la ricerca esaustiva richiede 10^4 anni

Improponibile!

Analisi statistica

- Ogni lettera cambia "abito", ma conserva la sua "identità"
  - Frequenza
  - Vicinanza con altre lettere (q è sempre seguita da u,…)
  - Altre regole (mai due vocali di seguito,…)
- Il cifrario può essere rotto considerando le regolarità del linguaggio
  - Calcolo della frequenza relativa delle lettere nel cifrato
  - Confronto con la distribuzione standard delle frequenze per quel linguaggio

Frequenze occorrenze lettere



	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
italiano	10,3	0,9	4,3	3,8	12,6	0,8	2,0	1,1	11,6	0,0	0,0	6,6	2,6	6,6	8,7	3,2	0,6	6,7	6,1	6,1	3,0	1,5	0,0	0,0	0,0	0,9
inglese	7,3	1,3	3,5	4,3	12,8	3,0	2,0	3,5	7,8	0,3	0,5	3,7	2,8	7,8	7,5	2,8	0,5	8,5	6,0	9,3	3,0	1,5	1,5	0,5	2,3	0,3
francese	8,3	1,3	3,3	3,8	17,8	1,3	1,3	1,3	7,3	0,8	0,0	5,8	3,2	7,2	5,7	3,7	1,2	7,3	8,3	7,2	6,3	1,8	0,0	0,0	0,8	0,0

Nulle

- Aggiungere simboli meno frequenti
  - in posizioni da non alterare il significato

testo in chiaro: QUELQRAMOQDELQLAGO…

testo cifrato: …

Aumento frequenze dei corrispondenti simboli

Omofoni

- Molti simboli per cifrare singoli caratteri frequenti

testo in chiaro: E

testo cifrato: □ Õ Ñ ® (scelti a caso!)

- Si abbassano le frequenze dei simboli del testo cifrato

12.6 per E ⟹ 3.15 per □ Õ Ñ ®

Nomenclatori

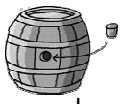
- In aggiunta all'alfabeto cifrante si usa un insieme di parole in codice
- Svantaggi:
  - Compilazione e trasporto del repertorio
  - Se cade in mani ostili, ripetizione della distribuzione
  - Non molto più sicuro della singola sostituzione monoalfabetica

La congiura di Babington

- Nel 1586 Maria Stuarda, regina di Scozia, fu condannata a morte per aver cospirato contro la cugina Elisabetta
- La congiura, organizzata da Anthony Babington, prevedeva
  - La liberazione di Maria dalla prigionia in Inghilterra
  - L'uccisione di Elisabetta
  - Una ribellione alla religione protestante
- Sir Walsingham, segretario di stato, provò che Maria aveva preso parte alla congiura

La congiura di Babington

- Maria e Babington comunicavano grazie a
  - Un corriere (Gilbert Gifford)
  - Un birraio, che nascondeva i messaggi dentro lo zipolo delle botti di birra
  - Un cifrario, costituito da
    - 23 simboli che sostituivano le lettere
    - Un nomenclatore di 35 simboli, che sostituivano parole o frasi
    - 4 nulle e un simbolo per le doppie



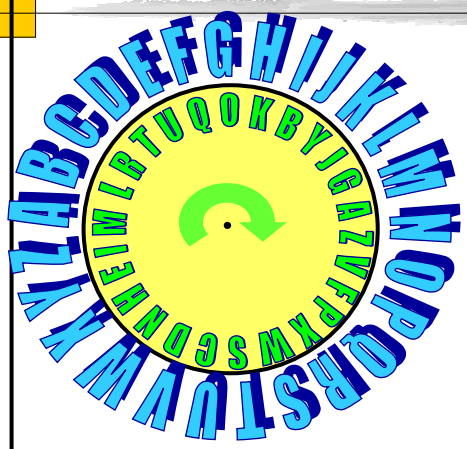
- Gifford consegnava a Walsingham tutti i messaggi, che venivano decifrati da Thomas Phelippes
  - Maria firmò la sua condanna a morte rispondendo alla lettera di Babington
  - Babington e complici furono arrestati e squartati vivi
  - Maria fu decapitata l'8 febbraio 1857

Oltre la cifratura monoalfabetica

Due approcci:

- Utilizzo di più alfabeti cifranti
  - Leon Battista Alberti
  - Vigenère
- Utilizzo di cifrature di più lettere per volta
  - Porta
  - Playfair

Disco di Alberti



Leon Battista Alberti,
architetto italiano, XV secolo

testo in chiaro

D I S C O
V Z T U G

testo cifrato con rotazione "AM"

Utilizzato nella guerra di secessione

Leon Battista Alberti

Proposta di usare più alfabeti cifranti e di sostituirli durante la cifratura

Alfabeto piano

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

I Alfabeto cifrante

II Alfabeto cifrante

Leone
hbttv

Cifrario di Porta

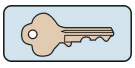
Giovanni Battista Porta, primo cifrario per digrammi [1563]

	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

Cifrario di Porta

testo in chiaro: DO MA NI

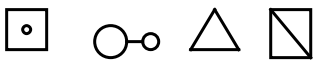
testo cifrato: 92 312 346



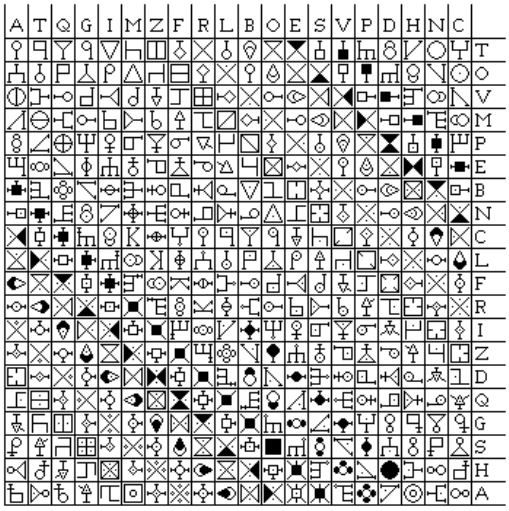
Chiave: permutazione arbitraria di:

- numeri del cifrato
- lettere su righe e colonne

Uso di caratteri speciali per alfabeto testo cifrato



Cifrario di Porta



Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro $M = M_0M_1M_2\ldots M_n$ → $C_i \leftarrow M_i + K_{i \bmod t} \bmod 26$ → **testo cifrato** $C = C_0C_1C_2\ldots C_n$

chiave $K = K_0K_1K_2\ldots K_{t-1}$

Testo in chiaro: CODICE MOLTO SICURO Chiave: REBUS

CODIC	EMOLT	OSICU	RO	testo in chiaro
REBUS	REBUS	REBUS	RE	chiave
TSECU	VQPFL	FWJWM	IS	testo cifrato

Cifrario 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

Cifrario di Vigenère

Blaise de Vigenère, 1586

Cifrario a sostituzione polialfabetica

testo in chiaro $M = M_0M_1M_2\ldots M_n$ → $C_i \leftarrow M_i + K_{i \bmod t} \bmod 26$ → **testo cifrato** $C = C_0C_1C_2\ldots C_n$

chiave $K = K_0K_1K_2\ldots K_{t-1}$

- Considerato inviolabile per molto tempo
- Numero possibili chiavi = 26^t

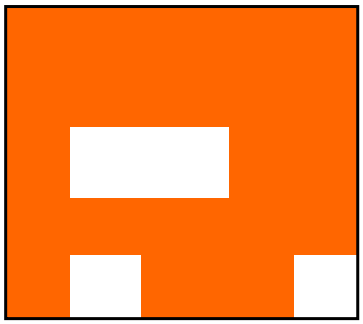
Cifrario di Vigenère

- Resiste all'analisi delle frequenze
  - Una lettera cifrata corrisponde a più simboli in chiaro
  - Esiste un numero grande di chiavi
- Babbage (1834) e Kasiski (1863) furono i primi a cimentarsi nella crittoanalisi
  - Studio delle ripetizioni per individuare la lunghezza della chiave
  - Analisi delle frequenze in ognuno degli alfabeti cifranti corrispondenti alle lettere della chiave

Griglie

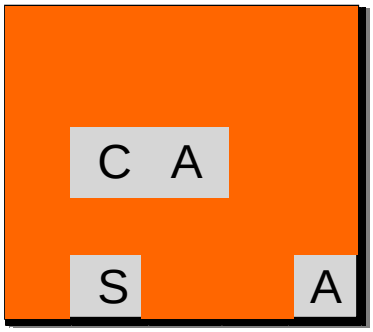
Girolamo Cardano, XVI secolo

N	E	L	M	E
Z	Z	O	D	E
L	C	A	M	M
I	N	D	I	N
O	S	T	R	A



Griglie

Girolamo Cardano, XVI secolo



Griglie con rotazioni

A	A	A	R	M	O
T	M	E	N	T	O
D	O	A	M	A	C
C	O	Z	N	Z	O
C	M	H	A	N	I
G	I	I	I	O	L

griglia
griglia ruotata di 90°
griglia ruotata di 180°
griglia ruotata di 270°

testo cifrato: **AAARMOTMENTODOAMACCOZNZOCMHANIGIIIOL**
testo in chiaro: **ATTACCHIAMODOMANIAMEZZOGIORNOCONMIL**

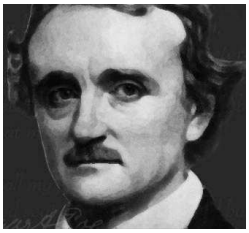
Crittografia e Letteratura

- Jules Verne (1828-1905), "Mathias Sandorf"
  - messaggio cifrato dal conte Sandorf, coinvolto in una cospirazione anti-austriaca
- Edgar Allan Poe (1809-1849), "Lo scarabeo d'oro"
  - messaggio scritto dal pirata Capitano Kidd, dice dove è nascosto il tesoro

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

Crittoanalisi

Edgar Allan Poe, "Lo scarabeo d'oro" (1843)



53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

caratteri	occorrenze
8	33
;	26
4	19
+)	16
*	13
5	12
6	11
! 1	8
0	6
9 2	5
: 3	4
?	3
`	2
- .	1

Assumiamo che 8 corrisponda al carattere e

7 occorrenze di ;48
Assumiamo che ; ⇨ t
4 ⇨ h
8 ⇨ e

...poi

Crittoanalisi

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

5	rappresenta	a
!	"	d
8	"	e
3	"	g
4	"	h
6	"	i
*	"	n
+	"	o
(	"	r
.	"	t

A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

I crittogrammi Beale

La vicenda inizia nel 1822 a Lynchburg, Virginia

Protagonisti:

- Thomas Beale, avventuriero del selvaggio West
- Robert Morris, gestore di un hotel di Lynchburg
- Un tesoro sepolto del valore di 20 milioni di dollari
- Tre crittogrammi
- Un opuscolo pubblicato nel 1885

I crittogrammi Beale

Nel 1822 Beale affidò a Morris una scatola chiusa a chiave chiedendogli di custodirla

- La scatola conteneva documenti cifrati

Se Beale non fosse tornato entro 10 anni, Morris avrebbe dovuto aprirla

- La chiave necessaria alla decifratura sarebbe stata recapitata a Morris nel 1832

I crittogrammi Beale

Beale non tornò mai e Morris non ricevette la chiave di decifratura

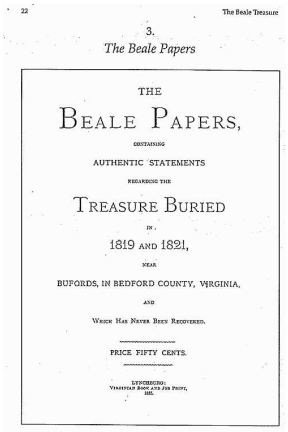
Nel 1845 Morris aprì la scatola

- All'interno c'erano tre crittogrammi e una lettera per Morris
- La lettera svelò che Beale aveva scoperto un giacimento d'oro
- I tre crittogrammi indicavano
  - l'ammontare del tesoro
  - la sua ubicazione
  - la ripartizione del tesoro tra gli eredi

I crittogrammi Beale

- Morris tentò per 20 anni di decifrare i crittogrammi, senza successo
- Nel 1862 mostrò i crittogrammi ad un amico che, dopo aver decifrato il secondo, pubblicò un opuscolo nel 1885
- Il secondo crittogramma fu decifrato usando come chiave la dichiarazione di indipendenza

I crittogrammi Beale

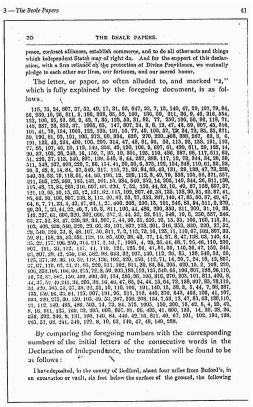


3.
The Beale Papers

THE
BEALE PAPERS,
CONTAINING
AUTHENTIC STATEMENTS
REGARDING THE
TREASURE BURIED
IN
1819 AND 1821,
NEAR
BUFORDS, IN BEDFORD COUNTY, VIRGINIA,
AND
WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

L'opuscolo



THE BEALE PAPERS.

Un crittogramma

Il secondo crittogramma

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41, 85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48…

La chiave

DECLARATION OF INDEPENDENCE

When(1) in(2) the(3) course(4) of(5) human(6) events(7) it(8) becomes(9) necessary(10) for(11) one(12) people(13) to(14) dissolve(15) the(16) political(17) bands(18) which(19) have(20) connected(21) them(22) with(23) another(24) and(25) to(26) assume(27) among(28) the(29) powers(30) of(31) the(32) earth(33) the(34) separate(35) and(36) equal(37) station(38) to(39) which(40) the(41) laws(42) of(43) nature(44) and(45) of(46) nature's(47) god(48) entitle(49) them(50) a(51) decent(52) respect(53) to(54) the(55) opinions(56) of(57) mankind(58) requires(59) that(60) they(61) should(62) declare(63) the(64) causes(65) which(66) impel(67) them(68) to(69) the(70) separation(71) we(72) hold(73) these(74) truths(75) to(76) be(77) self(78) evident(79) that(80) all(81) men(82) are(83) created(84) equal(85) that(86) they(87) are(88) endowed(89) by(90) their(91) creator(92) with(93) certain(94) unalienable(95) rights(96) that(97) among(98) these(99) are(100) life(101) liberty(102) and(103) the(104) pursuit(105) of(106) happiness(107) that(108) to(109) secure(110) these(111) rights(112) governments(113) are(114) instituted(115) among(116) men(117) …

Il crittogramma decifrato

" I have deposited in the county of Bedford, (Virginia) about four miles from Buford, in an excavation or vault, six feet below the surface of the ground, the following articles belonging jointly to the parties whose names are given in number three herewith. The first deposit consisted of ten hundred and fourteen pounds of gold and thirty eight hundred and twelve pounds of silver deposited Nov. Eighteen Nineteen. The second was made Dec. Eighteen Twenty one and consisted of nineteen hundred and eighty eight of silver, also jewels obtained in St. Louis in exchange to save transportation and valued at thirteen thousand dollars. The above is securely packed in iron pots with iron covers the vault is roughly lined with stone and the vessels rest on solid stone and are covered with others. Paper number one describes the exact locality of the vault so that no difficulty will be had in finding it."

Thomas Jefferson Beale

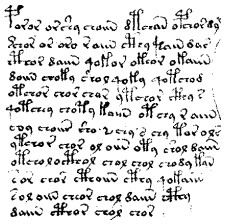
I crittogrammi Beale

- Il primo e il terzo crittogramma di Beale sono inviolati da più di un secolo
  - I crittogrammi potrebbero essere stati alterati dall'autore dell'opuscolo per impedirne la decifratura
- E il tesoro?
  - Qualcuno potrebbe averlo trovato utilizzando gli indizi dell'unico crittogramma decifrato
- L'intera storia potrebbe essere una montatura, ispirata dal romanzo di Edgar Allan Poe
- Ancora oggi crittoanalisti e cacciatori di tesori sono affascinati dalla vicenda

Il manoscritto Voynich

Manoscritto rinvenuto nel 1912 da un antiquario nella biblioteca di un convento di gesuiti vicino Roma

- Composto da circa 230 pagine, contenenti simboli ed illustrazioni (piante, pianeti, figure femminili)
- Probabilmente creato nel XIII secolo
- Dopo vari tentativi di decifratura, resta tuttora inviolato
- Donato alla Yale University nel 1969

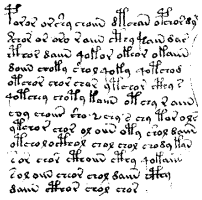


Il manoscritto Voynich

Una lettera del 1666 che accompagnava il manoscritto affermava che

- Il probabile autore era l'astronomo Roger Bacon (1214-1294)
- Nel 1586 l'imperatore Rodolfo di Boemia lo aveva acquistato per 600 ducati d'oro (l'equivalente di $14.000)

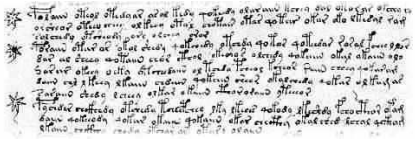
La lettera, inviata dall'ultimo proprietario ad un prete gesuita, chiedeva di decifrare il manoscritto…

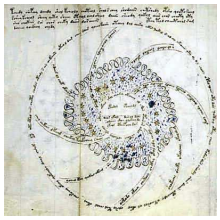


Il manoscritto Voynich

Composto da varie sezioni:

- Erbale: disegni di piante
- Cosmologica: disegni di stelle e pianeti
- Astrologica: disegni dello zodiaco e di figure femminili
- Biologica: disegni di parti del corpo e di figure femminili
- Farmaceutica: disegni di boccette di medicinali
- Ricettario: brevi paragrafi testuali con una stella a inizio margine

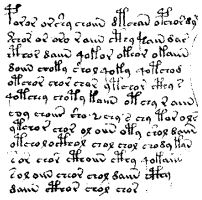




Il manoscritto Voynich

Alcune ipotesi

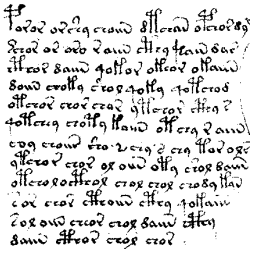
- Trattato scientifico scritto in un linguaggio sconosciuto
- Trattato scientifico scritto interamente in codice
- Del tutto privo di significato, frode ai danni dell'imperatore Rodolfo di Boemia



Il manoscritto Voynich

Trattato scientifico scritto in linguaggio sconosciuto???

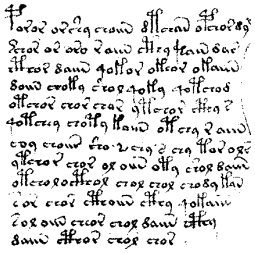
- L'alfabeto comprende
  - Caratteri dell'alfabeto romano: a,o,c,n,m
  - Numeri: 2,4,8,9,
  - Simboli usati nel Medioevo in alchimia



Il manoscritto Voynich

Trattato scientifico scritto interamente in codice???

- L'ultimo foglio contiene tre linee incomprensibili, forse una chiave per la decifratura
- Sistema di codifica completamente diverso da quelli in uso nel XV sec…e tuttora inviolato!!!

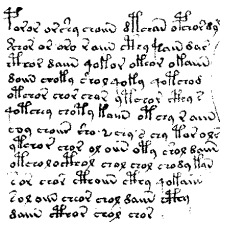


Il manoscritto Voynich

Nel 1921 W. Newbold propose una soluzione:

- Il manoscritto era effettivamente opera di R. Bacon
- Descriveva l'invenzione e l'uso di varie invenzioni
  - Il microscopio, per lo studio di cellule non note nel XV sec (!)
  - Il telescopio, per lo studio della galassia di Andromeda, visibile solo con telescopi del XX sec. (!!)

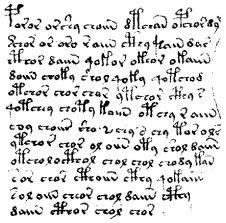
Tale soluzione fu screditata da J.M. Manly nel 1931



Il manoscritto Voynich

Altri tentativi di soluzione:

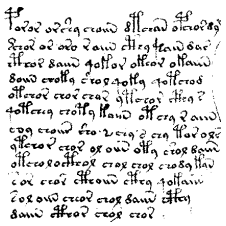
- Nel 1940 J.M. Feely e L.C. Strong usarono un codice a sotituzione (ottenendo un risultato incomprensibile…)
- Nel 1978 J. Stojko affermò che il testo era scritto in ucraino ma senza le vocali (ottenendo frasi del tipo "il Vuoto è ciò per cui combatte l'occhio del Dio bambino…")
- Nel 1987 L. Levitov affermò che il testo era opera dei Catari (ottenendo una traduzione che non coincideva con le concezioni teologiche catare…)



Il manoscritto Voynich

Frode ai danni dell'imperatore???

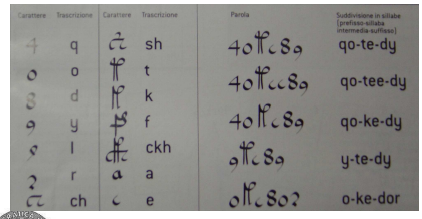
- Complessità linguistica troppo elevata
  - Testo composto da parole di 3 sillabe
    - Alcune sillabe compaiono solo all'inizio/fine delle parole
    - Altre sillabe non compaiono mai insieme
  - La lunghezza delle parole ha una distribuzione binomiale
- Componendo casualmente le sillabe non si può avere un testo con tante regolarità statistiche…

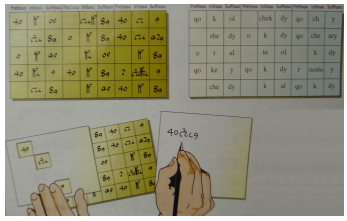


Il manoscritto Voynich

Un'ipotesi recente

- Testo creato usando le griglie di Cardano su una tabella di permutazioni di sillabe
  - Colonne dei prefissi, infissi, suffissi
  - Griglia con 3 aperture
- Con una tabella di 36 colonne e 40 righe è possibile creare un'intera pagina del manoscritto (40 righe di 8-12 parole)





Cifrario di Playfair

Progettato da Charles Wheatstone buon amico del Barone Lyon Playfair, XIX secolo

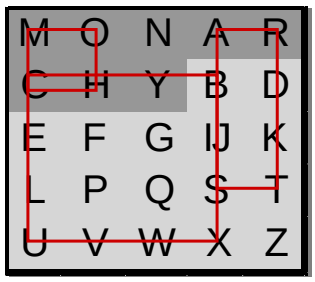
M	O	N	A	R
C	H	Y	B	D
E	F	G	IJ	K
L	P	Q	S	T
U	V	W	X	Z

Cifrario usato dai britannici. Anche dall'Australia durante la II guerra mondiale.

Anche rettangoli 4x7, 4x8,…

Cifrario di Playfair

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



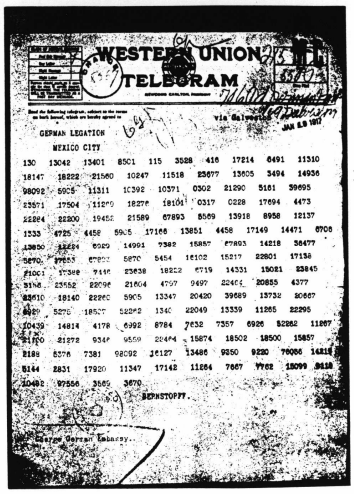
testo in chiaro: **AT TA CX CO**
testo cifrato: **RS SR BU HM**

Cifrario di Playfair

- Migliore rispetto alla cifratura monoalfabetica: 26x26=676 digrammi
  - Ma la struttura del testo rimane!
- Analisi condotta in base alla frequenza dei digrammi più comuni nella lingua
  - Es. es, er, on, re, el, er, de.

Il telegramma di Zimmermann

- La decifrazione di un telegramma tedesco, intercettato dagli inglesi nel 1917, influì sul corso della storia
- Il telegramma spinse gli Stati Uniti a riconsiderare la loro politica di neutralità



Il telegramma di Zimmermann

Nel 1915 un U-boot tedesco in immersione affondò il transatlantico Lusitania

- 1198 vittime, tra cui 128 civili americani

Per evitare l'entrata in guerra degli USA, la Germania promise che gli U-boot sarebbero emersi prima di attaccare

Nel 1917 la Germania decise di venir meno al suo impegno

- L'impiego senza restrizioni della flotta sottomarina avrebbe costretto la Gran Bretagna alla resa
- Bisognava fare presto ed evitare agli USA di entrare in guerra cambiando il corso del conflitto

Il telegramma di Zimmermann

Zimmermann, ministro tedesco degli esteri progettò un piano:

- Indurre il Messico e il Giappone ad attaccare gli USA
- In tal modo gli USA non avrebbero avuto il tempo di impegnarsi in Europa e la Gran Bretagna si sarebbe arresa

Il 16 gennaio 1917, Zimmermann inviò un telegramma cifrato a von Bernstorff, ambasciatore tedesco a Washington

- Il telegramma doveva essere ritrasmesso a von Eckhardt, ambasciatore tedesco a Città del Messico
- L'ambasciatore lo avrebbe consegnato al presidente messicano

Il telegramma di Zimmermann

Il telegramma fu intercettato dalla Gran Bretagna e decifrato dai suoi crittoanalisti

- Non fu inviato subito agli americani

Il 1 febbraio 1917 la Germania comunicò agli USA la decisione sull'uso illimitato degli U-boot

- Gli USA decisero di restare neutrali
- Bisognava mostrare loro il contenuto del telegramma senza svelare il ruolo dei crittoanalisti britannici

Un agente britannico in Messico trafugò la versione messicana del telegramma e la rese pubblica

- Il 2 aprile 1917 gli USA decisero di entrare in guerra

Decifratura del telegramma

Group-by-group decodement of the Zimmermann Telegram as sent by Ambassador Bernstorff to German Minister von Eckhardt in Mexico on January 19, 1917.

130	Nr. 3	13851	stop	18507	hinzufuegen
13042		4458	gemeinsamen	52262	Japan
13401	Auswaertiges Amt	17149	Friedenschluss	1340	von
8501	telegraphiert	14471	stop	22049	sich
115	vom 16ten Januar	6706	reichliche	13339	aus
3528	colon	13850	finanzielle	11265	zu
416	Nr. 1	12224	Unterstuetzung	22295	sofortiger
17214	Ganz geheim	6929	und	10439	Beitretung
6491	Selbst	14991	Einverstaendnis	14814	einladen
11310	zu	7382	unsererseits	4178	infinitive with zu
18147	entziffern	15857	dass	6992	und
18222	stop	67893	Mexiko	8784	gleichzeitig
21560	Wir	14218	in	7632	zwischen
10247	beabsichtigen	36477	Texas	7357	uns
11518	am	5870	comma	6926	und
23677	ersten	17553	Neu	52263	Japan
13605	Februar	67893	Mexiko	11267	zu
3494	un	5870	comma	21100	vermitteln
14936	eingeschraenkten	5454	Ar	21272	stop
98092	U-boot	16102	iz	9346	Bitte
5905	krelg	15217	on	9559	den
11311	zu	22801	a	22464	Praesidenten
10392	beginnen	17138	frueher	15874	darauf
10371	stop	21001	verlorenes	18502	hinweisen
0302	Es wird	17293	Oeltuch	18500	comma
21290	versucht	7446	zurueck	15857	dass
5161	werden	23638	erobert	2188	rueecksichtslose
39696	Vereinigte Staaten von Amerika	18222	stop	5376	Anwendung
23571	trotzdem	6719	Regelung	7381	unserer
17504	neutral	14331	im	98092	U-boote
11269	zu	15021	einzelnen	16127	jetzt
18276	erhalten	23845	Euer Hochwohlgeboren	13486	Aussicht
18101	stop	3156	ueberlassen	9350	bietet
0317	Fuer den Fall	23552	stop	9220	comma
0228	dass dies	22096	Sie	70036	England
17694	nicht	21604	wollen	14219	in
4473	gelingen	4797	Vorstehendes	5144	wenigen
22284	sollte	9497	dem	2831	Monat
22200	stop	22464	Praesidenten	17920	en
19452	schlagen	20855	streng	11347	zum
21589	wir	4377	geheim	17142	Frieden
67893	Mexiko	23610	eroeffnen	11264	zu
5569	auf	18140	comma	7667	zwingen
13918	folgender	22260	sobald	7762	stop
8598	Grundlage	5905	Kriege	16099	Empfang
12137	Buendnis	13347	ausbruch	9110	bestaetigen
1333	vor	20420	mit	10482	stop
4725	stop	39689	Vereinigten Staaten	97556	Zimmermann
4458	Gemeinsame	13732	fest	3569	stop
5905	Kriege	20667	steht	3670	Schluss der Depesche
17166	fuehrung	6929	und		
		5275	Anregung		

Un cifrario perfetto

One-time pad, Gilbert Vernam, impiegato AT&T, 1917

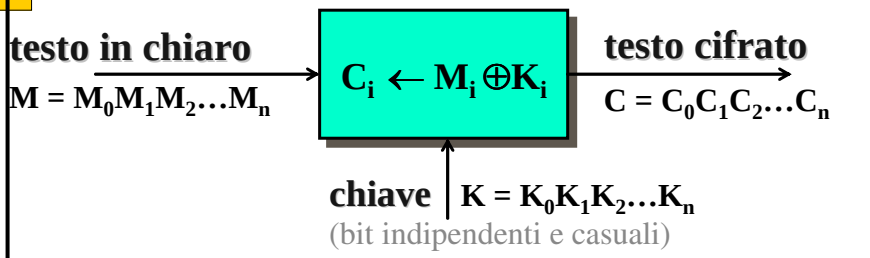
testo in chiaro $M = M_0M_1M_2\ldots M_n$ → $C_i \leftarrow M_i \oplus K_i$ → **testo cifrato** $C = C_0C_1C_2\ldots C_n$

chiave $K = K_0K_1K_2\ldots K_n$

(bit indipendenti e casuali)

Esempio:	1 0 0 1 0 1 1 1 0 1 1 0	testo in chiaro
	0 0 1 1 1 0 1 0 1 0 1 0	chiave
	1 0 1 0 1 1 0 1 1 1 0 0	testo cifrato

One-time Pad



cifrario perfetto: M e C sono indipendenti

Prob (M=M´) = Prob (M=M´ |C=C´)

lunghezza chiave = lunghezza testo in chiaro

One-time Pad

Usato da:

- Spie russe
- Linea rossa Washington-Mosca
- Che Guevara per mandare messaggi a Fidel Castro
  - Scoperto nel 1969
  - Messaggi scritti in Spagnolo
  - Relazione fissa tra lettere e numeri

A 6	E 8	I 39	M 70	Q 71	U 52	Y 1
B 38	F 30	J 31	N 76	R 58	V 50	Z 59
C 32	G 36	K 78	O 9	S 2	W 56	
D 4	H 34	L 72	P 79	T 0	X 54	

Cifrario di Che Guevara

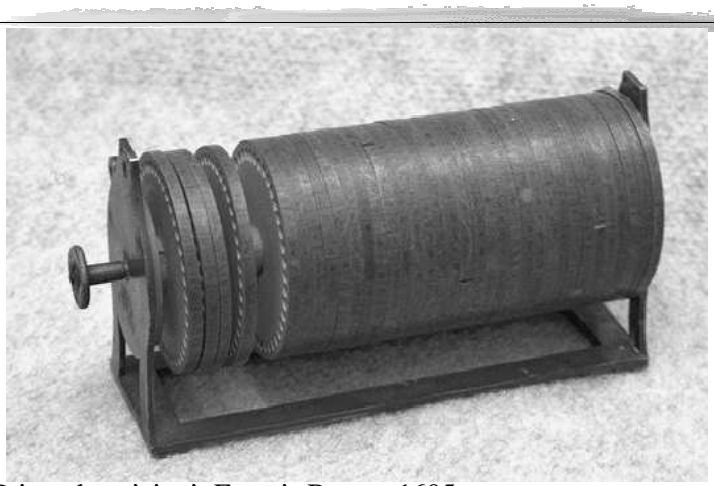
Messaggio diviso in gruppi di 5 cifre

random pad

Somma senza riporto

One time pad su alfabeto decimale

Cilindri cifranti

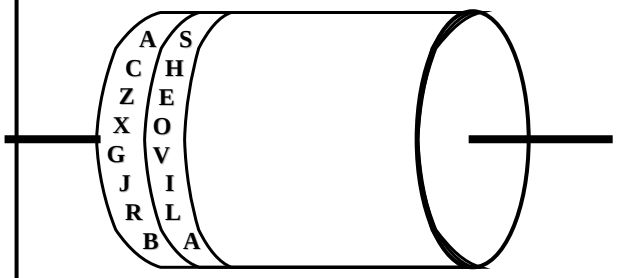


Prime descrizioni: Francis Bacon, 1605

Cilindro di Thomas Jefferson

Circa 1790 - 1800 (Terzo presidente US)

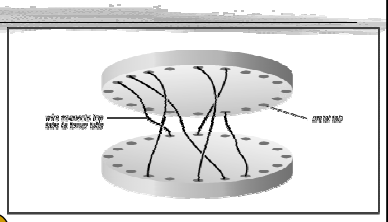
Cilindro di 15cm e 36 dischi di legno

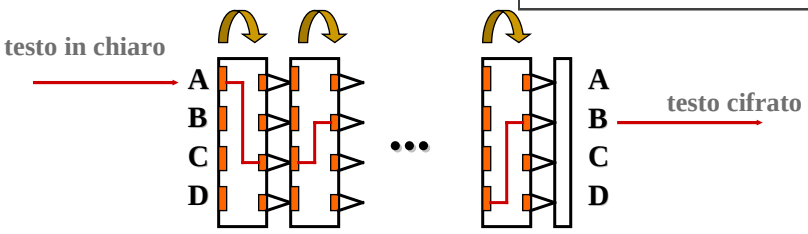


Numero possibili ordinamenti dei dischi = 36! ≈ $3.72 \cdot 10^{41}$

Rotori

Costruiti a partire dal 1918





Per alcuni, movimento come *odometro*

Rotori

Costruzione della prima macchina: E. H. Hebern [1918]

Primo brevetto [1921], *Hebern Electric Code, Inc.* prima azienda crittografica americana, bancarotta [1926]

- U. S. Navy, usa macchine a 5 rotori della *Hebern* [1929-1930]

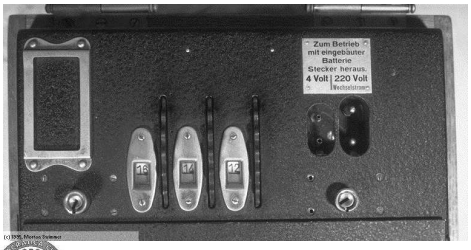
B. Hagelin, svedese, costruì:

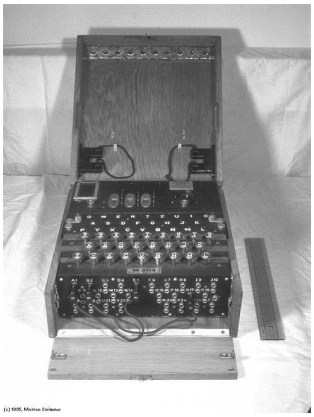
- B-21 [1925], usata dall'esercito svedese
- B-211
- C-36 per i Francesi [1934]
- C-48 (prodotte 140.000 macchine!), chiamate M-209 quando usate dall'esercito americano nella II guerra mondiale
- azienda svizzera dal 1948: C-52 CD-55, T-55, CD-57

Enigma

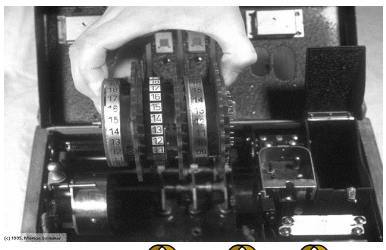
Sviluppata da Arthur Scherbius [1918]

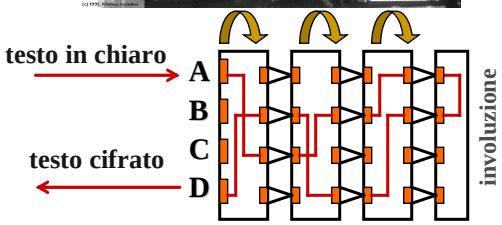
Usata nella II Guerra Mondiale



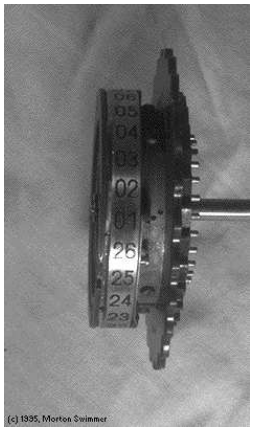


Enigma

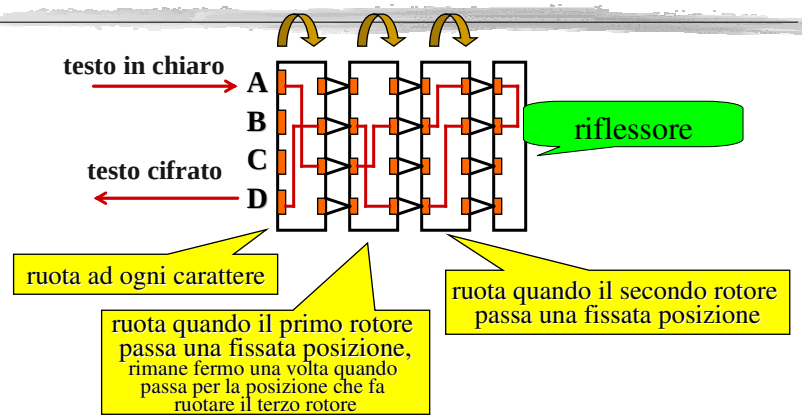




Enigma



Enigma: odometro



Con tre rotori, la cifratura torna al punto iniziale dopo 26x25x26=16900 sostituzione diverse

Le chiavi di Enigma

Rotori o scambiatori:
- 26x26x26=17576 combinazioni possibili

Unità cifrante:
- I tre rotori (1,2,3) potevano essere inseriti in 6 diverse posizioni: 123, 132, 213, 231, 312, 321

Pannello a prese multiple:
- Gli abbinamenti di 6x2 lettere sono 12 su 26 cioè 100.391.791.500

Numero di chiavi totali: 10 milioni di miliardi…

Chiave giornaliera

1. Assetto del pannello
   - Es. A/L – P/R – T/D – B/W – K/F – O/Y
2. Disposizione dei rotori
   - 1 -3 – 2
3. Orientamento dei rotori
   - Q – C – W

Per maggiore sicurezza si utilizza una chiave di messaggio:

- Es chiave giornaliera QCW
- Chiave messaggio PGH, ripetuta PGHPGH
- Cifratura di PGHPGH tramite QCW, → KIVBJE
- Cifratura e trasmissione del messaggio tramite PGH

Crittoanalisi in Polonia

Rejewski sfrutta la ripetizione della chiave di messaggio per ricostruire l'assetto iniziale di Enigma

- Studio delle concatenazioni
  - Il numero di collegamenti non dipende dal pannello a prese multiple
- Scoperta dell'assetto dei rotori che ha generato le concatenazioni osservate
  - 6 x 16900 = 101400…cento miliardi di volte più piccolo del numero di chiavi possibili!

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

Concatenazioni:	Numero di collegamenti:
A -> F -> W -> A	3
B -> Q -> Z -> K -> V -> E -> L -> R -> I -> B	9
C -> H -> G -> O -> Y -> D -> P -> C	7
J -> M -> X -> S -> T -> N -> U -> J	7

Crittoanalisi in Polonia

- Compilazione del repertorio del numero di collegamenti e degli assetti dei rotori (circa 1 anno di lavoro)
- Progettazione di "bombe" per la ricerca della chiave giornaliera
  - Poiché i rotori potevano essere posti in sei posizioni diverse occorrevano sei "bombe" che funzionavano in parallelo
- Nel 1938, modifiche ad Enigma
  - Aggiunti due nuovi rotori e pannello a prese multiple modificato da 6 a 10 coppie di lettere
  - Numero delle combinazioni dei rotori: da 6 a 60…necessarie altre 54 "bombe"…
  - Numero lettere scambiate: da 12 a 20 (su 26 possibili)
  - Numero di possibili chiavi: 159 miliardi di miliardi!

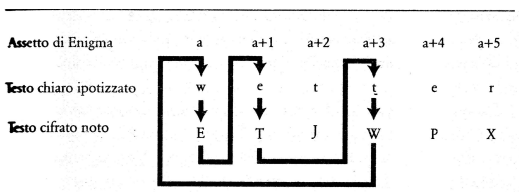
Crittoanalisi a Bletchley Park

- Nel 1939 il materiale dei polacchi fu trasferito alla *Government Code and Cipher School* di Bletchley Park, Inghilterra
  - Da 200 a 7000 persone in 5 anni (matematici, scienziati, linguisti, maestri di scacchi)

- Alcune debolezze di Enigma:
  - Nessuna lettera cifra sè stessa
  - Una lettera non cifra lettere contigue
  - Se LET1 cifra LET2
    allora LET2 cifra LET1
  - Utilizzo di cillies, chiavi semplici (es. qweqwe)

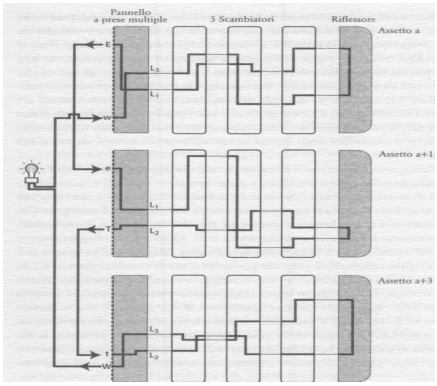
Crittoanalisi a Bletchley Park

- Il contributo più significativo fu dato da Alan Turing
  - Individuazione di "crib", frammenti di testo in chiaro che possono essere dedotti dal testo cifrato
    - Esame dei bollettini metereologici, trasmessi periodicamente
    - WETTER = tempo atmosferico, presente in posizioni fisse
  - Progettazione di un circuito che collegava tre Enigma, con assetti a, a+1, a+3



Crittoanalisi a Bletchley Park

- Il circuito è percorso dalla corrente solo quando tutte e 3 le macchine sono nel giusto assetto
  - Procedimento automatizzato, ma non semplificato (159 miliardi di miliardi di combinazioni per ogni macchina)

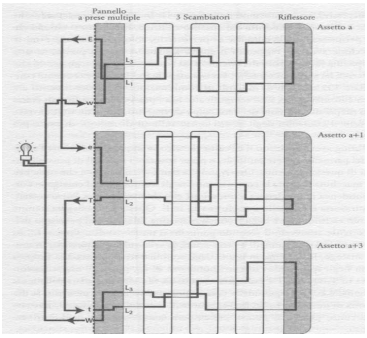


Crittoanalisi a Bletchley Park

- Idea: annullare gli effetti del pannello a prese multiple
  - Creare 26 circuiti, collegando le 26 uscite del primo gruppo di rotori con i 26 ingressi del secondo gruppo
  - Per controllare tutti gli orientamenti, con tre rotori e 60 combinazioni, necessari 60 gruppi di tre macchine che lavorano in parallelo

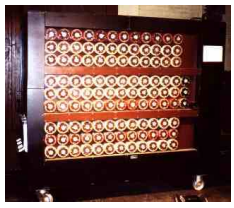
Solo 16.900 combinazioni per ogni macchina!

Controllo degli assetti cento milioni di volte più facile!



Crittoanalisi a Bletchley Park

- Nel 1940, costruzione di "Victory", la prima "bomba di Turing"
  - 10.000 sterline
  - Dodici gruppi di rotori collegati elettricamente
  - Lenta (7 giorni per scoprire una chiave giornaliera)
- Cinque mesi dopo, costruzione di "Agnus Dei"
  - Veloce (un'ora per scoprire una chiave giornaliera)
  - Necessitava di un crib di partenza

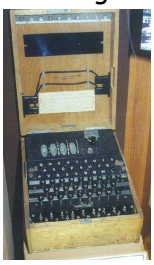


Testo chiaro ipotetico: w e t t e r n u l l s e c h s
Porzione del crittogramma: I P R E N L W K M J J S X C P L E J W Q

Testo chiaro ipotetico: w e t t e r n u l l s e c h s
Porzione del crittogramma: I P R E N L W K M J J S X C P L E J W Q

Crittoanalisi a Bletchley Park

- La Marina tedesca usava una versione più sofisticata di Enigma
  - 8 rotori invece di 5
  - 26 possibili orientamenti per il riflessore
  - Messaggi privi di formule stereotipate (niente crib)
  - Procedura per le chiavi di messaggio basato su sostituzioni di bigrammi



- Conseguenze:
  - 50 navi colate a picco al mese
  - 50.000 marinai alleati deceduti
- La risposta di Bletchley Park:
  - Attaccare le navi tedesche in punti determinati per costringerle ad inviare messaggi da cui ottenere crib
  - Trafugare le chiavi giornaliere mediante attacchi alle navi tedesche

Crittoanalisi a Bletchley Park

Impatto della decifrazione di Enigma secondo David Kahn:

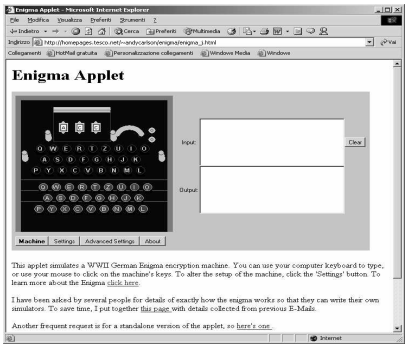
"Ha ridotto la perdita di vite umane.
Non solo vite di soldati alleati e russi, ma grazie alla minor durata del conflitto, anche di tedeschi, italiani e giapponesi.
Alcuni di loro che videro la fine del conflitto, avrebbero avuto una sorte diversa in mancanza di quelle decifrazioni.
E' questo il debito di tutti noi verso i crittoanalisti di Bletchley Park."

I successi di Bletchley Park rimasero segreti, fino al 1974

Simulatori di Enigma

Enigma applet

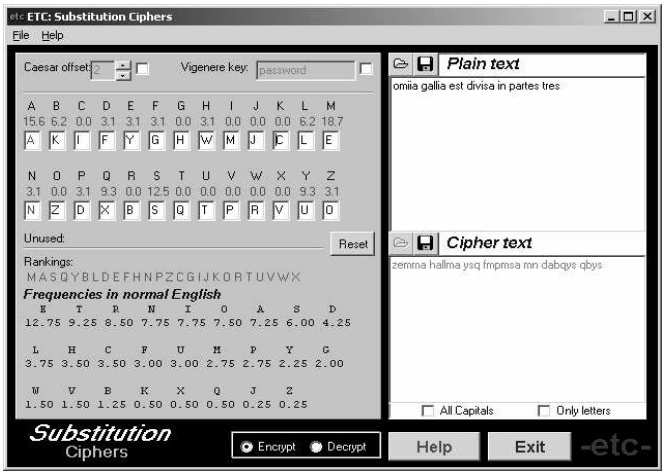
- http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html
- Versioni on-line e standalone, v2.3, 2001



Educational Tools for Cryptography

- http://www.cs.newcastle.edu.au/Research/DSG/
- etc.zip, 270 KB, luglio 1999
- Autore: Andrew White
- Windows
- Cifrari a sostituzione, con shift, Vigenere, analisi statistica

ETC



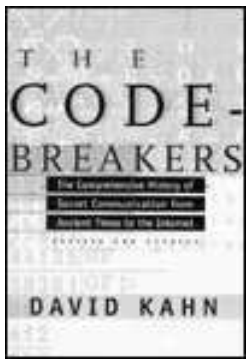
Bibliografia

David Kahn,

The codebreakers: the Story of Secret Writing

Macmillan, New York 1967

Simon & Schuster Trade 1200 pp., October 1996



Bibliografia

Simon Singh,
Codici & Segreti
Rizzoli ed., 1999

Bibliografia

- Cryptography: Theory and Practice, by D. Stinson (1995)
  - cap. 1
- Cryptography and Network Security by W. Stallings (2003)
  - cap. 1
- Tesina su crittografia classica
  - http://www.dia.unisa.it/professori/ads/
    - Sicurezza su reti, a.a. 1995-1996

Bibliografia

Richard J. Spillman,
Classical and Contemporary Cryptology
Pearson Prentice Hall, 2005