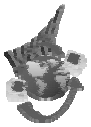
Crittografia

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

Crittografia Classica 0

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

Crittografia Classica 1

Caratteristiche delle scritture segrete

trasformazione
+
segretezza

↓

Crittografia

↙ Cryptos = segreto ↘ Grafien = scrittura

Crittografia Classica 2

Crittografia e civiltà antiche

- **Cina**: nessuna forma di crittografia pur essendo la scrittura antichissima
- **India**: crittografia sviluppata e praticata
  - Artha-Sastra servizi di spionaggio
  - Latila-Vistara esalta Budda, scritture perpendicolari, disordinate
  - Kama-Sutra tra le 64 arti (yoga), la 45-esima **mlecchita-vikalpa** che le donne debbono conoscere …

Crittografia Classica 3

Crittografia e civiltà antiche

- **Mesopotamia**: Assiri e Babilonesi (scritture cuneiformi) parti terminali delle parole sostituite con forme stereotipate (*colofoni*)
- **Iraq**: periodo terminale delle scritture cuneiformi

  Nomi vengono sostituiti da numeri

Crittografia Classica 4

Scritture segrete e Civiltà

La crittografia nasce **spontaneamente** non appena una società raggiunge un determinato livello di sviluppo

Crittografia Classica 5

Scritture segrete e Civiltà

- **Yezidis**: popolazione di circa 25.000 abitanti
  scritture segrete per proteggere i testi sacri dai musulmani
- **Tibetani**: scrittura segreta per la corrispondenza ufficiale
- **Nsibidi**: scrittura di tipo pittorico per esprimere concetti d'amore … tanto crittografica quanto pornografica

Scritture segrete e Civiltà

- **Thailandia**: diverse tecniche di cifratura
  - sostituzione
  - divisione delle lettere dell'alfabeto in gruppi
    Ogni lettera è indicata dal numero di gruppo e dalla posizione nel gruppo
- **Maldive**: due forme di scrittura segreta
- **Persia**: primo uso delle scritture segrete per documenti politici e di natura fiscale (600 d.C.)

Scritture segrete e testi sacri

Bibbia: tre tecniche 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

Daniele

Festa in onore di Baldassarre … (re babilonese)

… una mano apparsa dal cielo scrive sulla parete …

MENE MENE TELEK UPHARSIN

Il messaggio profetizzava la fine delle ricchezze del regno babilonese e la sua spartizione tra Medi e Persiani…

… il primo crittoanalista della storia!

Gorgo

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 ...

Alcuni metodi antichi di cifratura

- Erodoto
- **Scytala** spartana, 500 a.C. (Plutarco in *Vite parallele*)
- 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: C A S A

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

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 a sostituzione

chiave:

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

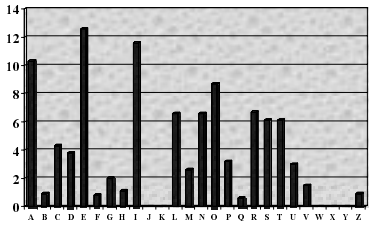
testo cifrato: T O P O

Cifrari con shift

Chiave K

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

Frequenze di 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	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

Crittoanalisi

Edgar Allan Poe, “Lo scarabeo d'oro”

messaggio scritto dal pirata Capitano Kidd, dice dove è nascosto il tesoro

5 3 ‡ † ı 3 0 5)) 6 * ; 4 8 2 6) 4 ‡ ı .) 4 ‡ ı) ; 8 0 6 *
A ΓΟΟΔ ΓΛΑΣΣ IN THE ΒΙΣΗΟΠ Σ ΗΟΣΤΕΛ IN
; 4 8 ı 8 ϒ 6 0)) 8 5 ; ‡ ı ı (; : ‡ ı * 8 ı 8 3 (8 8) 5 * ı
THE ΔΕξΙΛ Σ ΣΕΑΤ ΦΟΡΤΨ–ΟΝΕ ΔΕΓΡΕΕΣ ΑΝΔ

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 ®

Nulle

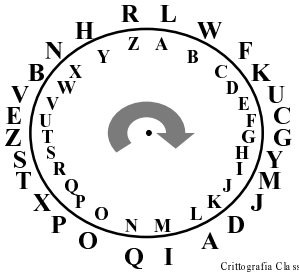
- Aggiungere simboli meno frequenti
  - in posizioni da non alterare il significato del testo in chiaro
- Aumento delle frequenze dei corrispondenti simboli

testo in chiaro: QUELQRAMODELQLAGO...

testo cifrato: …

Disco di Alberti

Leon Battista Alberti, architetto italiano, XV secolo



testo in chiaro

D I SCO

KMSFO

testo cifrato con rotazione "AL"

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 Playfair

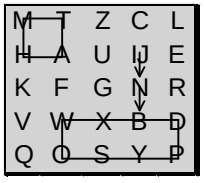
Progettato da Charles Wheatstone buon amico del Barone Lyon Playfair, XIX secolo

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

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

Anche rettangoli 4x7, 4x8,...

Cifrario di Playfair

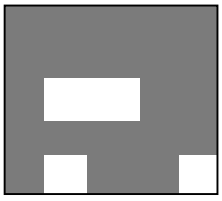


testo in chiaro: DO MA NI
testo cifrato: WP TH BN

Griglie

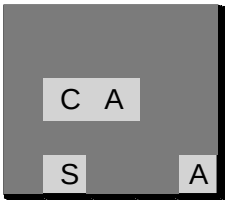
Girolamo Cardano, XVI secolo

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

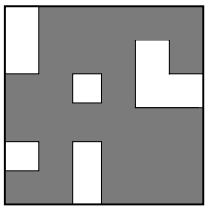
Girolamo Cardano, XVI secolo



Griglie con rotazioni

Usato dalla Germania poco prima della fine della I Guerra Mondiale
Quadrato invariante per rotazioni di 90° con 4 occorrenze di 1,…,9
Un solo quadrato per ogni intero

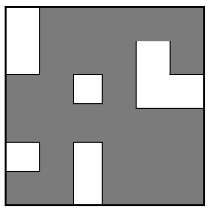
5	6	7	8	9	5
9	2	3	4	2	6
8	4	1	1	3	7
7	3	1	1	4	8
6	2	4	3	2	9
5	9	8	7	6	5



Griglie con rotazioni

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

5	6	7	8	9	5
9	2	3	4	2	6
8	4	1	1	3	7
7	3	1	1	4	8
6	2	4	3	2	9
5	9	8	7	6	5



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

Cifrari a sostituzione polialfabetica

Cifrario di Vigenère [1586] (Blaise de Vigenère, 1523-1596)

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 $K = K_0K_1K_2\ldots K_{i-1}$

Testo in chiaro: CODICE MOLTO SICURO Chiave: REBUS

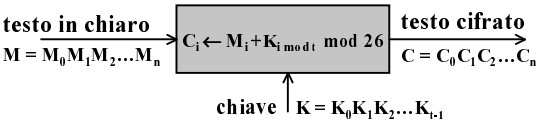
CODIC	EMOLT	OSICU	RO	testo in chiaro
REBUS	REBUS	REBUS	RE	chiave
TSECU	VQPFL	FWJWM	IS	testo cifrato

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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Cifrari a sostituzione polialfabetica

Cifrario di Vigenère [1586] (Blaise de Vigenère, 1523-1596)

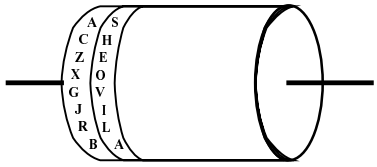


- Considerato inviolabile per molto tempo
- Numero possibili chiavi = 26^t
- Crittoanalisi: possibile romperlo usando *indice di coincidenza* ed *indice mutuo di coincidenza*

Cilindro di Thomas Jefferson

Circa 1790 - 1800 (Terzo presidente US)

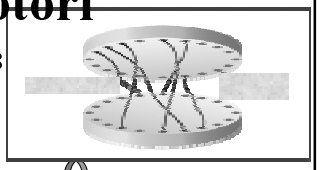
Cilindro di 15cm e 36 dischi di legno

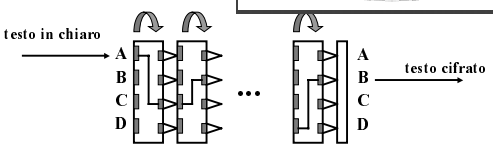


Numero possibili ordinamenti dei dischi = $36! \approx 3.72 \cdot 10^{41}$

Rotori

Costruiti a partire dal 1918





Per alcuni movimento come *odometro*

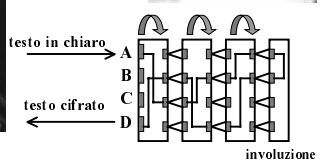
Rotori

- 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, costrui:
  - 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

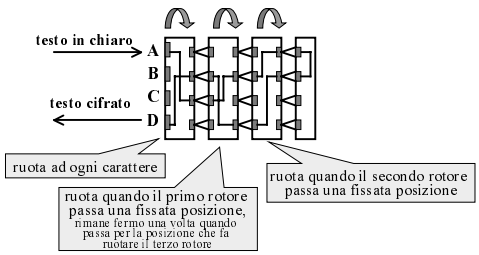
Enigma

Sviluppata da Arthur Scherbius [1918]

Usata nella II Guerra Mondiale



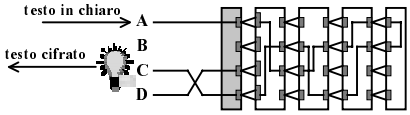
Enigma: odometro



Ciclo: 26 ·25 ·26 = 16.900 caratteri!

Enigma: inizializzazione

- **Walzenlage** scelta di 3 rotori tra 5 (Esercito e Aviazione) oppure tra 8 (Marina)
  Marina M4, quarto rotore, "greco" e sottile riflettore verso la fine della guerra
- **Umkehrwalze** scelta del riflettore
- **Ringstellung** posizionamento ordinato dei rotori
- **Steckers** posizionamento di una tavola di connessioni



Enigma: crittoanalisi

- Prima in Polonia
- Poi *Government Code and Cipher School* a Bletchley Park
- Alcune debolezze:
  - Nessuna lettera cifra se stessa
  - Se LET1 cifra LET2
    allora LET2 cifra LET1
  - Invio della posizione iniziale rotori

Alan Turing

Un cifrario perfetto

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

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

chiave $K = K_0K_1K_2...K_n$
(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

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

chiave $K = K_0K_1K_2...K_n$
(bit indipendenti e casuali)

cifrario perfetto: M e C sono indipendenti

Prob (M=M′) = Prob (M=M′ | C=C′)

One-time Pad

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

chiave $K = K_0K_1K_2...K_n$
(bit indipendenti e casuali)

cifrario perfetto: M e C sono indipendenti

Prob (M=M′) = Prob (M=M′ | C=C′)

lunghezza chiave = lunghezza testo in chiaro

Cifrario di Che Guevara

- Scoperto quando fu catturato dall'esercito Boliviano nel 1967
- Cifrario che usava con Fidel Castro
- Messaggi in spagnolo
- Associazione fissa lettere con 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

gruppi di 5 numeri
chiave: digit a caso
somma senza riporto

One-time Pad
alfabeto decimale

Esercizi

- Mostrare che:

  Prob (C=C′) = Prob (C=C′′)

  Prob (C=C′) = $1/2^{n+1}$
- Mostrare che:

  Prob (M=M′) = Prob (M=M′ | C=C′)

Bibliografia

David Kahn,

The codebreakers: the Story of Secret Writing

- Macmillan, New York 19
- Simon & Schuster Trade 1200 pp., October 1996