PRINCIPI DI CRITTOGRAFIA, IN PRATICA E IN TEORIA

Oggi festeggiamo pi greco

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

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

sostituzione

o g g i f e s t e g g i a m o p i g r e c o

q i i m h g u v g i i m c o q r m i t g e q

q i i m h g u v g i i

mco q r m i t g eq

trasposizione

q m i c i o m q h r g m u i v t g g i e i q

STEGANOGRAFIA

Steganografia tecnica:
- microfilm, inchiostri speciali,
- trasmissioni telegrafiche rapide,
- trasmissioni telefoniche a frequenza variabile, …

Steganografia simbolica:
- semagramma visuale (dettaglio grafico)
- semagramma linguistico (codice nascosto)
- messaggio in codice (alfabeto sconosciuto)

SEMAGRAMMI

Semagramma visuale:

viva la scienza

In un sottospazio vettoriale U la somma di due vettori qualsiasi v_1 e v_2 di U è ancora in U ed il prodotto esterno di un vettore v di U per uno scalare qualsiasi è ancora in U. Questo significa che U è "chiuso" rispetto alle operazioni dello spazio.

Semagramma linguistico:

sono pauroso e temo spesso i corsi di geometria

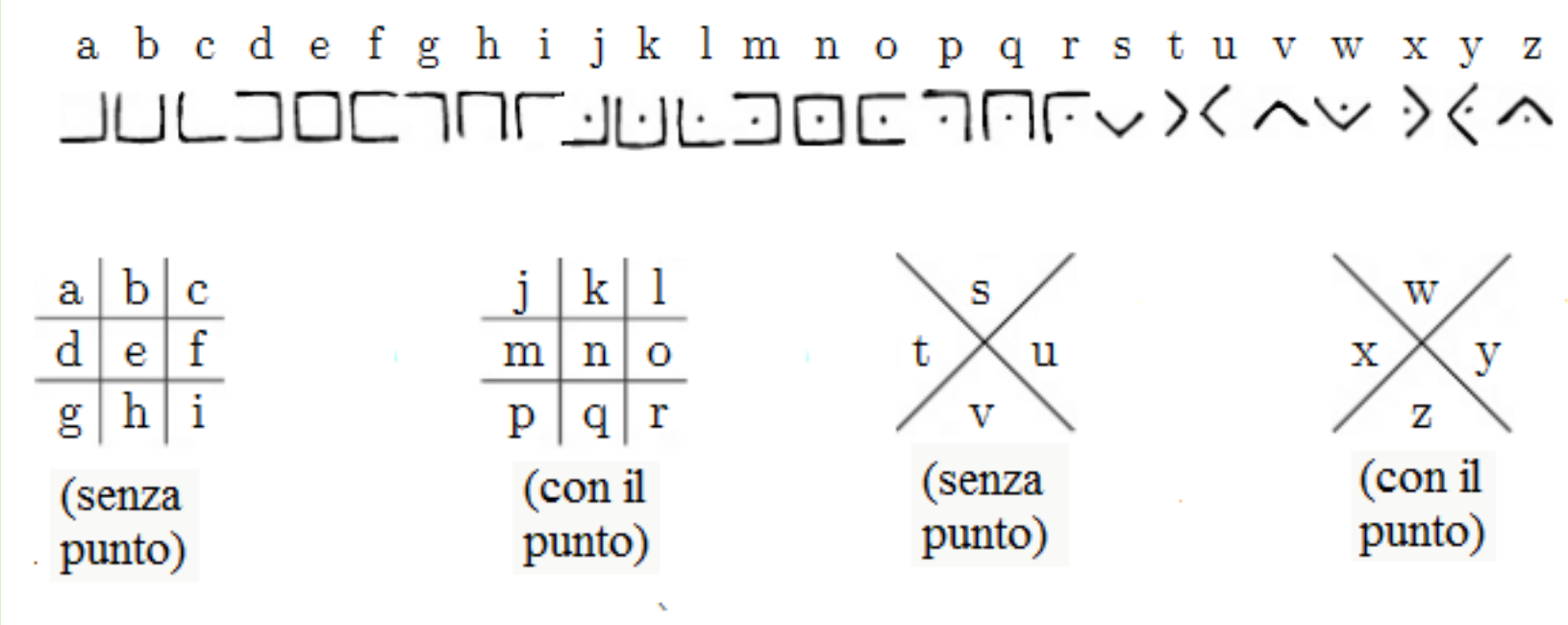
numero

Questo è un giorno speciale. Il testo di geometria dello spazio è stato finalmente pubblicato. È scritto in maniera straordinaria, in modo che si possa leggere in verticale o sdraiati sul letto.

CODICI SCONOSCIUTI

The Adventure of the Dancing Men (A. Conan Doyle)

AM HERE ABE SLANEY



Cifrario dei Rosacroce

SIMBOLI E NOMENCLATORI

Codice papale del XIV secolo: egiziani = ghibellini

figli di Israele = guelfi

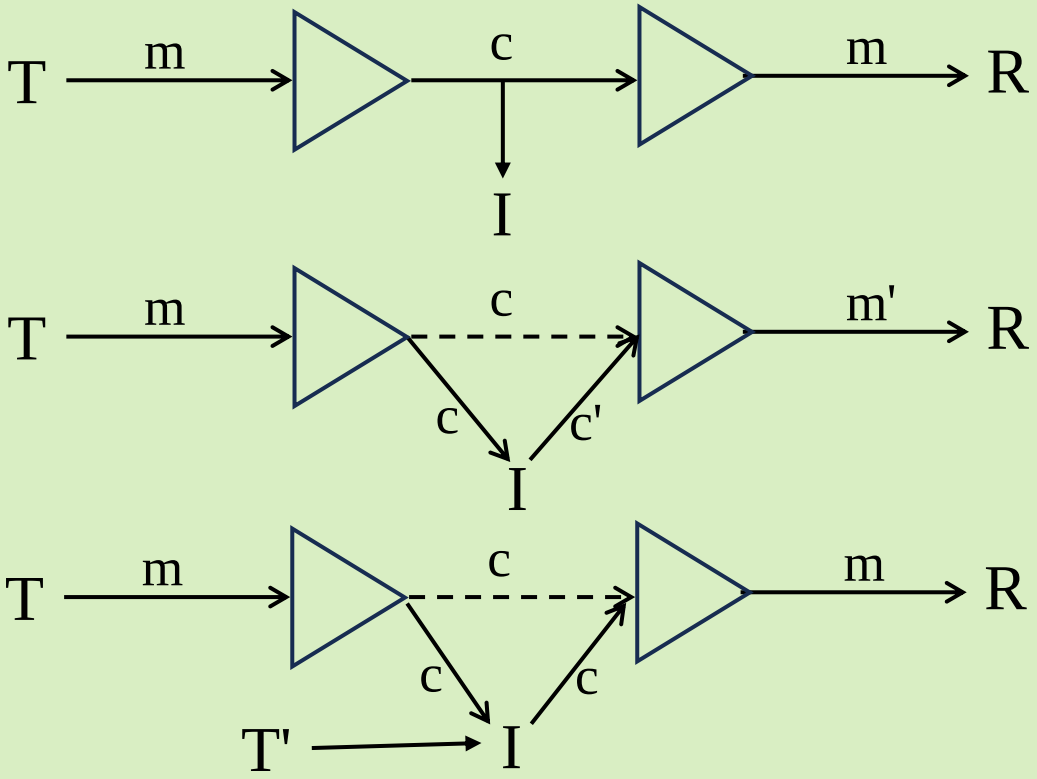
Codice francese XVII secolo: giardino = Roma

rosa = Papa

scuderia = Germania

finestra = fratello del re

CRITTOGRAFIA



Trasmissione / intercettazione del messaggio

Esempio: decrittazione di Enigma a Bletchey Park (Alan Turing, 1942)

Integrità del messaggio

Esempio: Romeo e Giulietta

Autenticità del mittente

Esempio: segretezza bancaria, sorteggio a distanza, “conoscenza zero”, …

CIFRARIO PER DIGRAMMI

(Giovan Battista della Porta, *De furtivis literarum notis*, 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

GA	LL	IA	ES	TD	IV	IS	AI	NP	AR	TE	ST	RE	S
156	297	208	122	497	229	226	8	353	17	498	487	446	18

PAROLA CHIAVE

Esempio: k = (AVE, 4)

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

o g g i f e s t e g g i amop i g r e c o
i b bd e vo pv b bd t g i l d b nv z i

	0 1 2 3 4 5 6 7 8 9
1	p i e t r o a b c d
2	f g h l m n q s u z

Giovanni Battista Argenti
(1580)

o g g i f e s t e g g i a m o p i g r e c o
15 21 21 11 20 12 27 13 12 21 21 11 16 24 15 10 11 21 14 12 18 15

PRINCIPIO DI KERCKHOFFS

k = permutazione arbitraria

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

$21! \approx 4 \times 10^{20}$ cifrari distinti

un computer che esamini un milione (10^6) di chiavi al secondo impiega milioni di anni per una ricerca completa

Auguste Kerkhoffs (*La criptographie militaire*, 1883):

La sicurezza di un sistema crittografico dipende <u>solo</u> dalla segretezza della chiave

LO SCARABEO D'ORO

Edgar Allan Poe (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(+?34;48)4+;161;:188;+?;

Claude Shannon, 1945 (Unicity distance): …con 30 lettere [di una cifratura monoalfabetica] si ha sempre una soluzione unica

8 = 33 → e
; = 26 → t
4 = 19 → h
+) = 16
* = 13
5 = 12
6 = 11
! 1 = 8
0 = 6
9 2 = 5
: 3 = 4
? = 3
` = 2
- = 1

. . .

CIFRARI A DOPPIACHIAVE

Il cifrario dei nichilisti (XIX sec.)

Chiave di cifrario AVE

Chiave di messaggio

Z A R

44 00 32

	0	1	2	3	4
0	**A**	**V**	**E**	B	C
1	D	F	G	H	IJ
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	W	X	Y	Z

P A L A Z Z O D I N V E R N O

30 00 21 00 44 44 24 10 14 23 01 02 32 23 24

44 00 32 44 00 32 44 00 32 44 00 32 44 00 32

24 00 03 44 44 21 13 10 41 12 01 34 21 23 01

O A B Z Z L H D W G V T L N V

DECRITTAZIONE STATISTICA

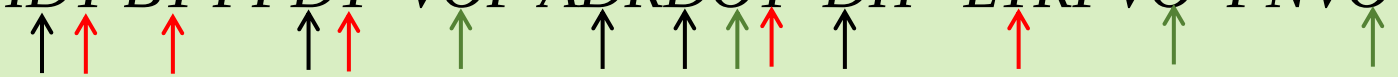
lett.	freq.	lett.	freq.
a	10,4	n	6,6
b	1,0	o	8,6
c	4,3	p	3,3
d	3,6	q	0,6
e	12,6	r	6,6
f	0,7	s	6,0
g	2,0	t	6,0
h	1,2	u	3,0
i	11,7	v	1,6
l	6,6	z	1,0
m	2,6		

Frequenza delle lettere
in un testo italiano

ESEMPIO

OMNIA GALL IA EST DIV I SA I N PARTES TRE S

I GHDT BT FFDT VOP ADRDOT DH LTRPVQ PNVQ



A = 1 *L* = 1

B = 1 *N* = 1

A, E, I ⟹ *D* = 5 *O* = 4 ⟸ R, S, T

F = 2 *P* = 3

G = 1 *R* = 1

H = 2 *T* = 5 ⟸ A, E, I

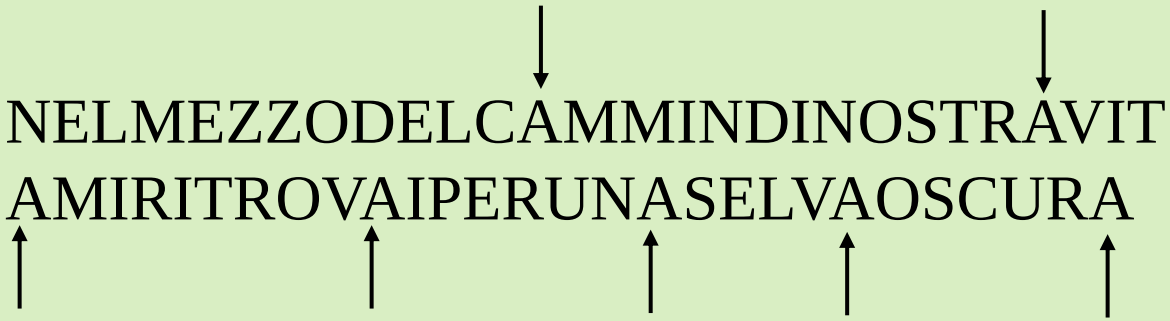
I = 1 *V* = 3

ESEMPIO

PGNOGBBQFGNECOOMPFMPQRITCAMV
COMTMVTQACMRGTZPCRGNACQREZTC

A = 3	H = 0	Q = 4
B = 2	I = 0	R = 4
C = 7	L = 0	S = 0
D = 0	M = 6	T = 5
E = 2	N = 3	U = 0
F = 2	O = 4	V = 3
G = 5	P = 4	Z = 2

Ipotesi: E, I, A
R, S



I CIFRARI POLIALFABETICI

Come rendere uguali le frequenze?

Omofoni

A → 11, 18, 37, 67, 54, 12, 43, 47, 98, 22
B → 72
C → 15, 29, 92, 32
D → 10, 36, 66
……

Nulle

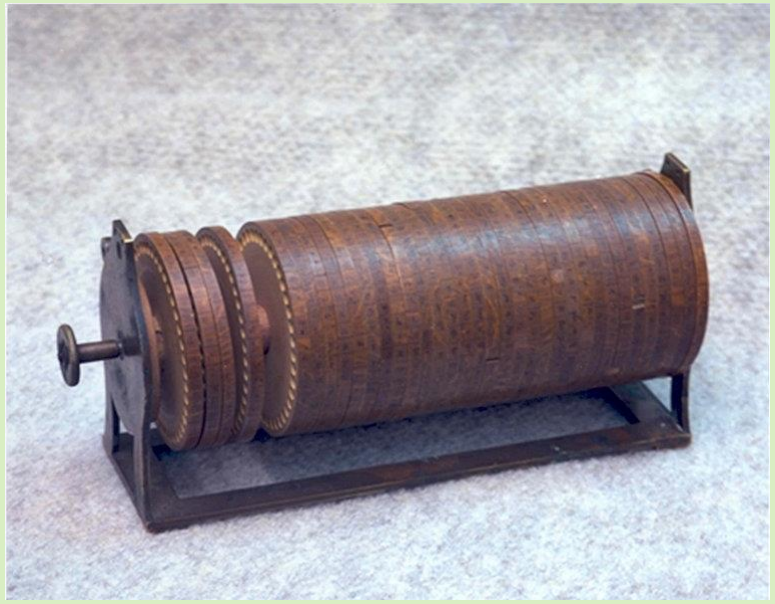
QUEL*Q*RAMO*U*DEL*Q*LAGO*U*DI*D*COMO...

IL DISCO CIFRANTE

Leon Battista Alberti (1404-1472)
(*De cifris*,1466)

CIFRATURE A DISCO ROTANTE

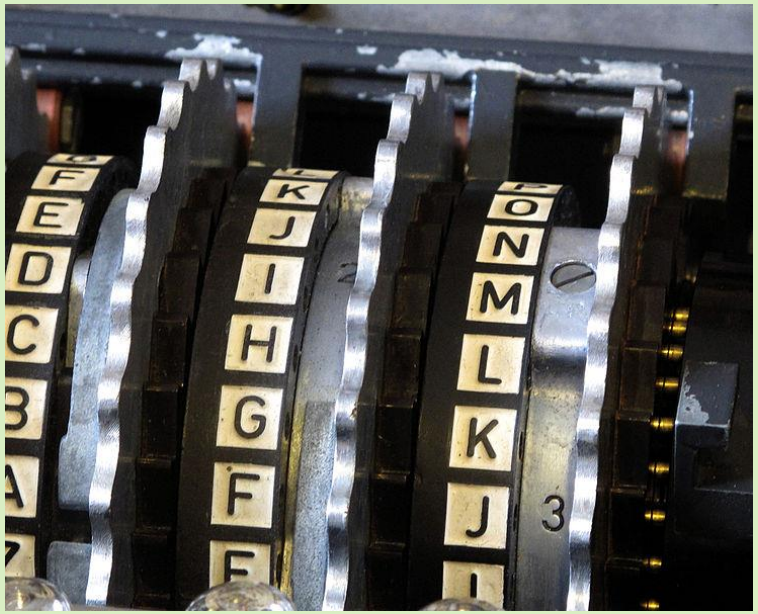
Disco di della Porta
(1563)



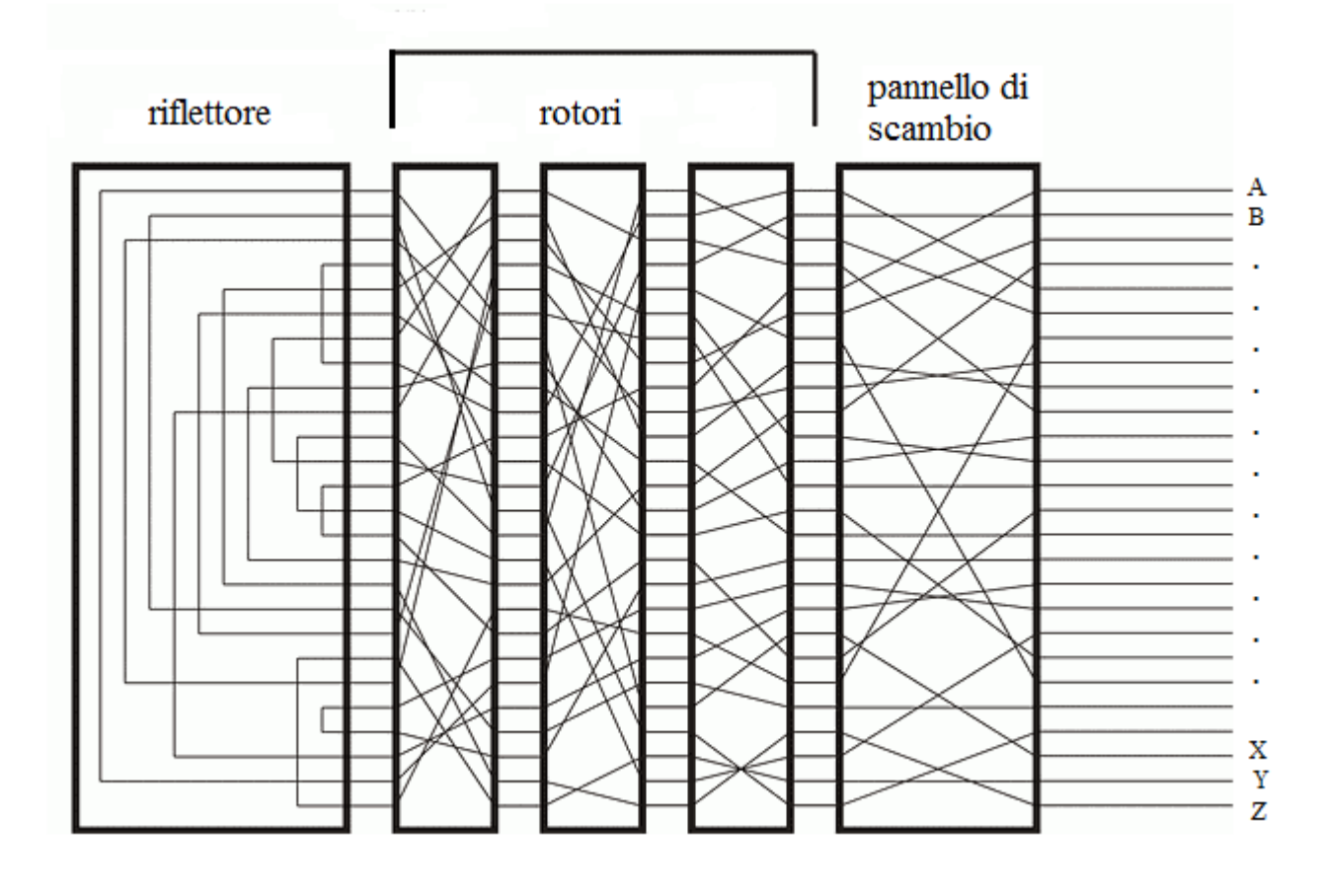
Disco di Jefferson
(1790-1800)
36 dischi di legno
$36! \approx 3.72 \cdot 10^{41}$

Disco di Hicks
(1893)

ENIGMA

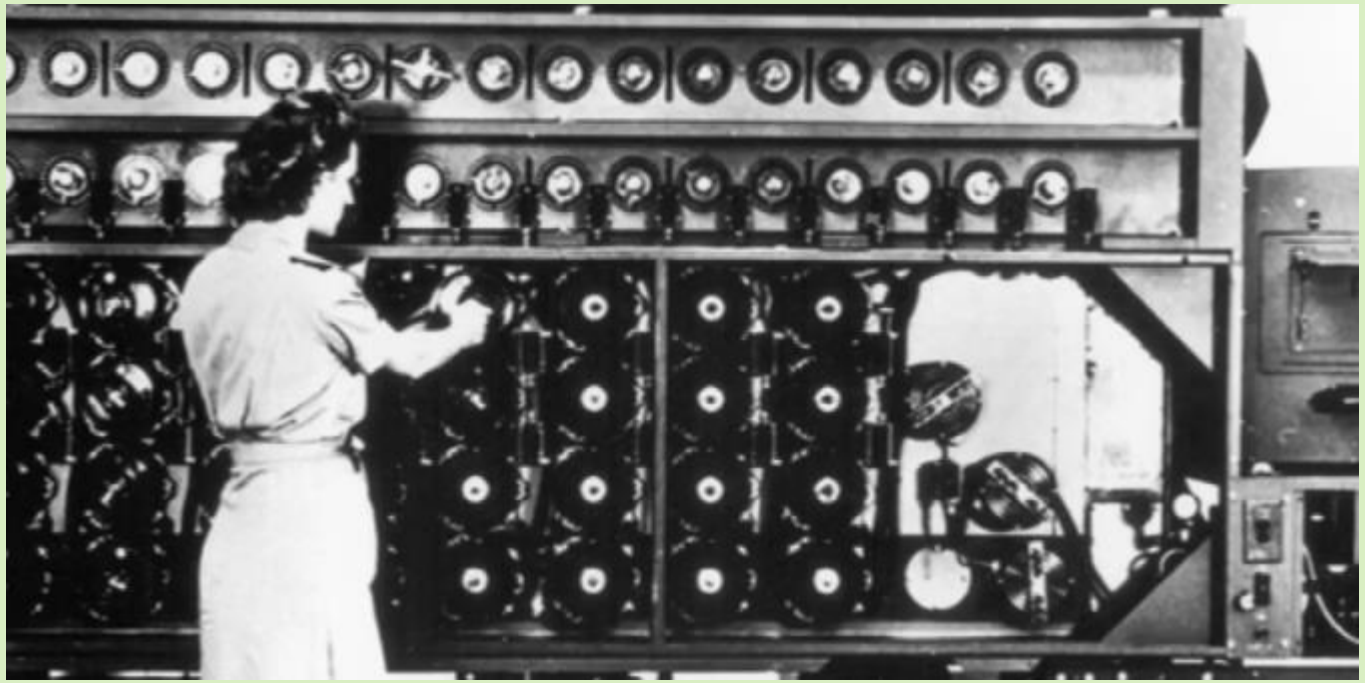


LO SCHEMA DI ENIGMA



$60 \times 17.576 \times 676 \times 1.507.382.749.373 \times 10^{14} \approx 10^{34}$ chiavi

LA BOMBA
(Alan Turing, 1942)



Ogni sistema di tamburi rotanti simula l’azione di un rotore di Enigma

IL CIFRARIO DI VIGENÈRE

Blaise de Vigenère (1523-1596)
Traité des chiffres ou secrètes manières d'escrire, 1586

NE LMEZZODELCAMMINDI …
P I G RECOP I GRECO P IGRE …

DORE …

IL METODO DI KASISKI
(1863)

Friedrich Kasiski (1805-1881), generale prussiano

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

18

E S S E R E O N O N E S S E R E Q U E S T O E I L P R O B L E M A
T O C T O C T O C T O C T O C T O C T O C T O C T O C T O C T O C

T O B E O R N O T T O BE T H A T I S T H E Q U E S T I O N
R U N RU N R U N R UN R U NR UNR UN R U N RU N R U N

K I O V I E E I G K I OV N UR N V J NU V K H VM G Z I A

9

L'INDICE DI COINCIDENZA

William Friedman (1891-1969) generale USA

Qual è la probabilità che due lettere di un testo, prese a caso siano uguali ?

Se P_A= 0,1 allora la probabilità di prendere a caso due lettere A è ≈ $P_A^2 = 0{,}01$

Indice di coincidenza: $K = P_A^2 + P_B^2 + \ldots + P_Z^2$

K_{it}	0,073	-	0,075
K_{en}	0,066	-	0,067
K_{fr}	0,077	-	0,080
K_{de}	0,076	-	0,082
K_{es}	0,076	-	0,077

K riflette la ridondanza della lingua

In un testo in cui tutte le lettere hanno la stessa frequenza: $P = 1/26$

$$K = \sum_{A}^{Z} \left(\frac{1}{26}\right)^2 = 26 \cdot \frac{1}{26^2} \approx 0{,}038$$

In un testo cifrato, K è tanto più vicino (ma maggiore) a = 0,038 quanto più il cifrario rende uguali le frequenze delle lettere

Se N è la lunghezza del testo
e K è l'indice di coincidenza:

$$L \approx \frac{0{,}037 \cdot N}{(N-1) \cdot K - 0{,}038 \cdot N + 0{,}075}$$

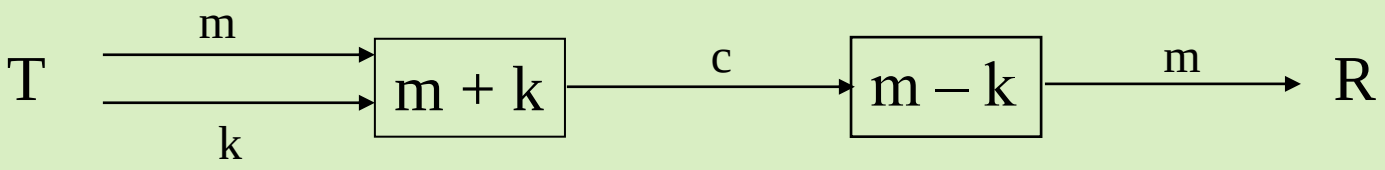
Se L è la lunghezza della parola chiave, allora le lettere nella posizione $1, L{+}1, 2L{+}1, 3L{+}1, \ldots$ sono cifrate in maniera monoalfabetica

LA CHIAVE INFINITA

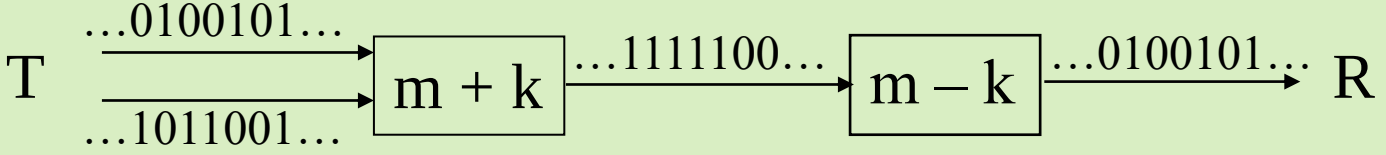
Esempio: La chiave è "I promessi sposi (edizione del 1841)" :

Quel ramo del lago di Como, che volge a mezzogiorno, tra due catene non interrotte di monti, tutto a seni e a golfi, a seconda dello sporgere e del rientrare di quelli, vien, quasi a un tratto …

Gilbert Vernam (1890-1960)



CIFRARI PERFETTI



+/−	0	1
0	0	1
1	1	0

somma binaria
/ or esclusivo

La chiave k deve essere
- casuale
- lunga quanto il messaggio
- usata una sola volta

Teorema (Shannon, 1949): *Il cifrario di Vernam è perfetto*

I CRITERI DI SHANNON

Claude Shannon (1916-2001): Communication Theory of Secrecy Systems, 1949

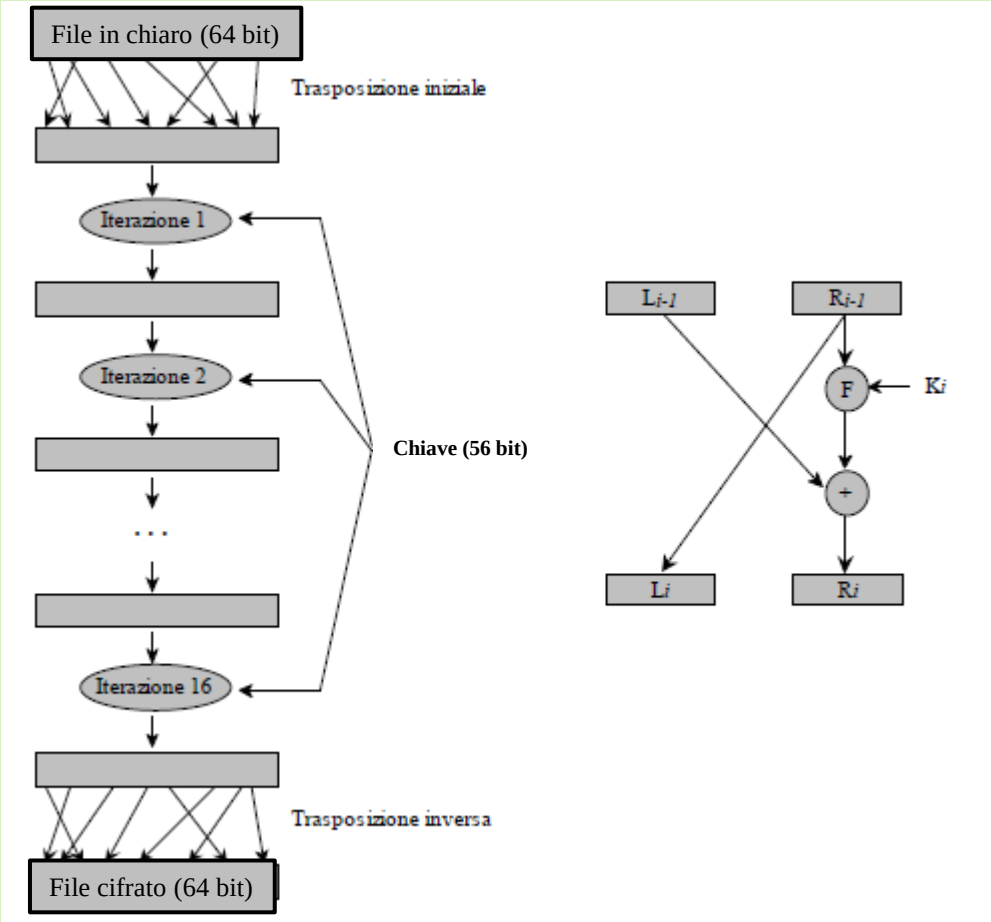
Diffusione: ogni simbolo del testo cifrato deve dipendere da tutti i simboli del testo in chiaro

Confusione: il testo in chiaro deve confondersi con la chiave

DES (Data Encryption Standard)

(algoritmo definito nel 1977 come standard di crittografia commerciale negli USA)

DES (DATA ENCRYPTION STANDARD)



Cifrario a blocchi di 64 bit (8 di controllo) con chiave di 56 bit

$$L_i = R_{i-1}$$

$$R_i = F(R_{i-1}, K_i) \oplus L_{i-1}$$

chiavi distinte $\approx 72 \times 10^{15}$

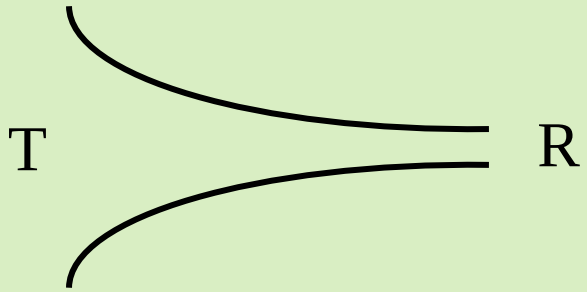
CANALI ASIMMETRICI

Difficoltà della trasmissione:

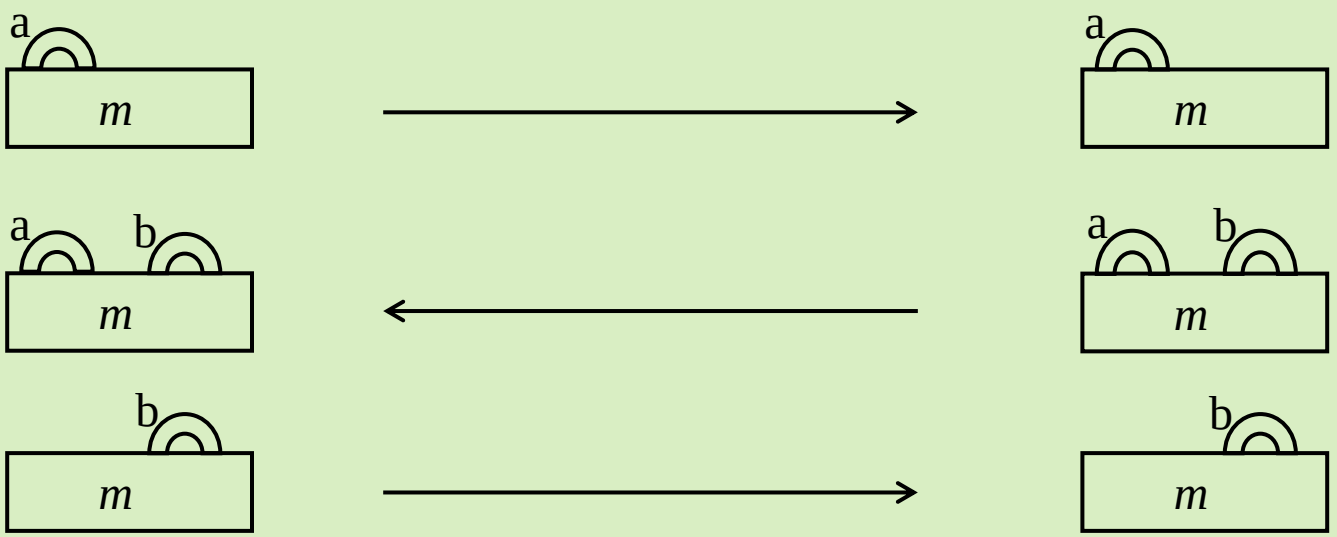
- riconoscimento del mittente
- condivisione della chiave
- necessità di $n(n-1)/2$ chiavi fra n corrispondenti

canale simmetrico

canale asimmetrico



LO SCAMBIO DELLE CHIAVI



T $\xrightarrow{n^a}$ R

R $\xrightarrow{n^b}$ T

$$n^{a \cdot b} = (n^a)^b = (n^b)^a$$

è la chiave comune di T ed R

LA CHIAVE PUBBLICA (1976)

$c = F(m)$ F è la chiave pubblica di ogni corrispondente: F_A, F_B, ….

$m = D(F(m))$ D è la chiave privata (da tenere segreta): D_A, D_B, …

F deve essere una "funzione unidirezionale" (one-way) facile da eseguire, che ammette una "inversa sinistra" D praticamente impossibile da determinare

Se inoltre vale anche $F(D(c)) = c$ (e quindi $D = F^{-1}$) allora F è una chiave pubblica "di autentificazione"

FUNZIONI UNIDIREZIONALI

Esempi:

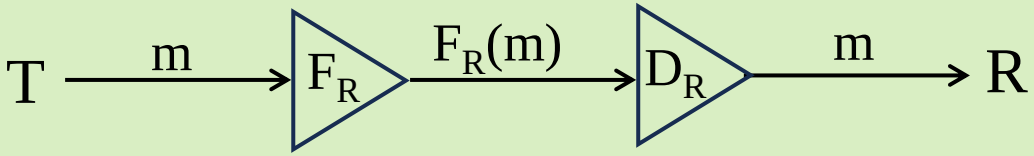
Prodotto di numeri interi / scomposizione in fattori primi
Esponenziale / logaritmo
Potenza / estrazione di radice

Vantaggi:

- Nessuno scambio di chiavi nella trasmissione del messaggio
- Occorrono meno chiavi in una comunità:
  Esempio ($n = 20$) partecipanti
  sistema simmetrico $n(n-1)/2 = 190$ chiavi diverse
  sistema asimmetrico $2n = 40$ "
- Facile accesso di nuovi utenti

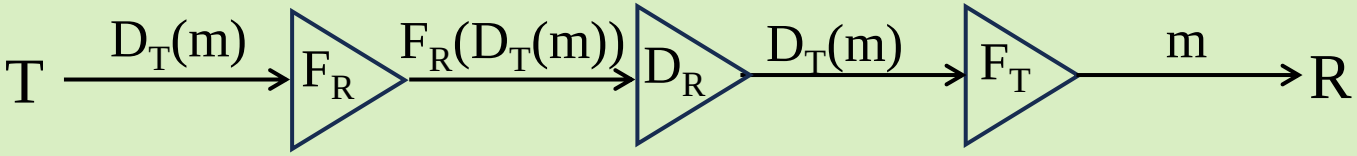
TRASMISSIONE DEL MESSAGGIO

F sia una funzione unidirezionale "a trabocchetto" (trapdoor one way)



$$D_R(F_R(m)) = m$$

Messaggio con firma



$$F_T(D_T(m)) = m$$

RSA

Rivest, Shamir, Adleman, 1978

Stabilità dei resti:

se a e b hanno lo stesso resto divisi per n ($a \equiv b$ modulo n)
se c e d hanno lo stesso resto divisi per n ($c \equiv d$ modulo n) allora
$a + c$ e b + d hanno lo stesso resto divisi per n ($a + c \equiv$ b + d modulo n)
e $a \cdot c \equiv$ b · d modulo n

Teorema di Eulero-Fermat:

Esiste una funzione (di Eulero) φ: $N \longrightarrow N$ tale che, se m ed n sono primi fra di loro, allora:

$$m^{\varphi(n)} \equiv 1 \text{ modulo } n$$

($m^{\varphi(n)}$ ha resto 1 se divisa per n)

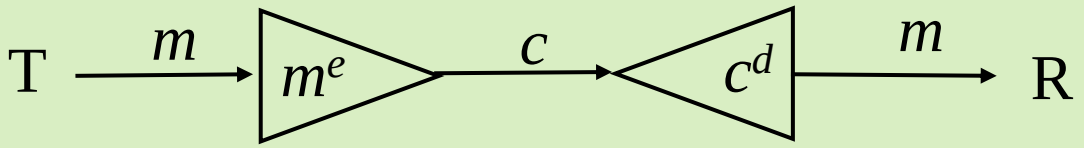
CRITTOGRAFIA RSA

R sceglie $n = p \cdot q$ prodotto di numeri primi. Allora $\varphi(n) = (p-1) \cdot (q-1)$

R pubblica la propria chiave pubblica (e,n), tale che e e $\varphi(n)$ siano primi fra di loro

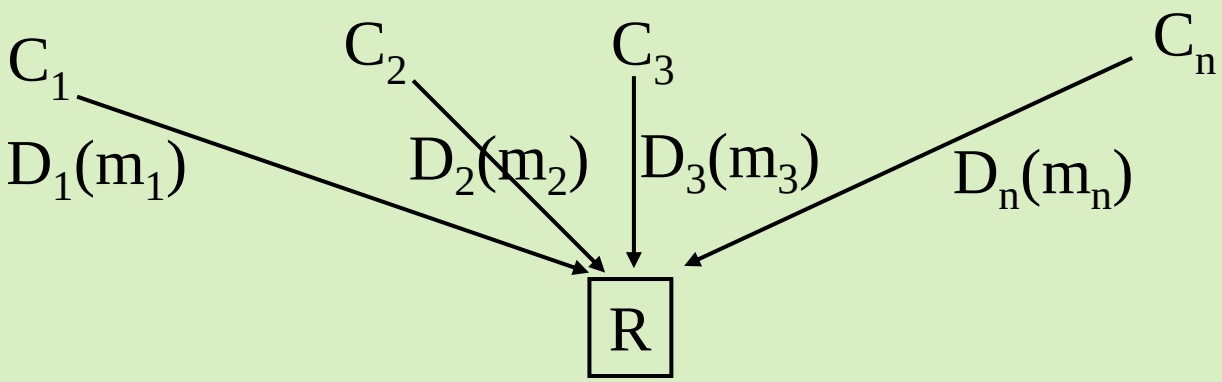
R calcola ma *non pubblica* la soluzione d dell'equazione $ex = k\varphi(n) + 1$

Se m è il messaggio in chiaro ($m < n$) di T, allora il messaggio in codice è c, resto della divisione di m^e per n



$$c^d \equiv (m^e)^d = m^{e \cdot d} = m^{k\varphi(n)+1} = m \cdot m^{k \cdot \varphi(n)} \equiv m$$

AUTENTICITÀ DEL MITTENTE



$$F_1(D_1(m_1)) = m_1$$
$$F_2(D_2(m_2)) = m_2$$
$$\ldots\ldots$$
$$F_n(D_n(m_n)) = m_n$$

SORTEGGIO A DISTANZA
(TESTA O CROCE)

- A sceglie n come prodotto di h fattori primi: $n = p_1 p_2 \ldots p_h$ e lo comunica a B (ma non dice i fattori, né – soprattutto – quanti sono)

- B deve indovinare se h (il numero dei fattori di n) è pari o dispari

- Se B indovina, vince. Altrimenti vince A

- B può controllare che la risposta è giusta quando **A** gli comunica i fattori $p_1\, p_2 \ldots .\, p_h$

BIBLIOGRAFIA

A. Sgarro, *Crittografia*, Muzzio 1985

L. Berardi, A. Beutelspacher, *Crittologia*, Franco Angeli 1996

S. Singh, *Codici e segreti*, Rizzoli 1997

C. Giustozzi, A. Monti, E. Zimuel, *Segreti, spie, codici cifrati*, Apogeo 1999

P. Ferragina, F. Luccio, *Crittografia. Principi, algoritmi, applicazioni*, Bollati Boringhieri 2001

S. Leonesi, C. Toffalori, *Numeri e crittografia*, Springer Italia 2006

D. Kahn, *The codebreakers: the story of secret writing*, Macmillan 1967

W. Diffie, M.E.Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory 1976

R. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM 1978

F.L. Bauer, *Decrypted secrets. Methods and maxims of cryptology,* Springer 1997