Codici Segreti

Agostino Dovier

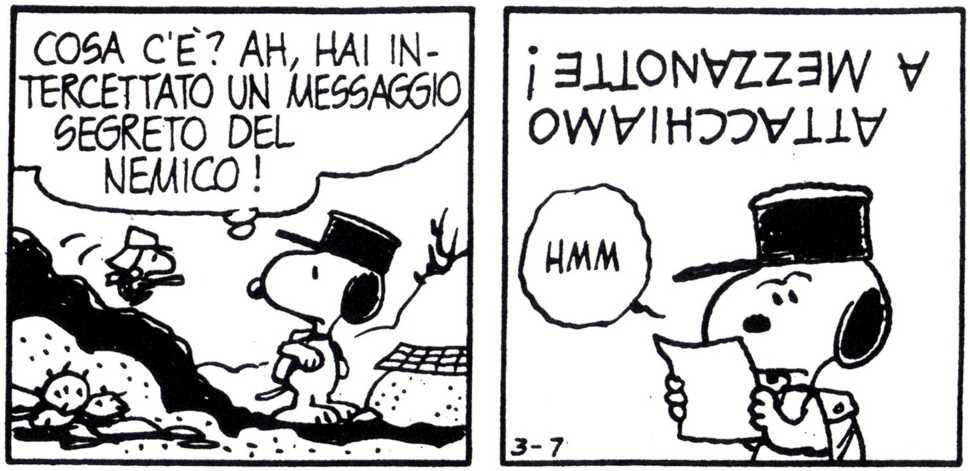
Dip di Matematica e Informatica, Univ. di Udine

Il festino di Baldassarre

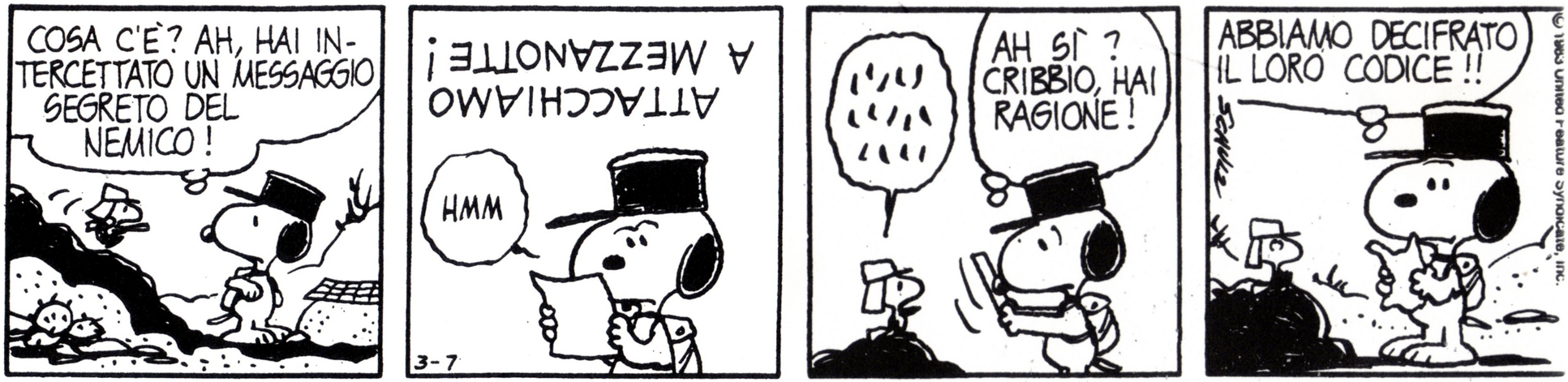
La profezia di Daniele

- Mene $\approx$ mnh (misurare), Tekel $\approx$ tql (pesare), Peres $\approx$ prs (dividere)
- Dio ha misurato il regno di Baldassarre e gli ha posto un termine, l'ha pesato sulla bilancia trovandolo mancante, il regno sta per essere diviso e consegnato ai Medi e ai Persiani.

Codici a Trasposizione



Codici a Trasposizione



Giulio Cesare (100–44 AC)

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

Cifrari a sostituzione polialfabetica

Algebra in $\mathbb{Z}_{26}$

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

Parola chiave: UDINE (=20,3,8,13,4).
Testo in chiaro: Oggi la lezione è noiosa.

O	G	G	I	L	A	L	E	Z	I	O	N	E	E	N	O	I	O	S	A
14	6	6	8	11	1	11	4	25	8	13	14	4	4	13	14	8	14	18	1
20	3	8	13	4	20	3	8	13	4	20	3	8	13	4	20	3	8	13	4
8	9	14	21	15	21	14	12	12	12	7	17	12	17	17	8	11	22	5	5
I	J	O	V	P	V	O	M	M	M	H	Q	M	R	R	I	L	W	F	E

Testo in cifra: IJOVPVOMMMHQMRRILWFE

Cifrari a sostituzione polialfabetica

Algebra in $\mathbb{Z}_2$

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 26 27 28 29	30 31

Chiave: UDINE= 20,3,8,13,4 = 10100, 00011, 01000, 01101, 00100

Testo in chiaro: Oggi la lezione è noiosa.

O	G	G	I	L	A	L	E	Z	I
01110	00110	00110	01000	01011	00001	01011	00100	11001	01000
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
11010	00101	01110	00101	01111	10101	01000	01100	10100	01100
♣	F	O	F	P	V	Q	M	U	M

O	N	E	E	N	O	I	O	S	A
01101	01110	00100	00100	01101	01110	01000	01110	01010	00001
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
01001	01101	01100	01001	01001	11010	01011	00110	00111	00101
J	N	M	J	J	♣	L	G	H	F

Testo in cifra: ♣FOFPVQMUMJNMJJ♣LGHF

Il cifrario perfetto

Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- È indecifrabile.
- Come comunichiamo la chiave?

Il cifrario perfetto

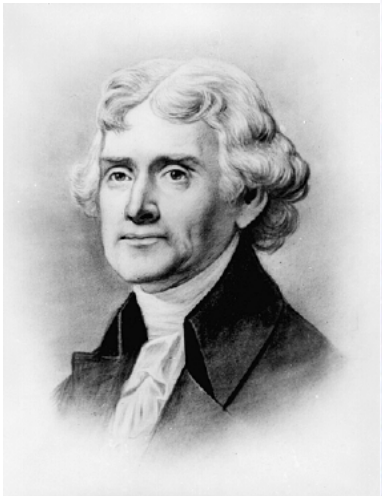
La linea rossa

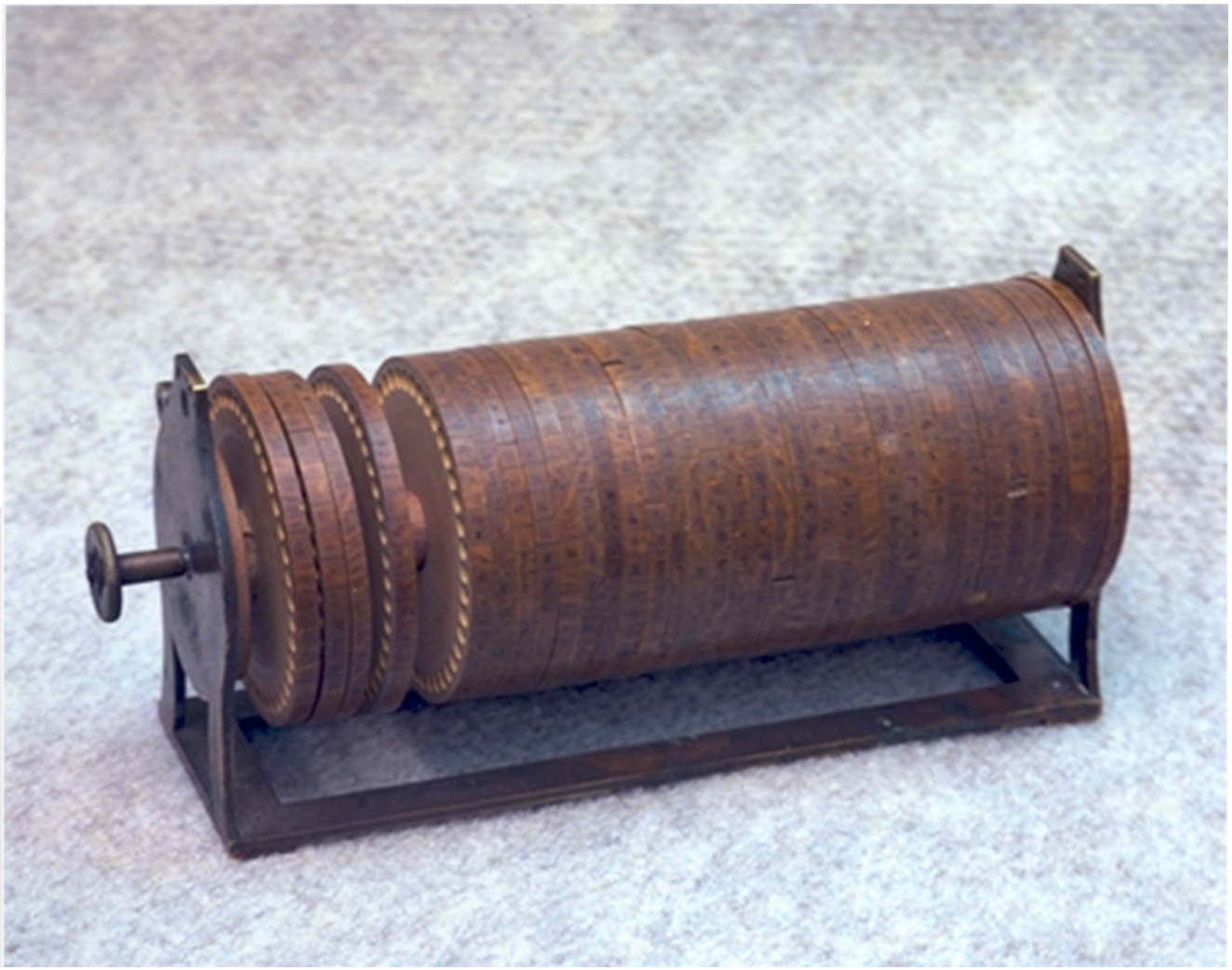
Il cifrario one-time-pad fu usato nelle comunicazioni USA–URSS durante la guerra fredda.




Ci dev'essere stato un piccolo esercito di lanciatori di monete.

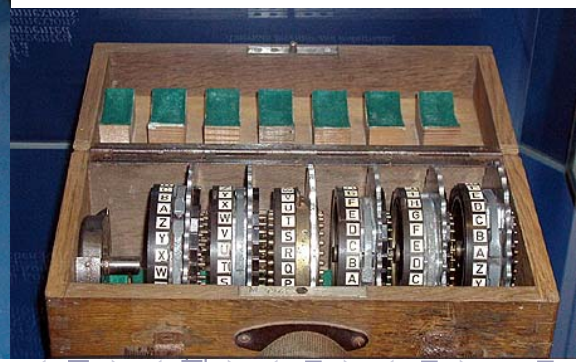
Il rotore di Thomas Jefferson (1743–1826)



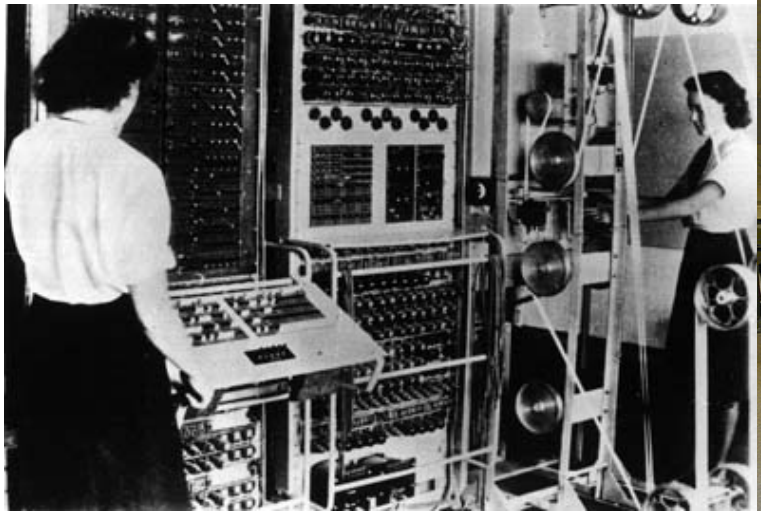


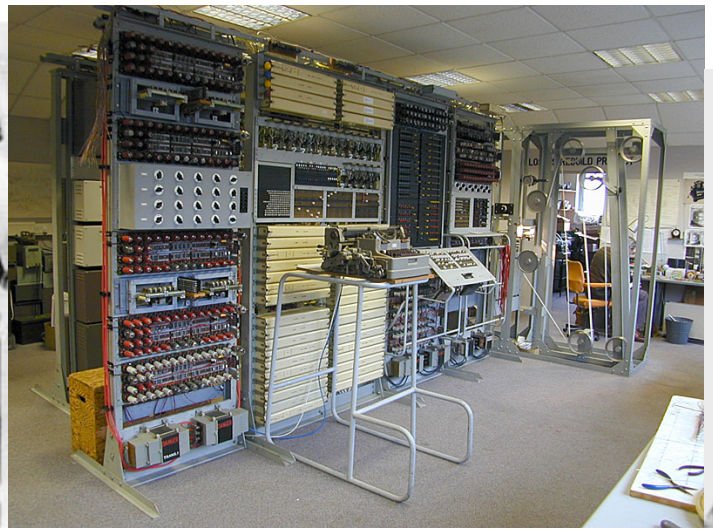
Enigma

Nel 1923 Scherbius commercializza l'Enigma.



Decrittazione automatica: Bombe e Colossi





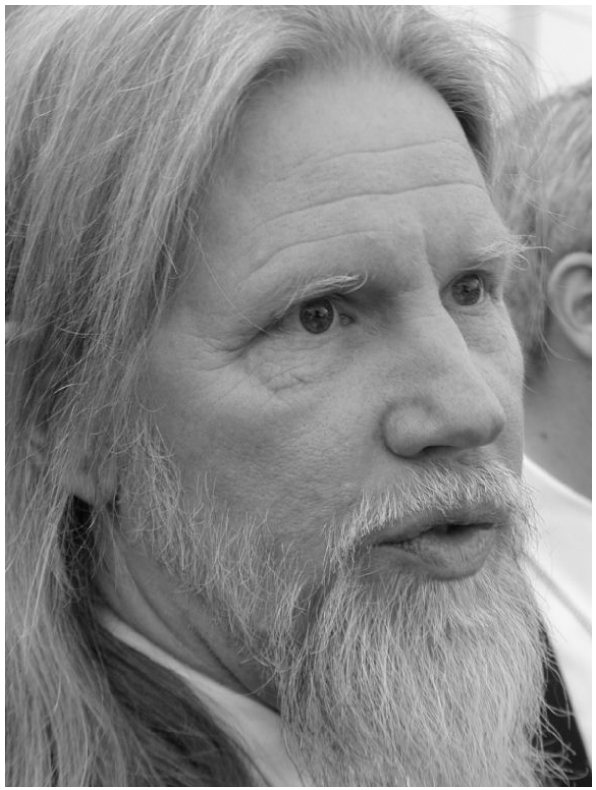
Nacque il calcolatore elettronico

Data/Advanced Encryption Standard

- DES (1975) fu forzato in diversi modi dal 1997 in poi.
- AES (Rijndael) fu annunciato dalla NIST come standard nel 2002
- Autori: Joan Daemen and Vincent Rijmen.

Crittografia a chiave pubblica

Diffie e Hellman



Crittografia a chiave pubblica

Idee generali

- Bob genera due chiavi, una privata H_B e una pubblica K_B. Lo stesso fa Alice (H_A e K_A).
- Alice e Bob (e tutti) pubblicano (in un elenco telefonico o in internet) una volta per sempre la loro chiave pubblica (K_A quella di Alice, K_B quella di Bob, etc.), nota a tutti.
- Alice vuole inviare il messaggio m a Bob.
- Alice codifica il messaggio m per Bob con la chiave pubblica di Bob (K_B) e invia il messaggio cifrato $COD(m, K_B)$.
- Bob riceve il messaggio $COD(m, K_B)$ e usa la sua chiave privata H_B per decodificare il messaggio.

Crittografia a chiave pubblica

Idee generali

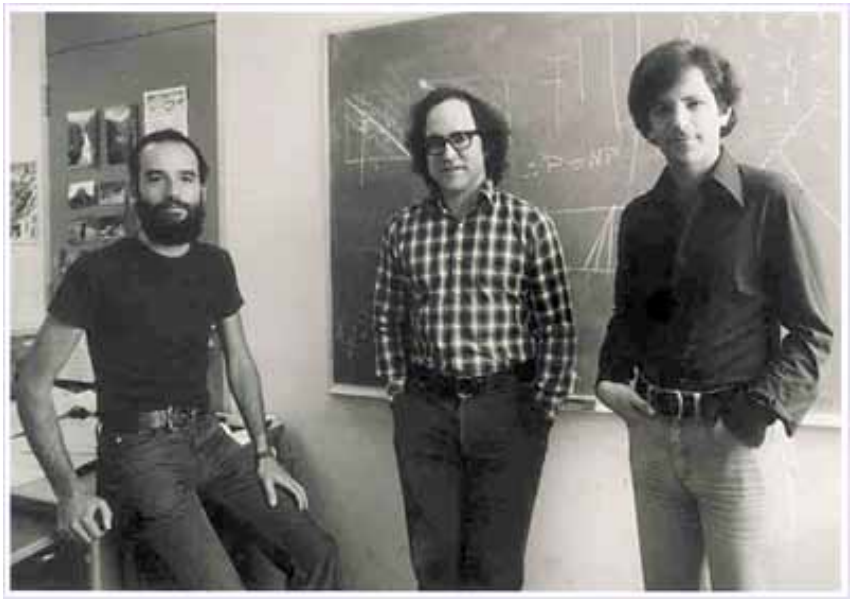
- Le due chiavi sono progettate in modo che

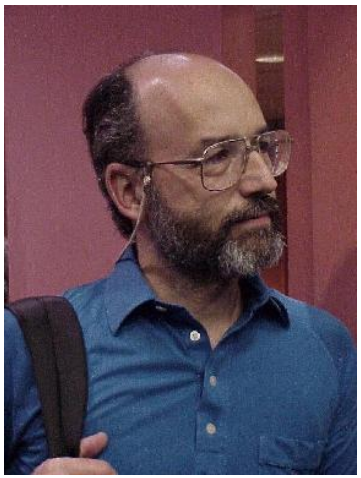
$$DEC(COD(m, K_B), H_B) = m$$

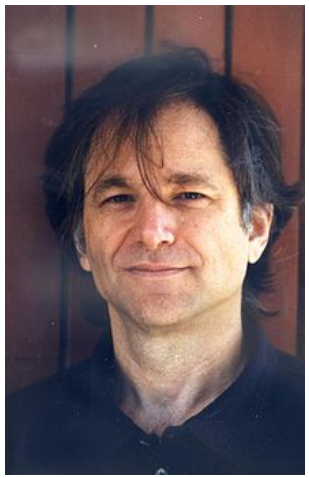
- L'operazione di decifrazione, sapendo la chiave privata dev'essere algoritmicamente facile
- L'operazione di decrittazione (per Charlie) deve essere algoritmicamente impraticabile.
- Anche se l'impresa è possibile: conoscendo K_B e $c = COD(m, K_B)$ si possono generare uno ad uno i messaggi di lunghezza opportuna, $m_1, m_2, \ldots, m_\ell$.
- Dunque si codificano uno ad uno con la chiave K_B e si vede se $COD(m_i, K_B) = c$.

Crittografia a chiave pubblica

Rivest, Shamir, e Adleman — Turing award 2002







Crittografia a chiave pubblica

Fattorizzazione

```
fattorizza(n)
    for i = 2 to sqrt(n)
        if n mod i == 0 {
            print(i," e' un divisore di ",n);
            exit;
        }
```

Nel caso peggiore compie un numero di passi pari a $\sqrt{n}$.
Possiamo togliere i pari, i multipli di 3, i multipli di 5, ma la sostanza non cambia.

Crittografia a chiave pubblica

Fattorizzazione

```
fattorizza(n)
   for i = 2 to sqrt(n)
      if n mod i == 0 {
         print(i," e' un divisore di ",n);
         exit;
      }
```

Nel caso peggiore compie un numero di passi pari a $\sqrt{n}$.
Possiamo togliere i pari, i multipli di 3, i multipli di 5, ma la sostanza non cambia.
Se n è un numero di 100 cifre, ogni divisione mi costa $10^{-10}s$, e dispongo di 10^9 processori, mi serve tempo

$$\approx \frac{10^{-10}\sqrt{10^{100}}}{3600 \cdot 24 \cdot 365 \cdot 10^9} = 3 \cdot 10^{23}\text{ANNI}$$

Sommario

http://www.dimi.uniud.it/dovier/CRYPTO

Si introdurranno, contestualizzandole storicamente, le principali tecniche impiegate nella cifratura e nella crittanalisi dei dati, partendo dai celebri codici cifrati dell'antico testamento, passando per la crittografia rinascimentale, per la crittografia meccanica della seconda guerra mondiale, e per il cifrario perfetto usato nella guerra fredda.

Saranno realizzati semplici programmi per automatizzare cifrazione e decifrazione e per la decrittazione basati sulla statistica.

Si giungerà alla crittografia a chiave pubblica enfatizzando come gran parte della sicurezza mondiale sia basata su un problema matematico apparentemente molto semplice su cui val la pena riflettere: la fattorizzazione di un numero naturale.

Anche in questo caso si verificherà sperimentalmente la difficoltà dello sviluppo di un fattorizzatore èfficiente.