Da Giulio Cesare al Datagate

Esplorare la matematica attraverso la crittografia

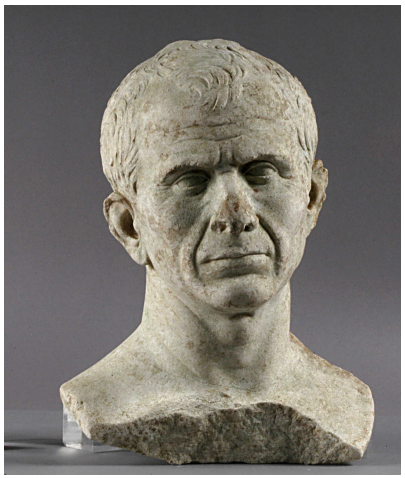
Ottavio Giulio Rizzo
Ottavio.Rizzo@UniMI.it

Dipartimento di matematica «Federigo Enriques»
Università degli Studi di Milano

XXXI convegno UMI–CIIM
Salerno, 17 ottobre 2013

Crittografia

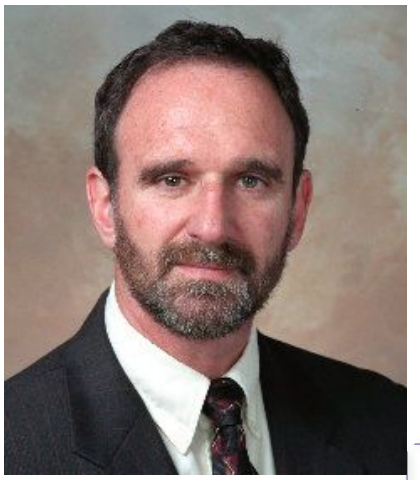
- κρυπτός nascosto — γράφω scrivere



Caio Giulio Cesare
(100-44 a.C.)

Leon Battista Alberti
(1404-1472)

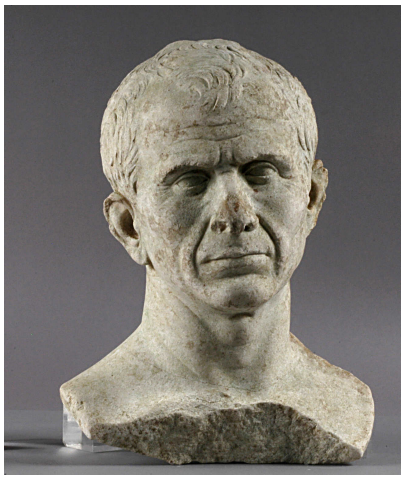
Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

Crittografia

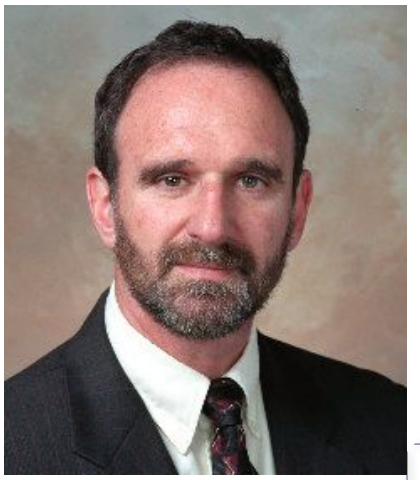
- κρυπτός nascosto — γράφω scrivere
- Cryptography is about communication in the presence of adversaries
  Ron Rivest



Caio Giulio Cesare
(100-44 a.C.)

Leon Battista Alberti
(1404-1472)

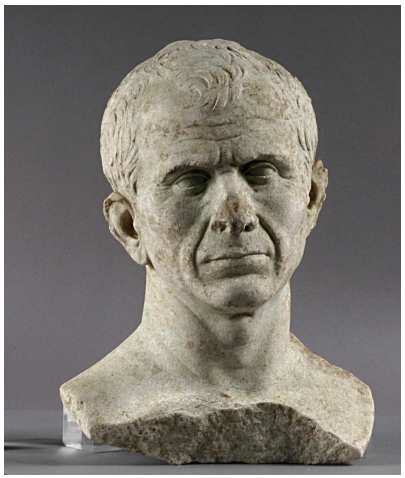
Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

Crittografia

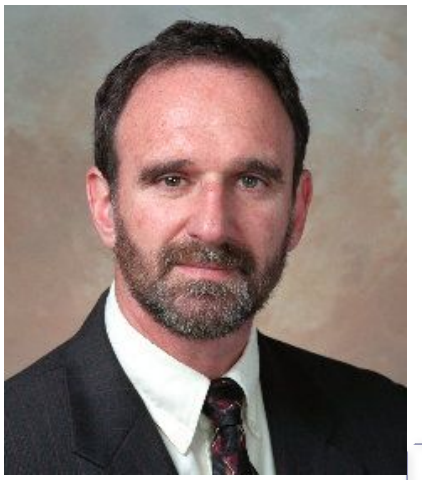
- κρυπτός nascosto — γράφω scrivere
- Cryptography is about communication in the presence of adversaries
  Ron Rivest
- La crittografia serve per:
  - Celare il significato del messaggio
  - Garantire l'autenticità del messaggio
  - Identificare l'autore del messaggio
  - Firmare e datare il messaggio



Caio Giulio Cesare
(100-44 a.C.)

Leon Battista Alberti
(1404-1472)

Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

Arnold, 2000 Tutta la matematica si divide in tre parti: crittografia (pagata da CIA, KGB e simili), idrodinamica (sostenuta dai fabbricanti di sottomarini nucleari) e meccanica celeste (finanziata dai militari e da altri istituti che hanno a che fare coi missili, come la NASA)

Влади́мир И́горевич Арно́льд
Vladimir Ìgorevič Arnol'd (1937-2010)

Arnold, 2000 Tutta la matematica si divide in tre parti: crittografia (pagata da CIA, KGB e simili), idrodinamica (sostenuta dai fabbricanti di sottomarini nucleari) e meccanica celeste (finanziata dai militari e da altri istituti che hanno a che fare coi missili, come la NASA)

- La crittografia ha generato la teoria dei numeri, la geometria algebrica su campi finiti, l'algebra, il calcolo combinatorio e i computer

Влади́мир И́горевич Арно́льд
Vladimir Ìgorevič Arnol'd (1937-2010)

Arnold, 2000 Tutta la matematica si divide in tre parti: crittografia (pagata da CIA, KGB e simili), idrodinamica (sostenuta dai fabbricanti di sottomarini nucleari) e meccanica celeste (finanziata dai militari e da altri istituti che hanno a che fare coi missili, come la NASA)

- La crittografia ha generato la teoria dei numeri, la geometria algebrica su campi finiti, l'algebra, il calcolo combinatorio e i computer
- L'idrodinamica procreò l'analisi complessa, le equazioni alle derivate parziali, i gruppi di Lie, l'algebra, la coomologia e il calcolo scientifico

Влади́мир И́горевич Арно́льд
Vladimir Ìgorevič Arnol'd (1937-2010)

Arnold, 2000 Tutta la matematica si divide in tre parti: crittografia (pagata da CIA, KGB e simili), idrodinamica (sostenuta dai fabbricanti di sottomarini nucleari) e meccanica celeste (finanziata dai militari e da altri istituti che hanno a che fare coi missili, come la NASA)

- La crittografia ha generato la teoria dei numeri, la geometria algebrica su campi finiti, l'algebra, il calcolo combinatorio e i computer
- L'idrodinamica procreò l'analisi complessa, le equazioni alle derivate parziali, i gruppi di Lie, l'algebra, la coomologia e il calcolo scientifico
- La meccanica celeste è all'origine dei sistemi dinamici, dell'algebra lineare, della topologia, del calcolo delle variazioni e della geometria simplettica

Влади́мир И́горевич Арно́льд
Vladimir Ìgorevič Arnol'd (1937-2010)

Atabash

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Atabash

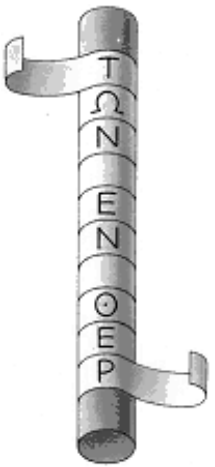
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Esempio: בבל (BaBeL = Babilonia) diventa ששכ ($S^heS^haC^h$)

> *a tutti i re del settentrione, vicini e lontani, agli uni e agli altri e a tutti i regni che sono sulla terra; il re di Sesach berrà dopo di essi.*
> *Geremia 25:26* (VII *sec. a.C.*)

Scitala lacedemone

Pausania [...] laggiù, secondo le voci che ne trapelavano a Sparta, intratteneva relazioni poco chiare con la Persia: era evidente che il suo soggiorno era dovuto a scopi politici nient'affatto onesti. Gli efori decisero di far cessare lo scandalo: inviarono un araldo a consegnargli la scitala e a ingiungergli di seguirlo. *Tucidide, Storie* I.129 *(*V *sec. a.C.)*



Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

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

Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

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

Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

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

Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

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

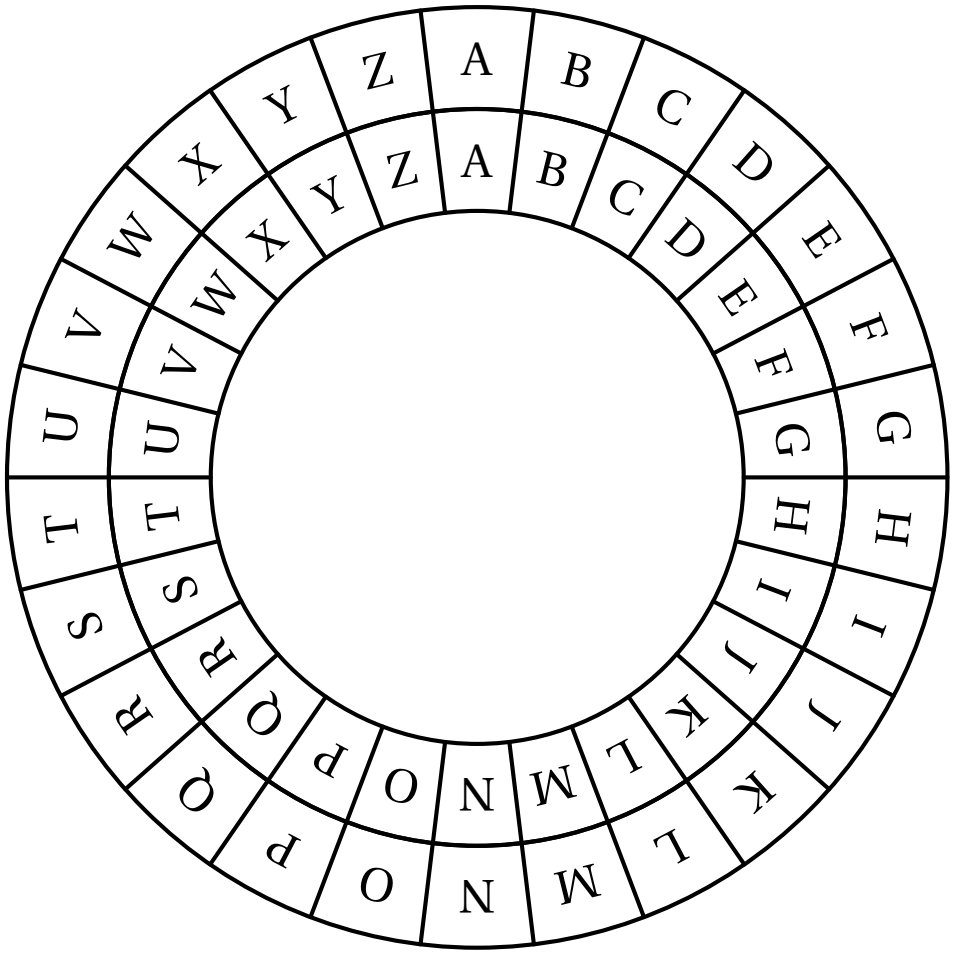
Cesare

Ci sono anche [lettere] a Cicerone [...] in cui [Cesare], dovendo discutere di argomenti confidenziali, scriveva in cifra, cioè cambiando l'ordine di ciascuna lettera in modo che nessuna parola ne risultasse; e se qualcuno le volesse decifrare e trascrivere, dovrebbe sostituire la quarta lettera dell'alfabeto, cioè la D, con la A e così con le altre.
Svetonio, Vita di Giulio Cesare, 56

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

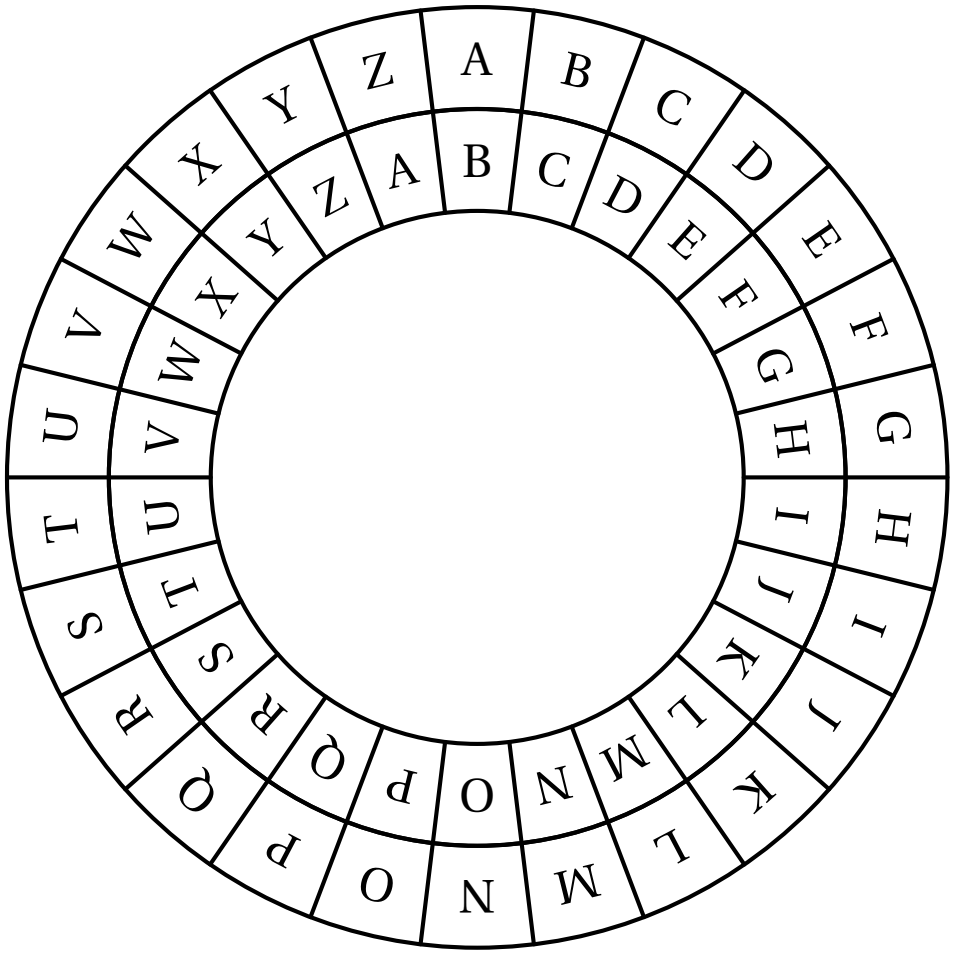
Esempio: AVE diventa DZH.

Leon Battista Alberti (1404–1472)



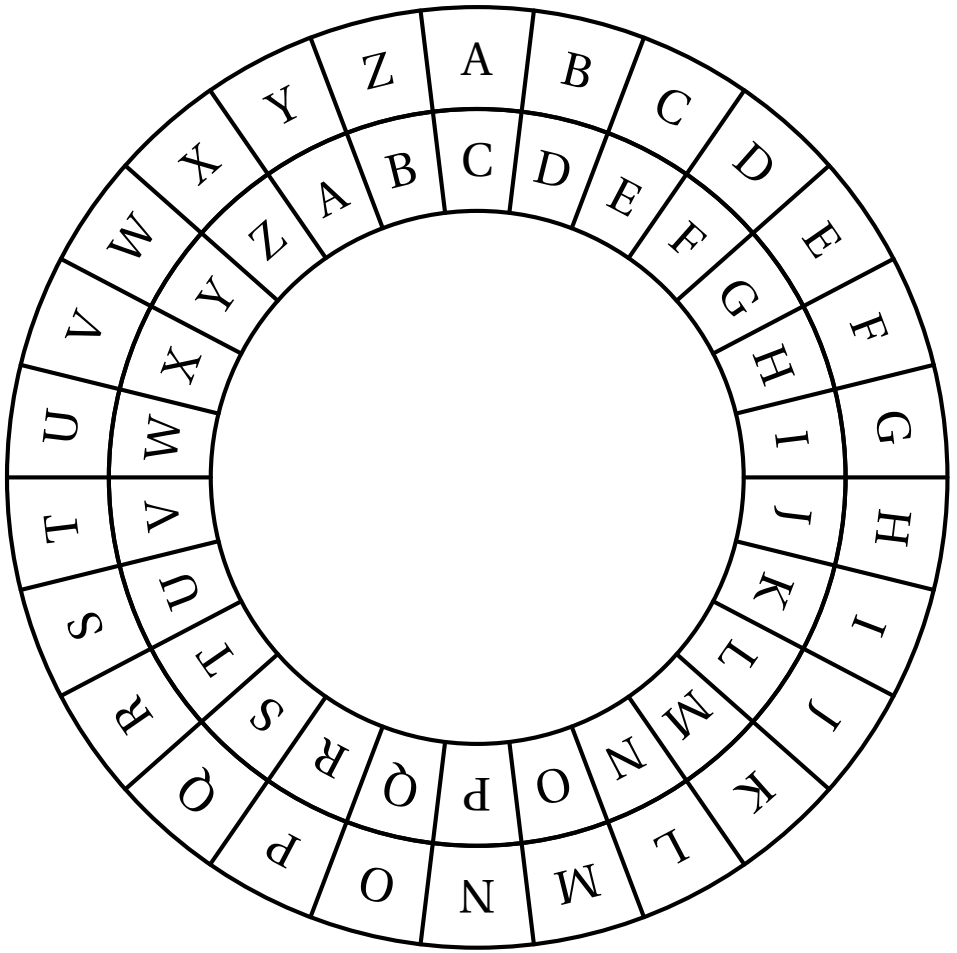
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



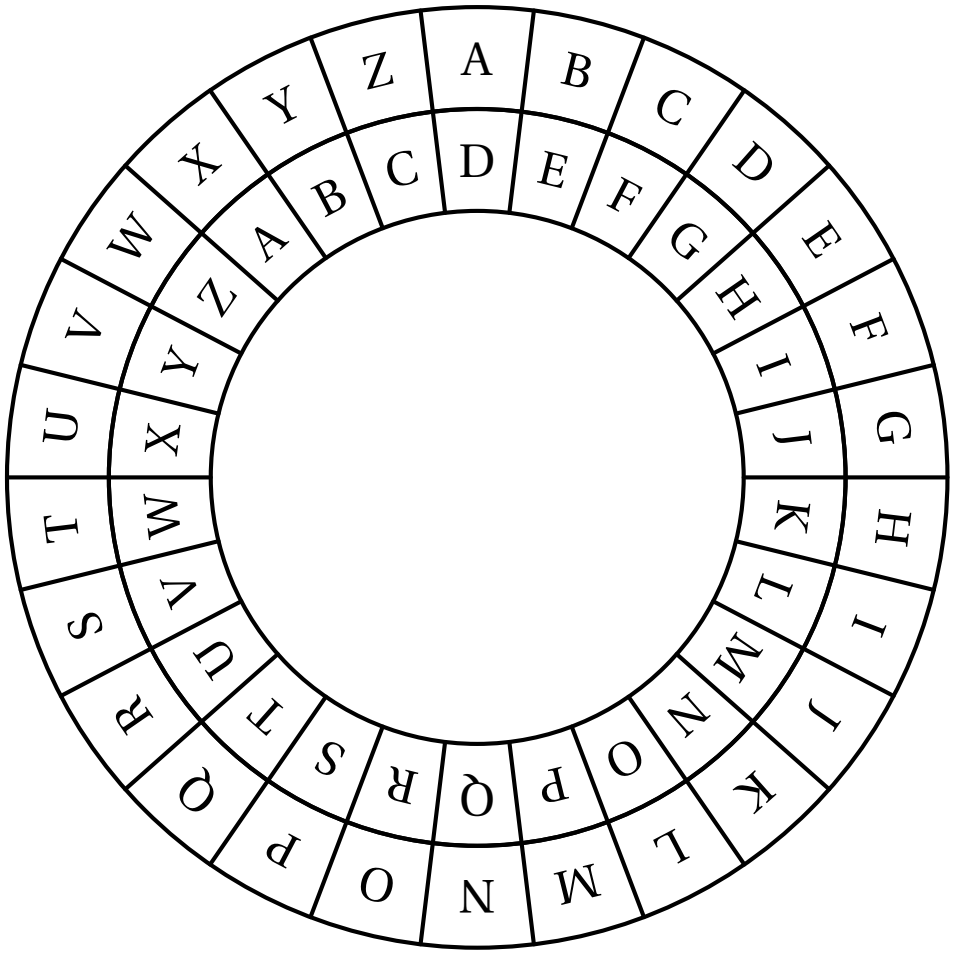
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



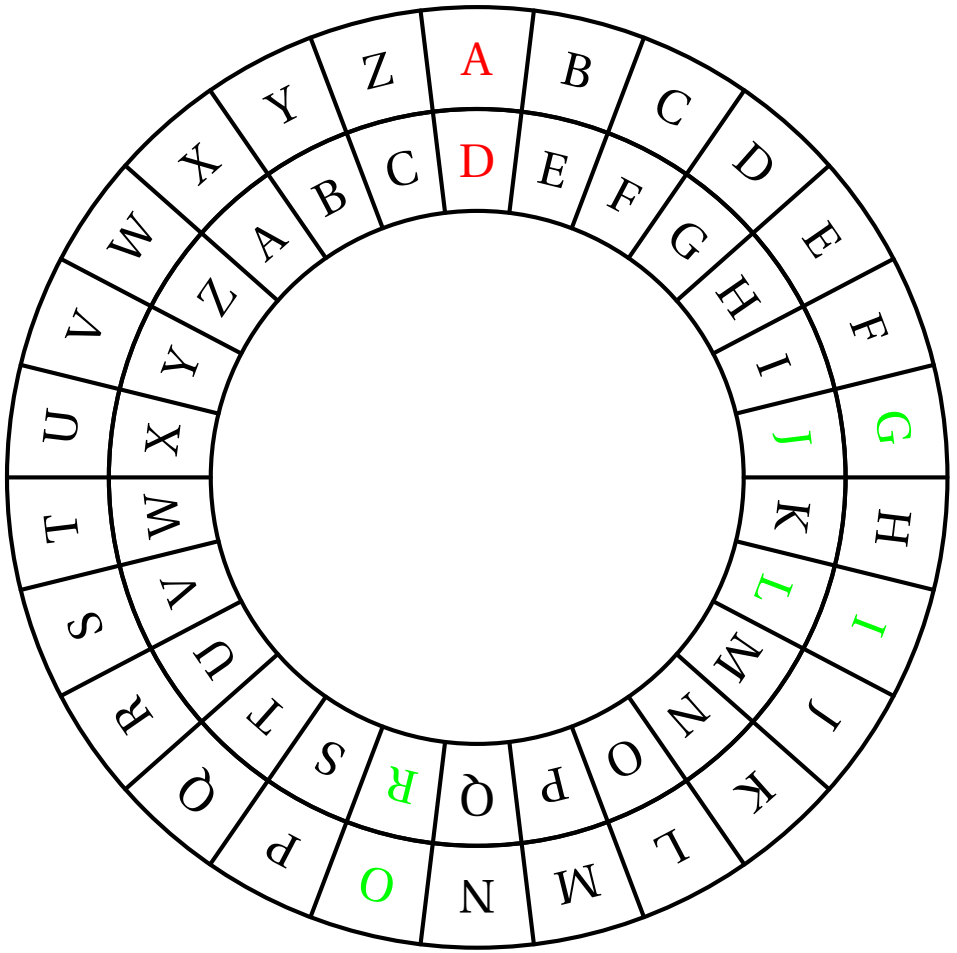
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



Disco cifrante: varianti di Cesare

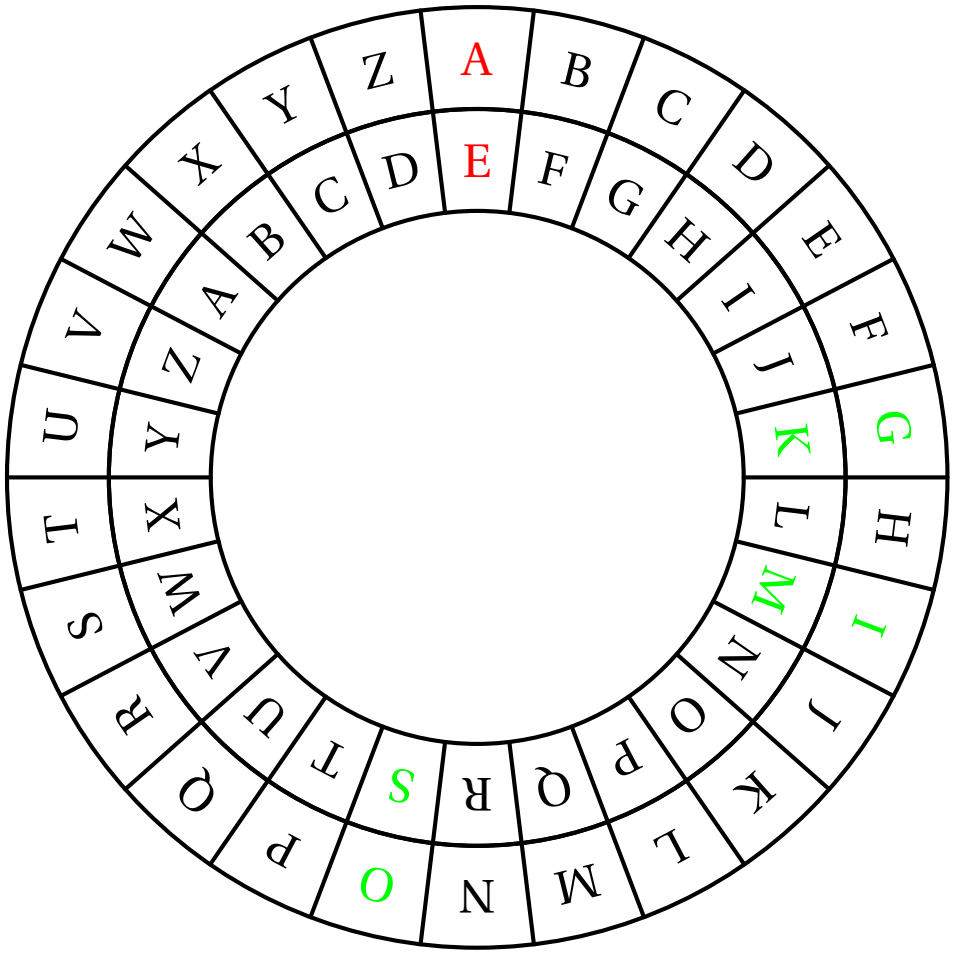
Leon Battista Alberti (1404–1472)



- Chiave D: OGGI → RJJL

Disco cifrante: varianti di Cesare

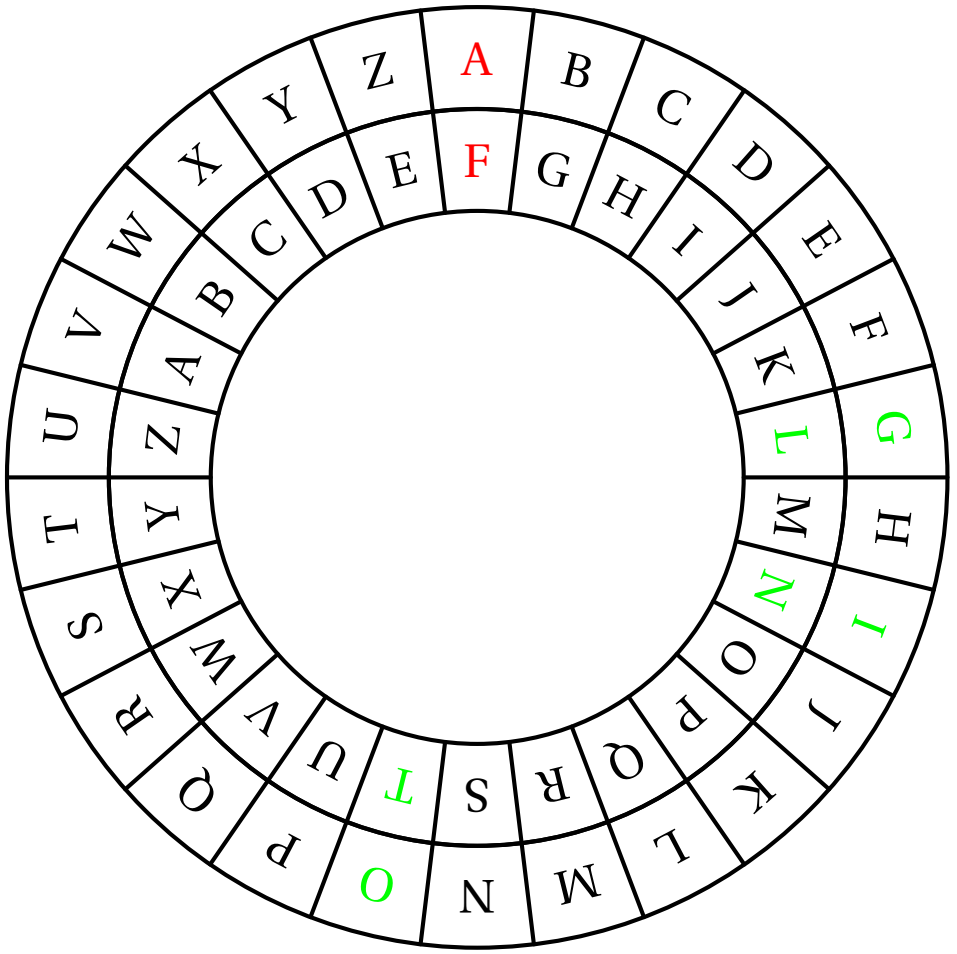
Leon Battista Alberti (1404–1472)



- Chiave D: OGGI → RJJL
- Chiave E: OGGI → SKKM

Disco cifrante: varianti di Cesare

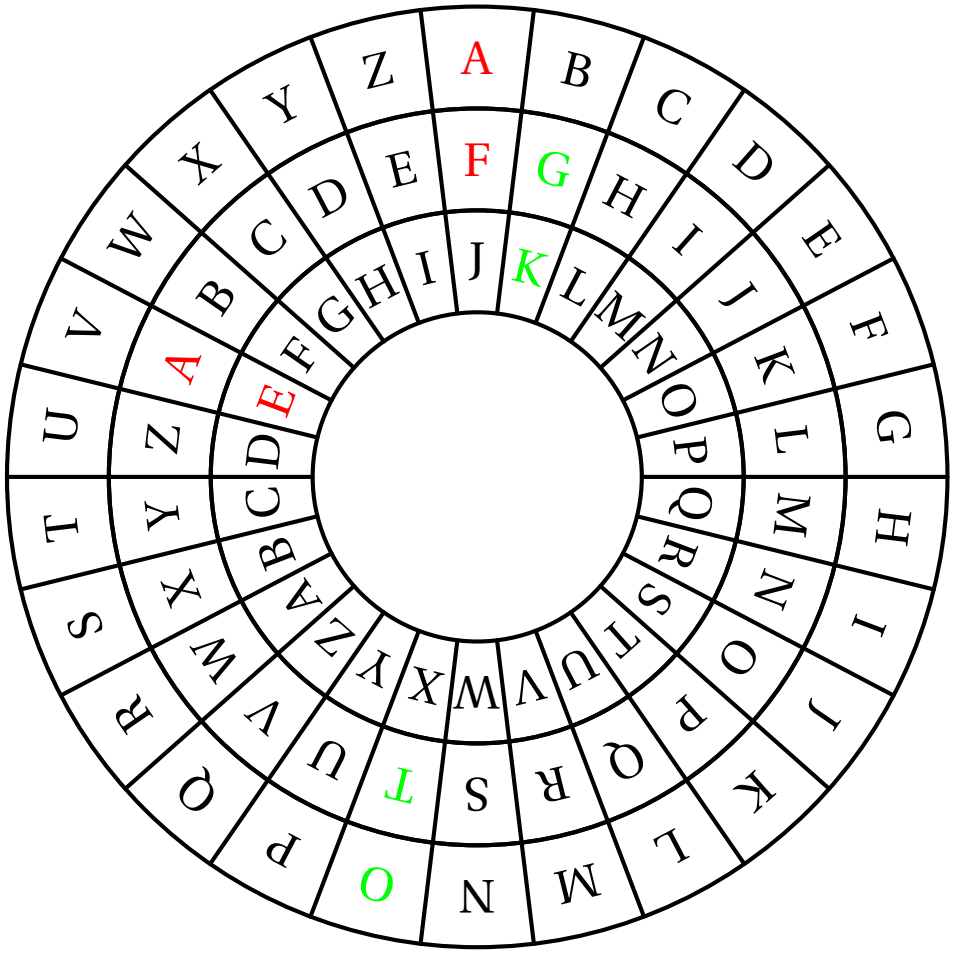
Leon Battista Alberti (1404–1472)



- Chiave D: OGGI → RJJL
- Chiave E: OGGI → SKKM
- Chiave F: OGGI → TLLN

Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)

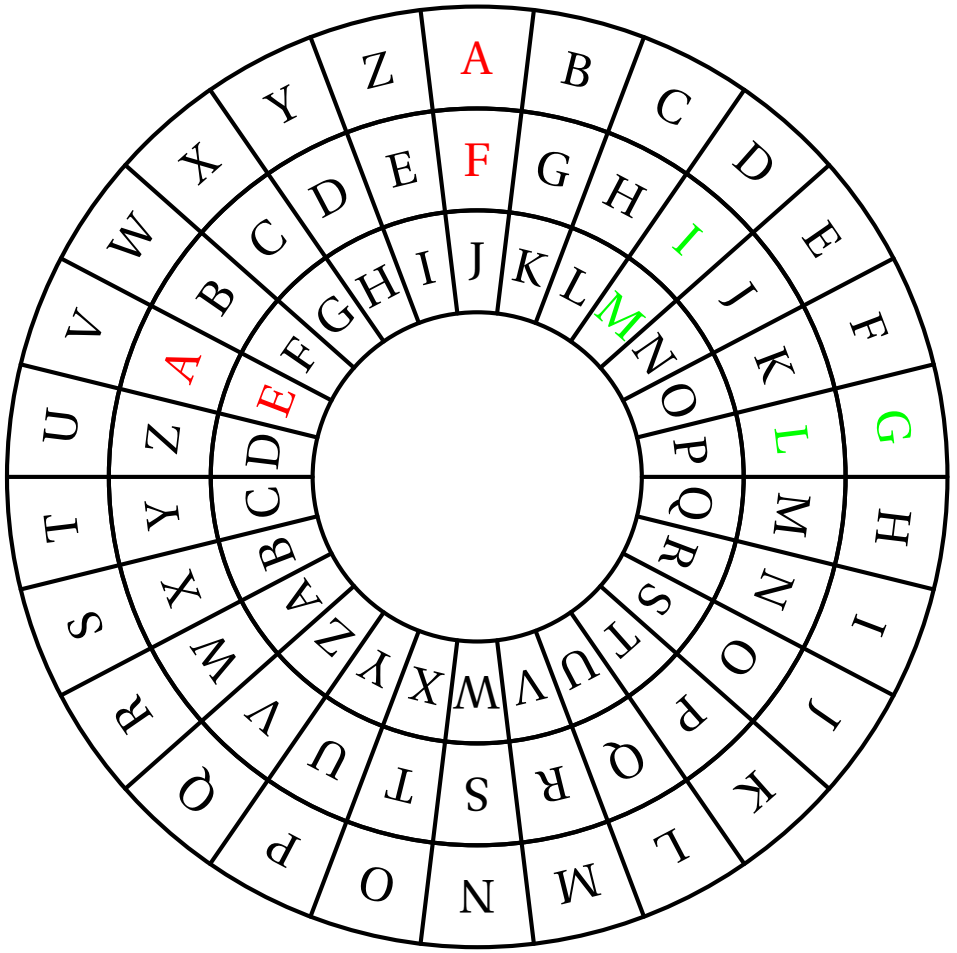


- Chiave D: OGGI → RJJL
- Chiave E: OGGI → SKKM
- Chiave F: OGGI → TLLN

- Chiave FE: OG → TK

Disco cifrante: cifrario poliafabetico

Leon Battista Alberti (1404–1472)



Disco cifrante: cifrario poliafabetico

- Chiave D: OGGI → RJJL
- Chiave E: OGGI → SKKM
- Chiave F: OGGI → TLLN

- Chiave FE: OG → TK
- GI → LM
- OGGI → TKLM

Crittoanalisi

L'avversario vuole negare gli scopi della crittografia

- Celare il significato del messaggio $\Longrightarrow$ leggere il messaggio
- Garantire l'autenticità del messaggio $\Longrightarrow$ modificare il messaggio
- Identificare l'autore del messaggio $\Longrightarrow$ impersonare
- Firmare e datare il messaggio $\Longrightarrow$ ripudiare

Crittoanalisi

L'avversario vuole negare gli scopi della crittografia

- Celare il significato del messaggio $\Longrightarrow$ leggere il messaggio
- Garantire l'autenticità del messaggio $\Longrightarrow$ modificare il messaggio
- Identificare l'autore del messaggio $\Longrightarrow$ impersonare
- Firmare e datare il messaggio $\Longrightarrow$ ripudiare

Auguste Kerkhoffs (1835-1903)

Principio di Kerkhoffs Un sistema deve essere sicuro anche se l'intero sistema, eccetto la chiave, è pubblico

Crittoanalisi

L'avversario vuole negare gli scopi della crittografia

- Celare il significato del messaggio $\Longrightarrow$ leggere il messaggio
- Garantire l'autenticità del messaggio $\Longrightarrow$ modificare il messaggio
- Identificare l'autore del messaggio $\Longrightarrow$ impersonare
- Firmare e datare il messaggio $\Longrightarrow$ ripudiare

Auguste Kerkhoffs (1835-1903)

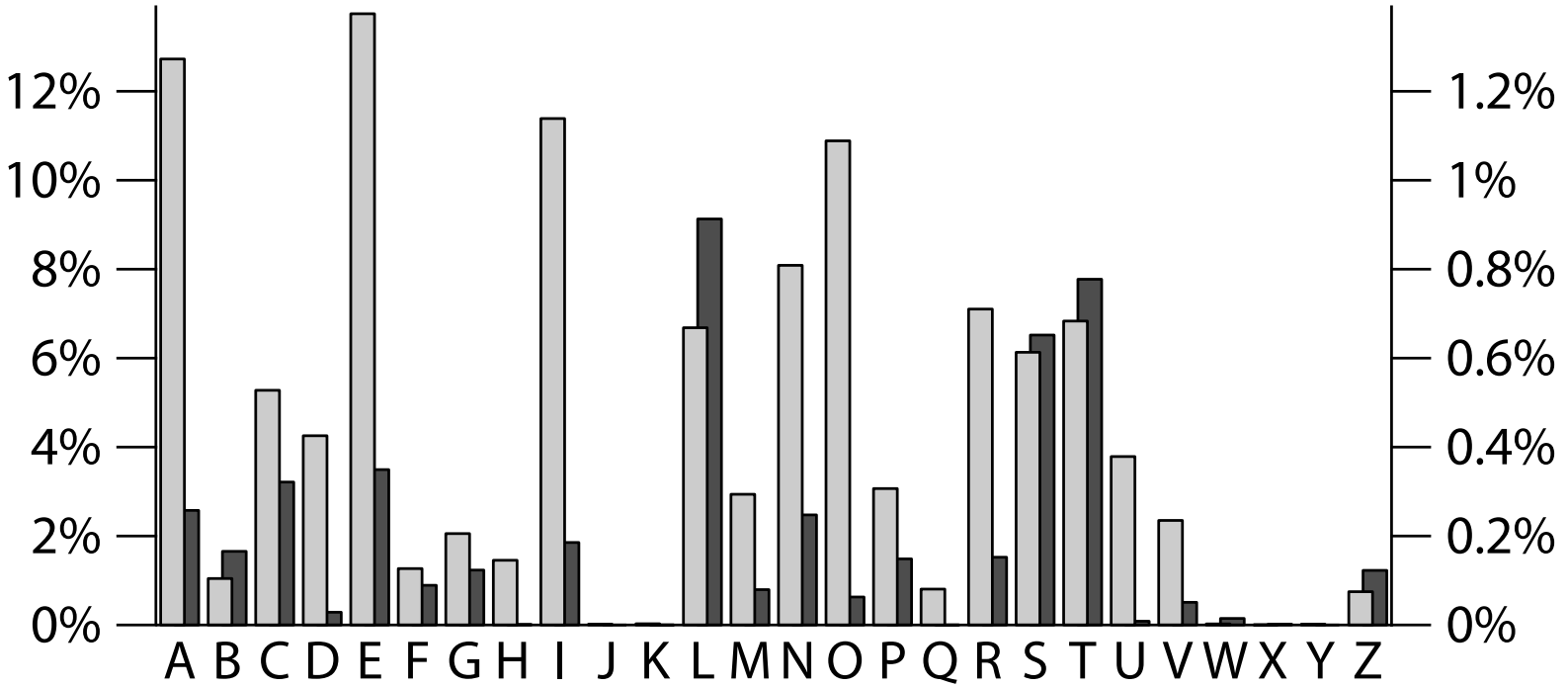
Principio di Kerkhoffs Un sistema deve essere sicuro anche se l'intero sistema, eccetto la chiave, è pubblico

Massima di Shannon Il nemico conosce il sistema

Proverbio Sicurezza tramite segretezza non dà nessuna sicurezza

Analisi delle frequenze

- Le lingue naturali hanno molte ridondanze
- Sfruttiamole per riconoscere il testo
- Permette di attaccare facilmente gli algoritmi classici

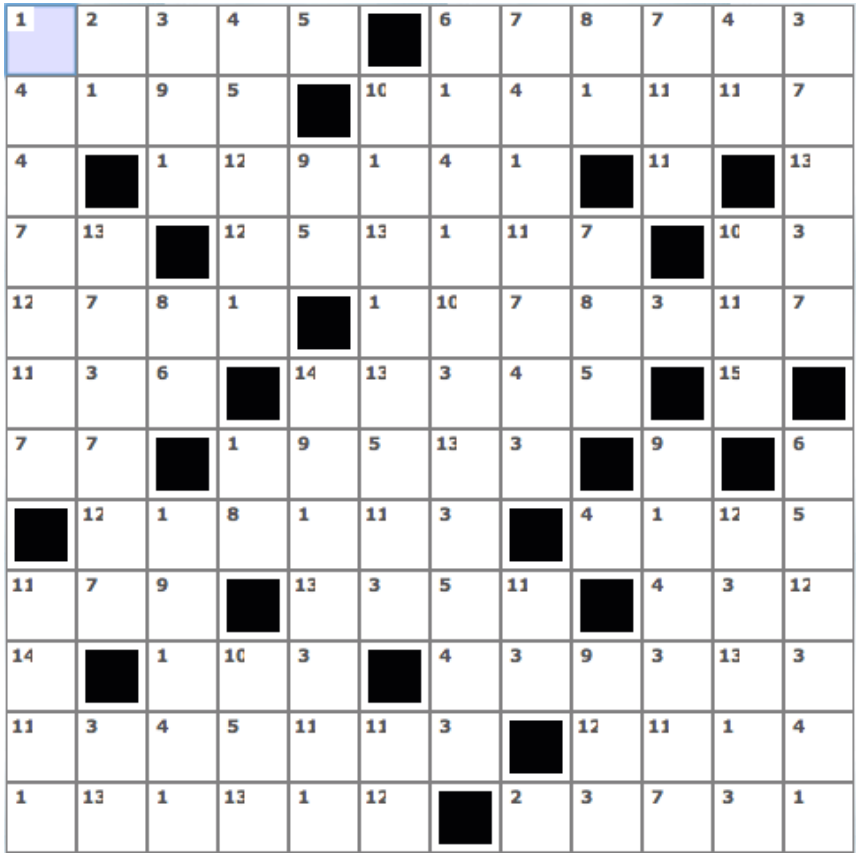


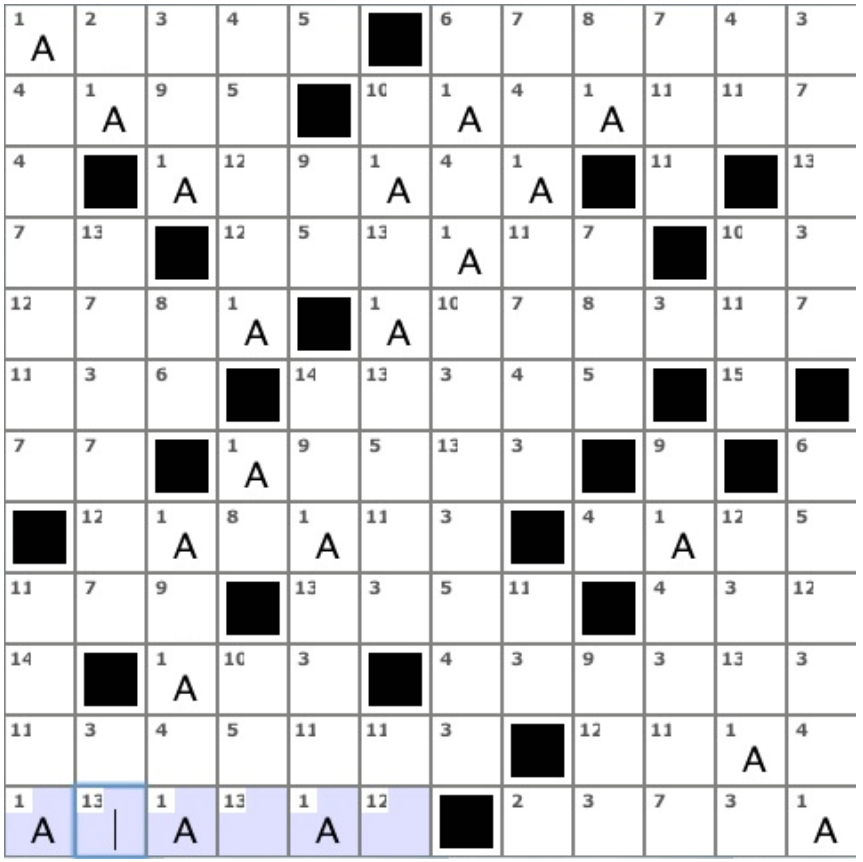
Frequenza delle lettere in italiano, in chiaro a sinistra e, a destra, delle doppie

Sostituzione

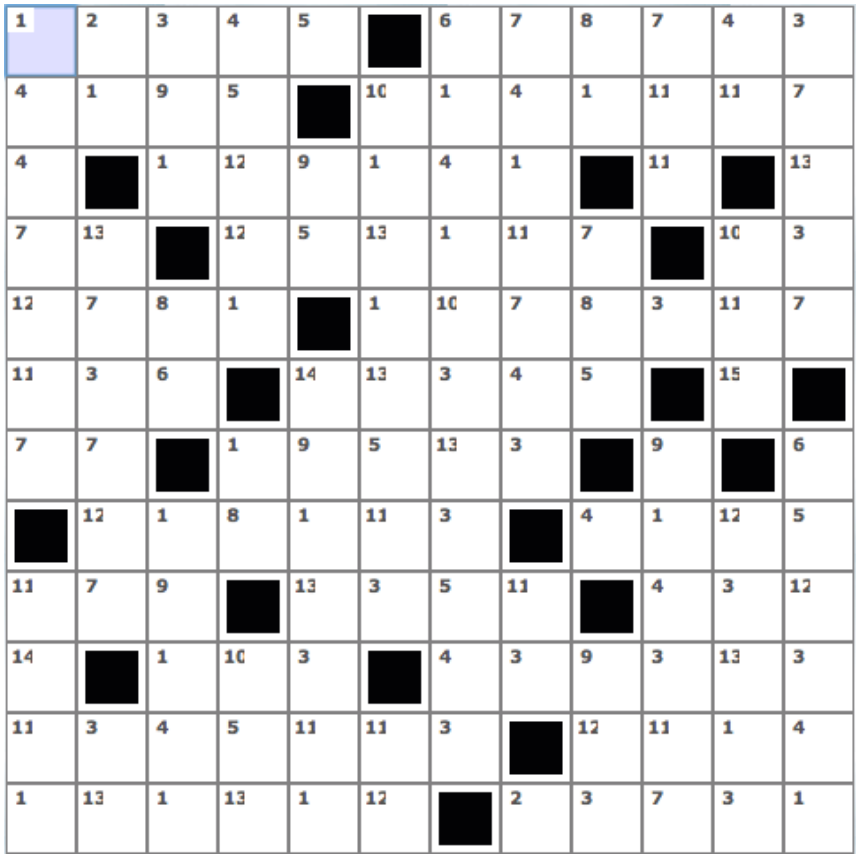
1	2	3	4	5	■	6	7	8	7	4	3
4	1	9	5	■	10	1	4	1	11	11	7
4	■	1	12	9	1	4	1	■	11	■	13
7	13	■	12	5	13	1	11	7	■	10	3
12	7	8	1	■	1	10	7	8	3	11	7
11	3	6	■	14	13	3	4	5	■	15	■
7	7	■	1	9	5	13	3	■	9	■	6
■	12	1	8	1	11	3	■	4	1	12	5
11	7	9	■	13	3	5	11	■	4	3	12
14	■	1	10	3	■	4	3	9	3	13	3
11	3	4	5	11	11	3	■	12	11	1	4
1	13	1	13	1	12	■	2	3	7	3	1

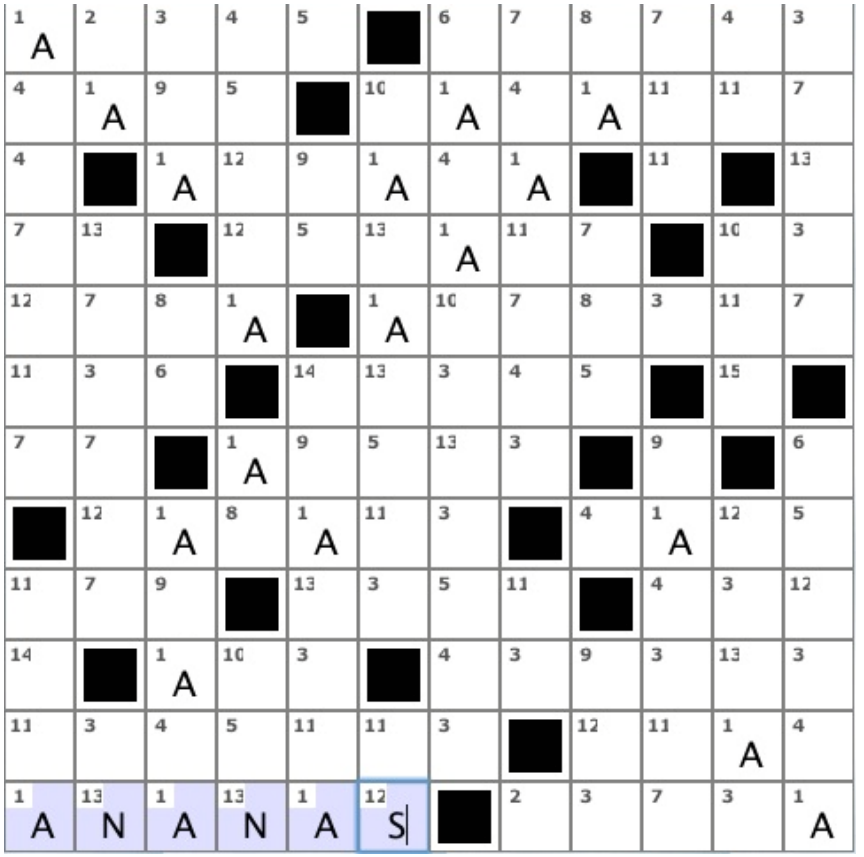
Sostituzione



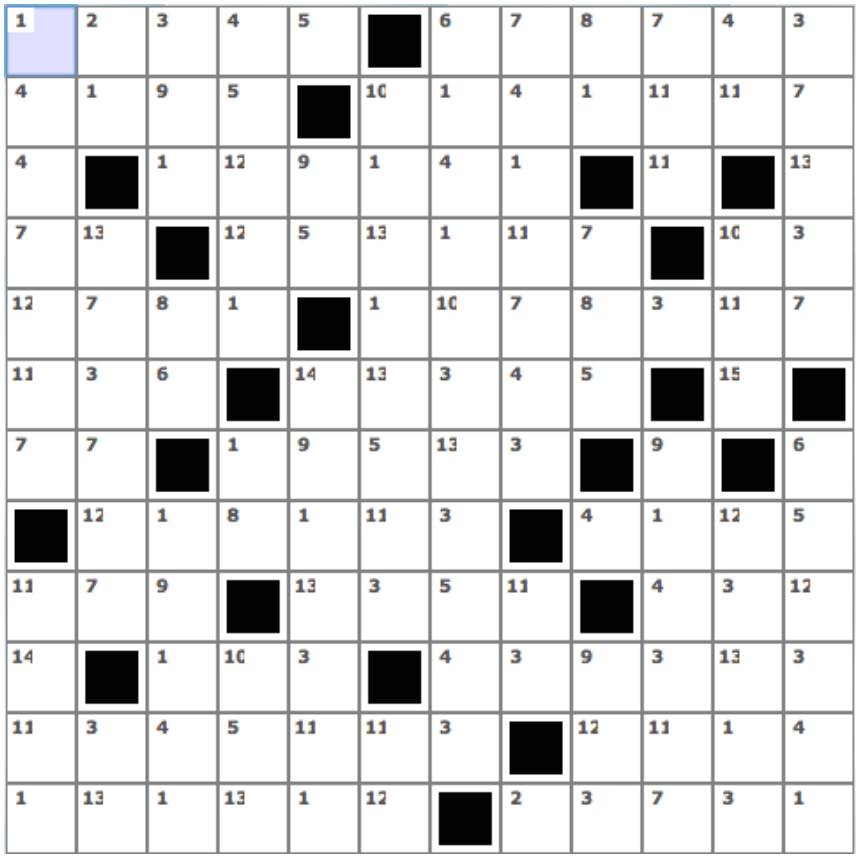


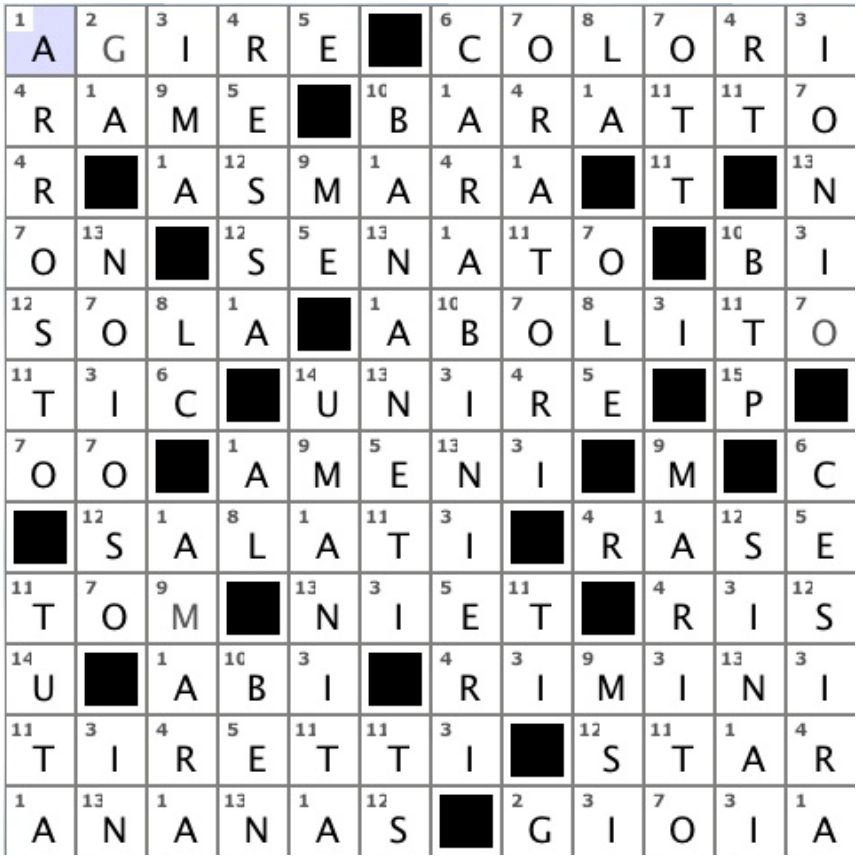
Sostituzione





Sostituzione





Attaccare Cesare

MPPUAYAZFUEADSQZFUPMXXMOCGQQPQXQHMFUMXOUQXAOUYQUZGSGMXUZAFQMOTUODQ
EOUGFAFDMHAUQUYBDQEEQZQXXMEGMYQZFQZAZYQZAOTQXAEUMXMEBQFFAPQEGAUBUR
MYUXUMDUFADDQZFUPQCGMXUPUEFUZSGQXAEODAEOUAOAYQUXEGAZAPQXXQHAOUPAYQ
EFUOTQHUXXQEBMDEQQNUMZOTQSSUMZFUEGXBQZPAOAYQNDMZOTUPUBQOADQBMEOQZF
UMPPUACGMZFAFDUEFAUXBMEEAPUOTUODQEOUGFAFDMHAUEQZQMXXAZFMZMMXXMRMZF
MEUMPUCGQXXAEFQEEAOTQEQZQBMDFQHAXAZFMDUMYQZFQFDMFFAPMXXMEBQDMZLMPU
RMDQMXFDAHQRADFGZMEUPUEMNNQXXUEOAZAUZCGQXYAYQZFAUEASZUPQXXMDUOOTQL
LMQSXUEUYMDMHUSXUMPQEEQDEUBAFGFADUEAXHQDQQFADZQDQNNQMXXADMUZPUQFDA
EQZAZBQZEMEEQOTQGZSUADZAFADZQDPAHULUAEACGMZFABUEUMHMZLMZQXBUMZAUXE
GAAOOTUAEUDUFUDMPUESGEFMFAQEFMZOAPMCGQXXMYBUQLLMGZURADYQXMDUMSXUBM
DSDMHAEMQYADFMEUZAXFDMYQEFAQPUEMFFQZFAZQXXQOUFFFGYGXFGAEQXQOMEQMSS
UGZFQMOMEQXQEFDMPQOTQENAOOMZAZQXXQEFDMPQBMDQOTQSXUXQHUZAUXDQEBUDAQ
PMHMZFUMSXUQPURULUMYYUDMFUPMXXAEFDMZUQDABQZEMOAZPQEUPQDUAUZCGUQFAM
XOMYBUOQXXAPQXEGABMQEQMXXMOMEGOOUMMOGUTMSUYQEEASXUAOOTUMPP
AEEAPMSDMZFQYBAQOTQOAYBDQDFADZMZPADUOOAMEGAUYAZFU

Attacco per forza bruta

Proviamo tutte le chiavi

Attacco per forza bruta

Proviamo tutte le chiavi

Cesare Per decifrare RJJL proviamo tutte le 26 chiavi

SKKM	TLLN	UMMO	VNNP	WOOQ
XPPR	YQQS	ZRRT	ASSU	BTTV
CUUW	DVVX	EWWY	FXXZ	GYYA
HZZB	IAAC	JBBD	KCCE	LDDF
MEEG	NFFH	OGGI	PHHJ	QIIK

Attacco per forza bruta

Proviamo tutte le chiavi

Cesare Per decifrare RJJL proviamo tutte le 26 chiavi

SKKM	TLLN	UMMO	VNNP	WOOQ
XPPR	YQQS	ZRRT	ASSU	BTTV
CUUW	DVVX	EWWY	FXXZ	GYYA
HZZB	IAAC	JBBD	KCCE	LDDF
MEEG	NFFH	OGGI	PHHJ	QIIK

Attacco per forza bruta

Proviamo tutte le chiavi

Cesare Per decifrare RJJL proviamo tutte le 26 chiavi

SKKM	TLLN	UMMO	VNNP	WOOQ
XPPR	YQQS	ZRRT	ASSU	BTTV
CUUW	DVVX	EWWY	FXXZ	GYYA
HZZB	IAAC	JBBD	KCCE	LDDF
MEEG	NFFH	OGGI	PHHJ	QIIK

Esercizio

Decifriamo ZMXYH

Ricadute didattiche

Aritmetica modulare

- Perché decifrare con Cesare e chiave E è equivalente a cifrare con chiave W?

Ricadute didattiche

Aritmetica modulare

- Perché decifrare con Cesare e chiave E è equivalente a cifrare con chiave W?
- Struttura di anello delle classi di resto modulo n?

Ricadute didattiche

Aritmetica modulare

- Perché decifrare con Cesare e chiave E è equivalente a cifrare con chiave W?
- Struttura di anello delle classi di resto modulo n?
- Matematica non convenzionale

Ricadute didattiche

Aritmetica modulare

- Perché decifrare con Cesare e chiave E è equivalente a cifrare con chiave W?
- Struttura di anello delle classi di resto modulo n?
- Matematica non convenzionale

Combinatoria

- Numero delle chiavi
- Difficoltà degli attacchi

Componenti primitive

Possiamo interpretare gli algoritmi classici come

Sostituzione $\mathrm{O} \longleftrightarrow \mathrm{X}$, $\mathrm{G} \longleftrightarrow \mathrm{J}$, $\mathrm{I} \longleftrightarrow \mathrm{A}$, $\ldots$:

$$\mathrm{OGGI} \Longrightarrow \mathrm{XJJA}$$

Componenti primitive

Possiamo interpretare gli algoritmi classici come

Sostituzione $\mathrm{O} \longleftrightarrow \mathrm{X}$, $\mathrm{G} \longleftrightarrow \mathrm{J}$, $\mathrm{I} \longleftrightarrow \mathrm{A}$, $\ldots$:

$$\mathrm{OGGI} \Longrightarrow \mathrm{XJJA}$$

Trasposizione $(1, 4, 3)$:

$$\mathrm{XJJA} \Longrightarrow \mathrm{JJAX}$$

Componenti primitive

Possiamo interpretare gli algoritmi classici come

Sostituzione $O \longleftrightarrow X$, $G \longleftrightarrow J$, $I \longleftrightarrow A$, $\ldots$:

$$OGGI \Longrightarrow XJJA$$

Trasposizione $(1,4,3)$:

$$XJJA \Longrightarrow JJAX$$

Somma della chiave $AA \mapsto FE$:

$$JJAX \Longrightarrow ONFB$$

Componenti primitive

Possiamo interpretare gli algoritmi classici come

Sostituzione $\mathrm{O} \longleftrightarrow \mathrm{X}$, $\mathrm{G} \longleftrightarrow \mathrm{J}$, $\mathrm{I} \longleftrightarrow \mathrm{A}$, $\ldots$:

$$\mathrm{OGGI} \Longrightarrow \mathrm{XJJA}$$

Trasposizione $(1, 4, 3)$:

$$\mathrm{XJJA} \Longrightarrow \mathrm{JJAX}$$

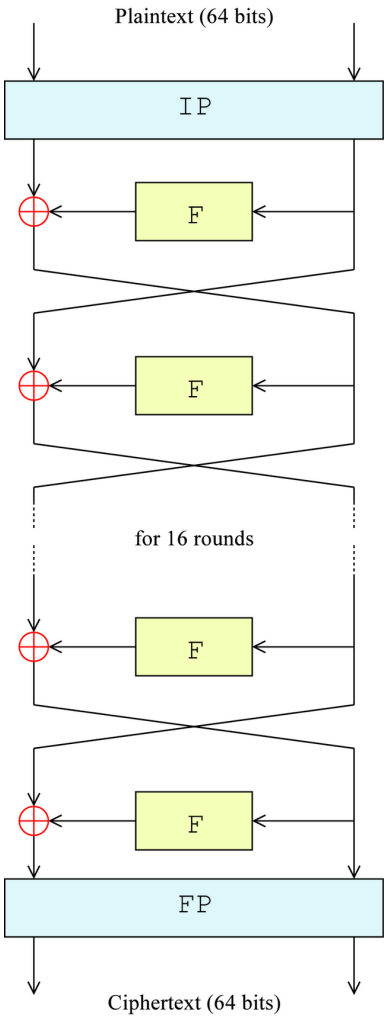
Somma della chiave $\mathrm{AA} \mapsto \mathrm{FE}$:

$$\mathrm{JJAX} \Longrightarrow \mathrm{ONFB}$$

La crittografia moderna è una combinazione, ripetuta più e più volte, di

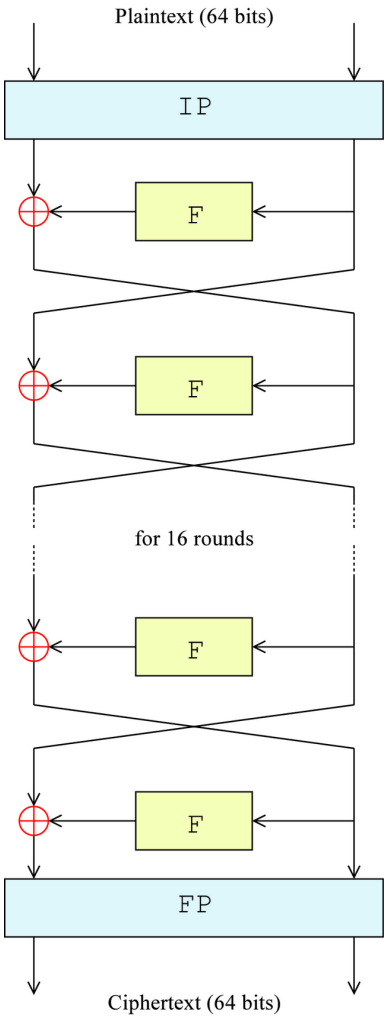
- sostituzione = confusione
- trasposizione = diffusione
- somma della chiave

DES



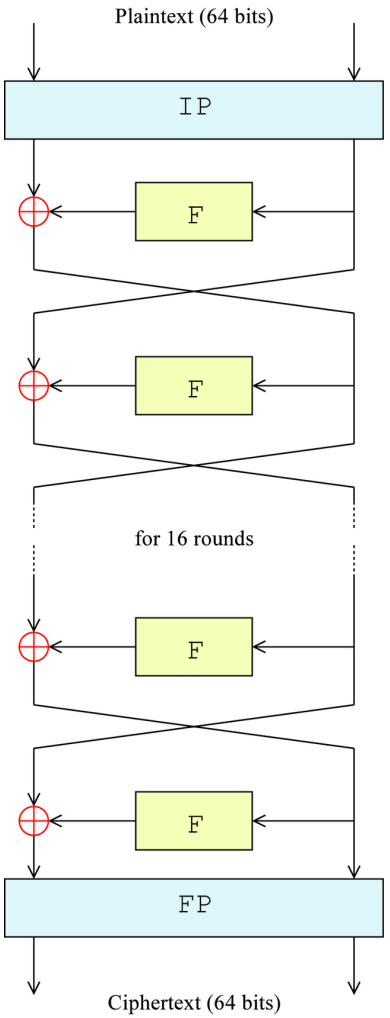
- Data Encryption Standard, 1976

DES



- Data Encryption Standard, 1976
- Combinazione elettronica delle tecniche precedenti ripetute 16 volte

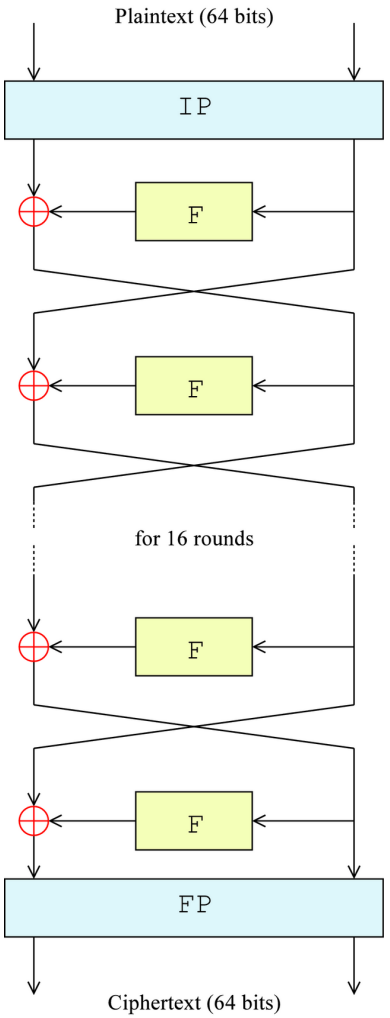
DES



- Data Encryption Standard, 1976
- Combinazione elettronica delle tecniche precedenti ripetute 16 volte
- Facilmente attaccabile: solo 2^{56} chiavi

anno	costo	tempo
1977	15 000 000 €	1 giorno
1997	200 000 €	2 giorni
1997	gratis	96 giorni
2002	800€	23 giorni
2006	50 000 €	20 ore

DES



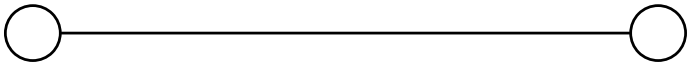
- Data Encryption Standard, 1976
- Combinazione elettronica delle tecniche precedenti ripetute 16 volte
- Facilmente attaccabile: solo 2^{56} chiavi

anno	costo	tempo
1977	15 000 000 €	1 giorno
1997	200 000 €	2 giorni
1997	gratis	96 giorni
2002	800€	23 giorni
2006	50 000 €	20 ore

- Le sostituzioni sono tali da rendere DES resistente ad un attacco scoperto 10 anni dopo!

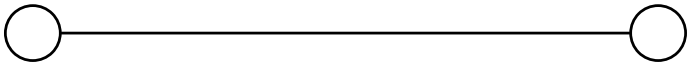
Il problema delle chiavi

- Per ogni coppia che comunica: una chiave

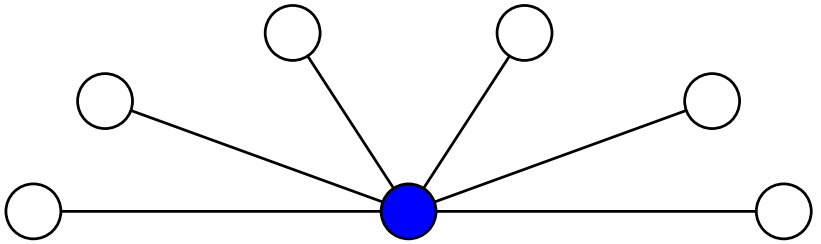


Il problema delle chiavi

- Per ogni coppia che comunica: una chiave

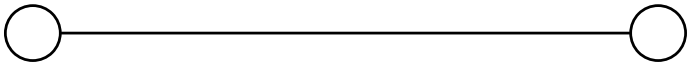


- n parti che comunicano con un sito centrale: n chiavi

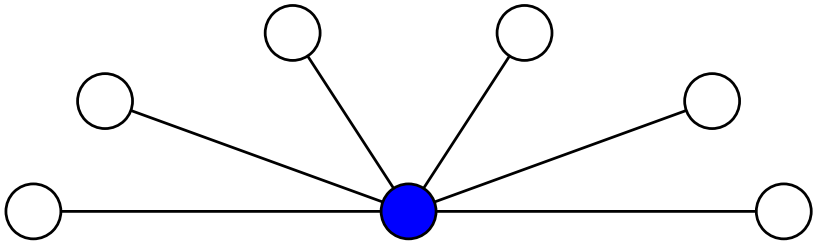


Il problema delle chiavi

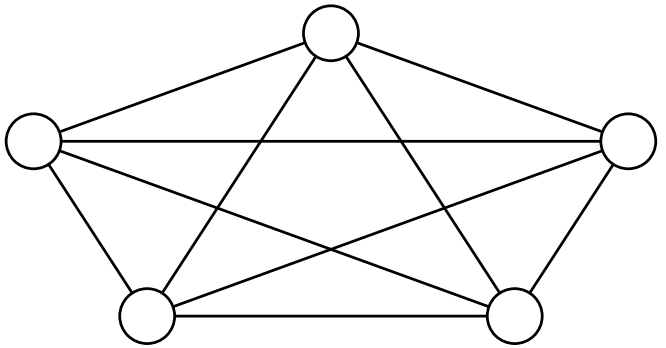
- Per ogni coppia che comunica: una chiave



- n parti che comunicano con un sito centrale: n chiavi



- n parti che comunicano fra di loro: $\frac{n(n-1)}{2}$ chiavi



Scambiare chiavi in pubblico

- Io non ho la donna

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B
  - Andrea e Barbara si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B
  - Andrea e Barbara si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$
  - Andrea e Barbara hanno condiviso il segreto $2^{n_A n_B}$

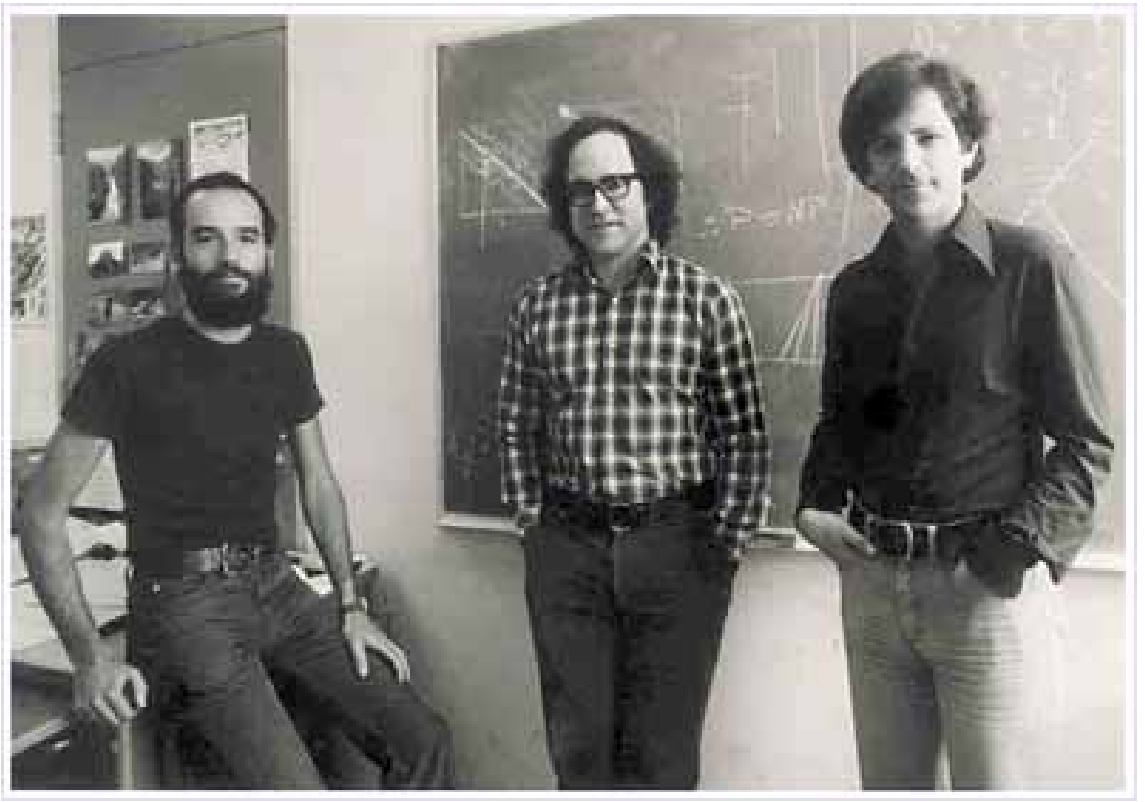
Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B
  - Andrea e Barbara si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$
  - Andrea e Barbara hanno condiviso il segreto $2^{n_A n_B}$
- Idea: noto $2^n \bmod p$ è praticamente impossibile calcolare n.

Scambiare chiavi in pubblico

- Io non ho la donna
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un primo interno p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B
  - Andrea e Barbara si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$
  - Andrea e Barbara hanno condiviso il segreto $2^{n_A n_B}$
- Idea: noto $2^n \bmod p$ è praticamente impossibile calcolare n.
- Laboratorio didattico in via di sviluppo

Ralph Merkle, Martin Hellman, Whit Diffie



Adi Shamir, Ronald Rivest, Leonard Adleman

RSA

- Fissato $n = pq$ con p e q primi grandi
- Sia $\phi(n) = (p-1)(q-1)$
- Sia e un intero scelto a caso e sia d tale che $ed \equiv 1 \bmod \phi(n)$

RSA

- Fissato $n = pq$ con p e q primi grandi
- Sia $\phi(n) = (p-1)(q-1)$
- Sia e un intero scelto a caso e sia d tale che $ed \equiv 1 \bmod \phi(n)$
- Allora possiamo cifrare un messaggio t come $c = t^e \bmod n$ e decifrare c come $t = c^d \bmod n$
- La coppia (n, e) è la chiave pubblica, la coppia (n, d) è la chiave privata

RSA

- Fissato $n = pq$ con p e q primi grandi
- Sia $\phi(n) = (p-1)(q-1)$
- Sia e un intero scelto a caso e sia d tale che $ed \equiv 1 \bmod \phi(n)$
- Allora possiamo cifrare un messaggio t come $c = t^e \bmod n$ e decifrare c come $t = c^d \bmod n$
- La coppia (n, e) è la chiave pubblica, la coppia (n, d) è la chiave privata

Problema

Didatticamente non funziona

- Richiede maturità matematica da eccellenza, e anche così...
- Applicare regole non comprese $\neq$ matematica

Kid Crypto

Lo sviluppo di protocolli crittografici comprensibili e attraenti (nonché discretamente sicuri) per studenti che non posseggono conoscenze matematiche a livello universitario. (Neal Koblitz)

Kid Crypto

Lo sviluppo di protocolli crittografici comprensibili e attraenti (nonché discretamente sicuri) per studenti che non posseggono conoscenze matematiche a livello universitario. (Neal Koblitz)

- Stabilire un valore totale senza rivelare i singoli valori

$$(s_0 + a_1) + a_2 + \cdots + a_n - s_0 = a_1 + a_2 + \cdots + a_n$$

Kid Crypto

Lo sviluppo di protocolli crittografici comprensibili e attraenti (nonché discretamente sicuri) per studenti che non posseggono conoscenze matematiche a livello universitario. (Neal Koblitz)

- Stabilire un valore totale senza rivelare i singoli valori

$$(s_0 + a_1) + a_2 + \cdots + a_n - s_0 = a_1 + a_2 + \cdots + a_n$$

- Kid-RSA
  - Andrea sceglie due interi a, b; pone $M = ab - 1$
  - Andrea sceglie due altri interi a', b'; pone

$$e = a'M + a, \quad d = b'M + b, \quad n = (ed - 1)/M = a'b'M + ab' + a'b + 1$$

  - La chiave pubblica di Andrea è (n, e), la chiave privata è (n, d)
  - Barbara cifra il messaggio t come $c = et \bmod n$
  - Andrea decifra il messaggio c con $t = dc \bmod n$

Analisi di Kid-RSA

- La dimostrazione della sua correttezza è al livello di scuola superiore
- Possiamo romperla facilmente se conosciamo l'algoritmo euclideo esteso

Analisi di Kid-RSA

- La dimostrazione della sua correttezza è al livello di scuola superiore
- Possiamo romperla facilmente se conosciamo l'algoritmo euclideo esteso
- Ricadute didattiche:
  - perché occorre dimostrare?
  - calcoli semplici ma non standard
  - fare matematica