Crittografia, logaritmi e sicurezza

Perché è difficile rompere la crittografia moderna?

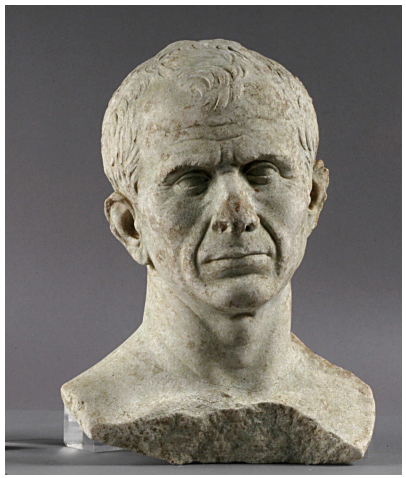
Ottavio Giulio Rizzo
Ottavio.Rizzo@UniMI.it

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

XXXV convegno UMI–CIIM
Cagliari, 4 ottobre 2018

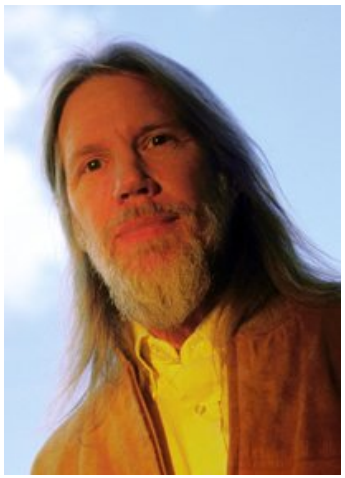
Crittografia

- κρυπτός nascosto — γράφω scrivere

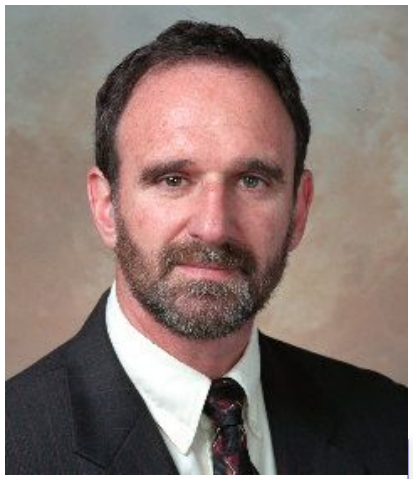


Caio Giulio Cesare
(100-44 a.C.)

Leon Battista Alberti
(1404-1472)



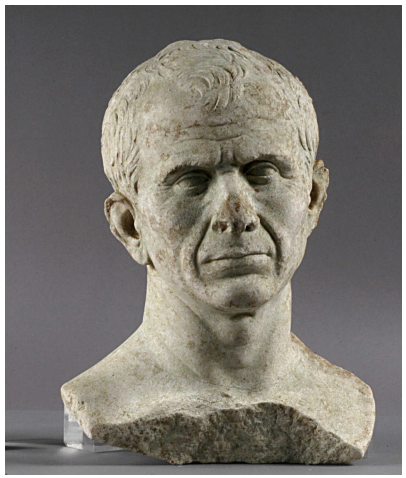
Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

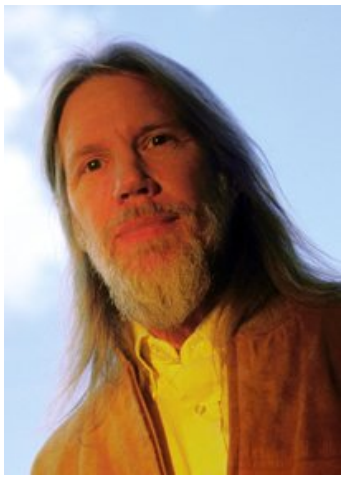
Crittografia

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

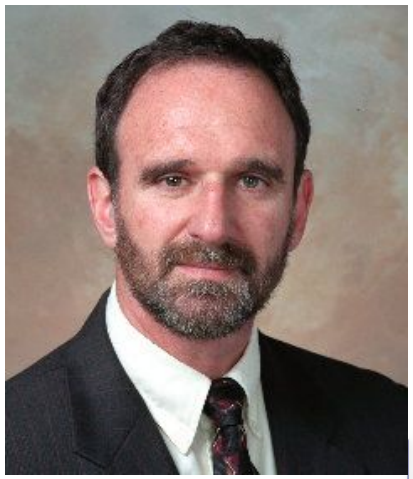


Caio Giulio Cesare
(100-44 a.C.)

Leon Battista Alberti
(1404-1472)



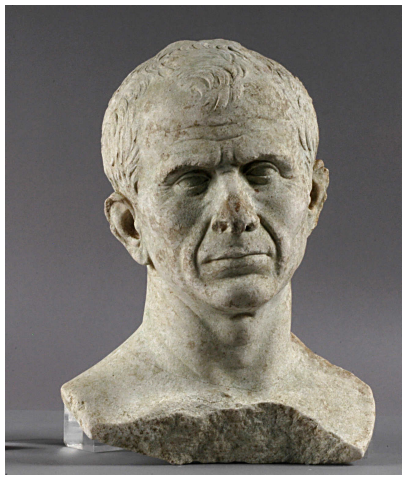
Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

Crittografia

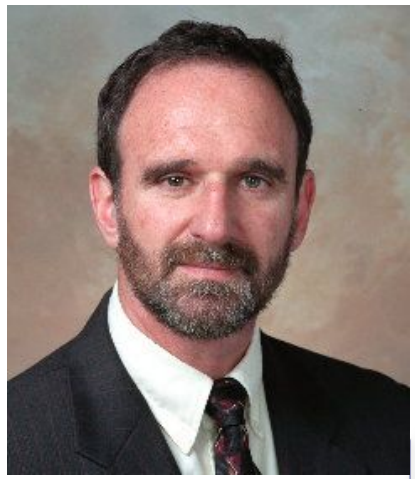
- κρυπτός nascosto — γράφω scrivere
- Cryptography is about communication in the presence of adversaries
  Ron Rivest
- La crittografia serve per:
  - Celare il significato del messaggio
  - Garantire l'autenticità del messaggio
  - Identificare l'autore del messaggio
  - Firmare e datare il messaggio



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

Leon Battista Alberti
(1404-1472)

Whit Diffie
(1944-)



Martin E. Hellman
(1945-)

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

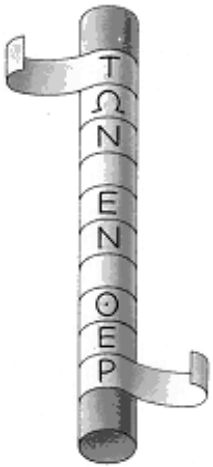
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

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.)*



Τ	Μ	Α	Κ	Α
Ω	Ο	Ν	Λ	
Ν	Π	Ο	Ε	Τ
	Υ	Ν	Η	Υ
Ε	Λ	Τ	Σ	Χ
Ν	Α	Ω		Α
	Ι	Ν	Μ	
Θ	Σ		Ε	
Ε		Ε	Ν	
Ρ	Θ	Υ		

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

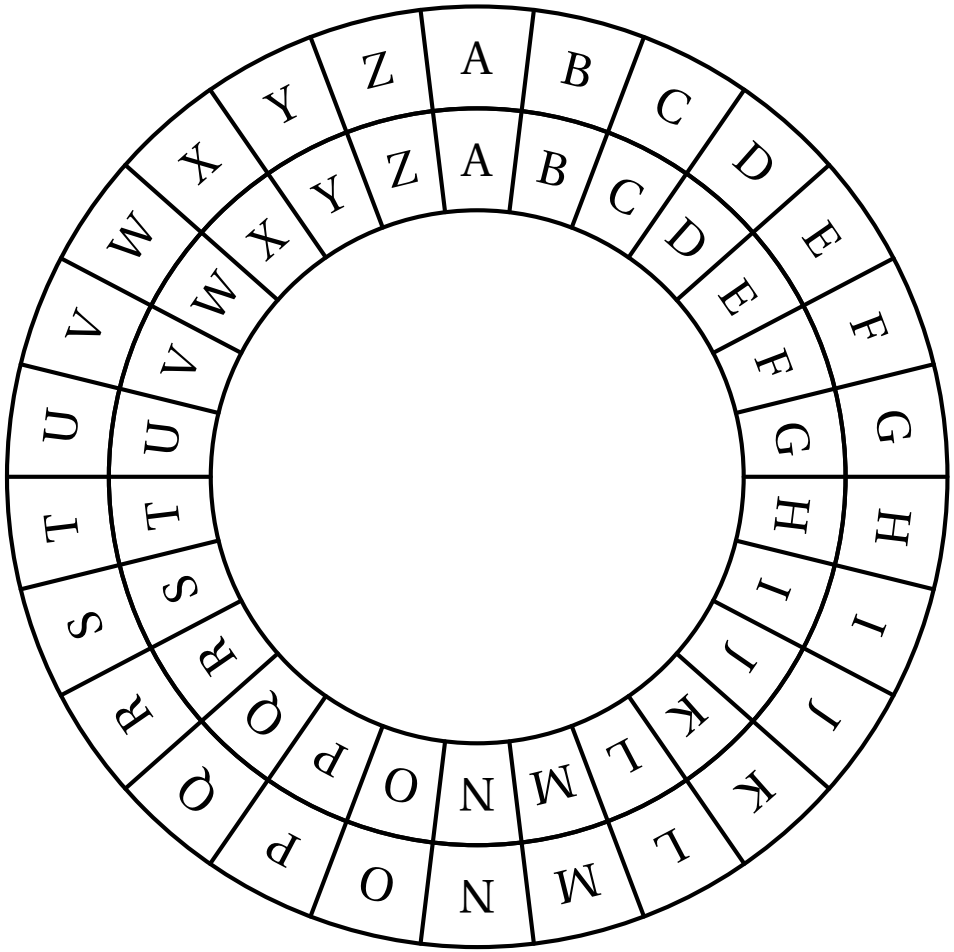
Cesare

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

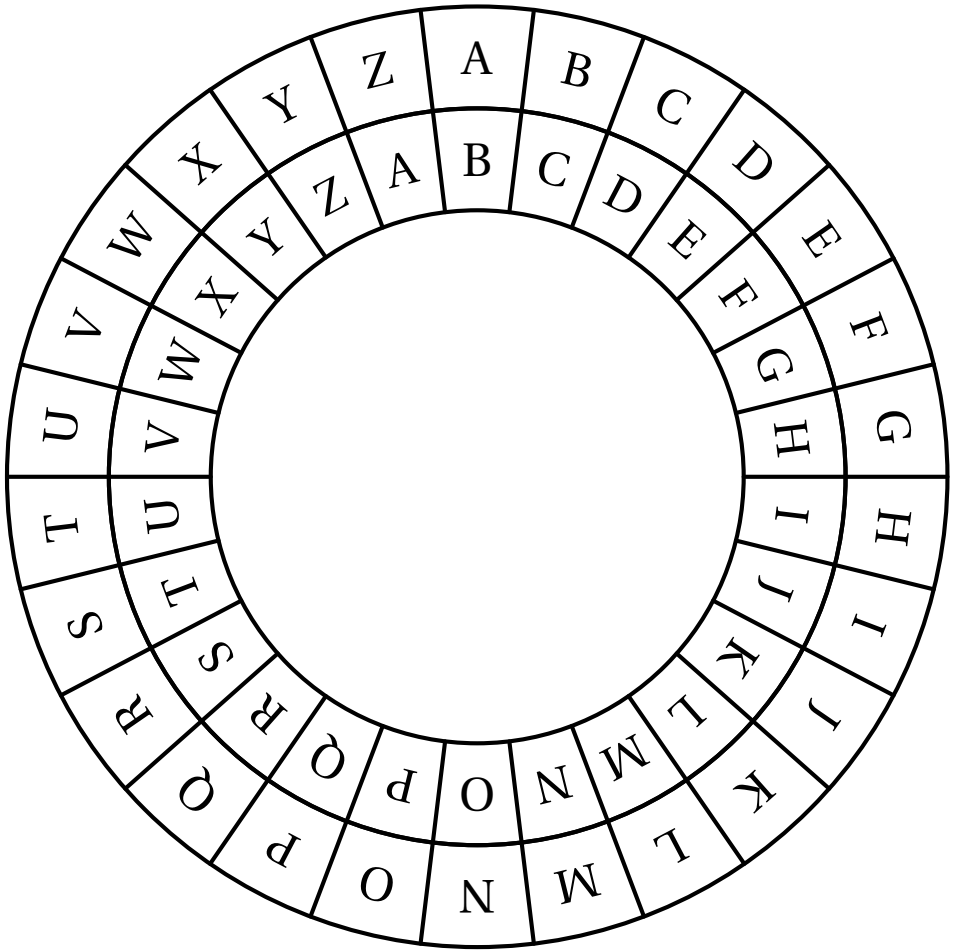
Esempio: AVE diventa DZH.

Leon Battista Alberti (1404–1472)



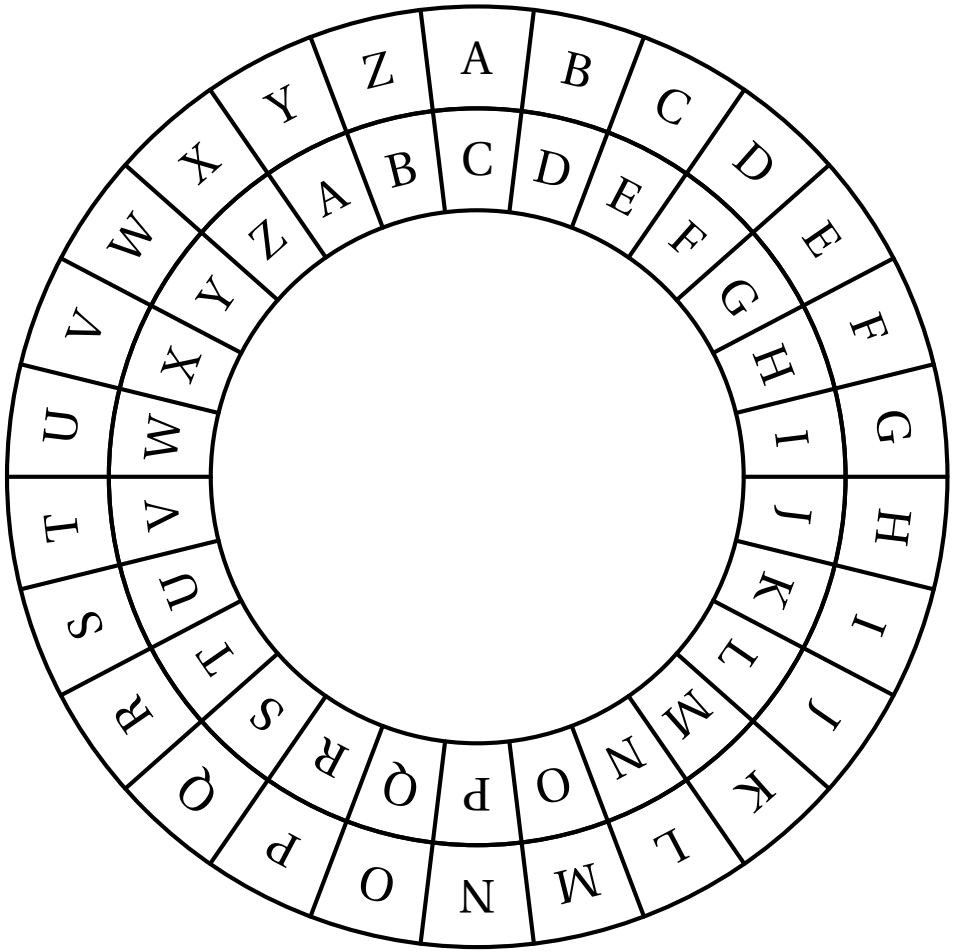
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



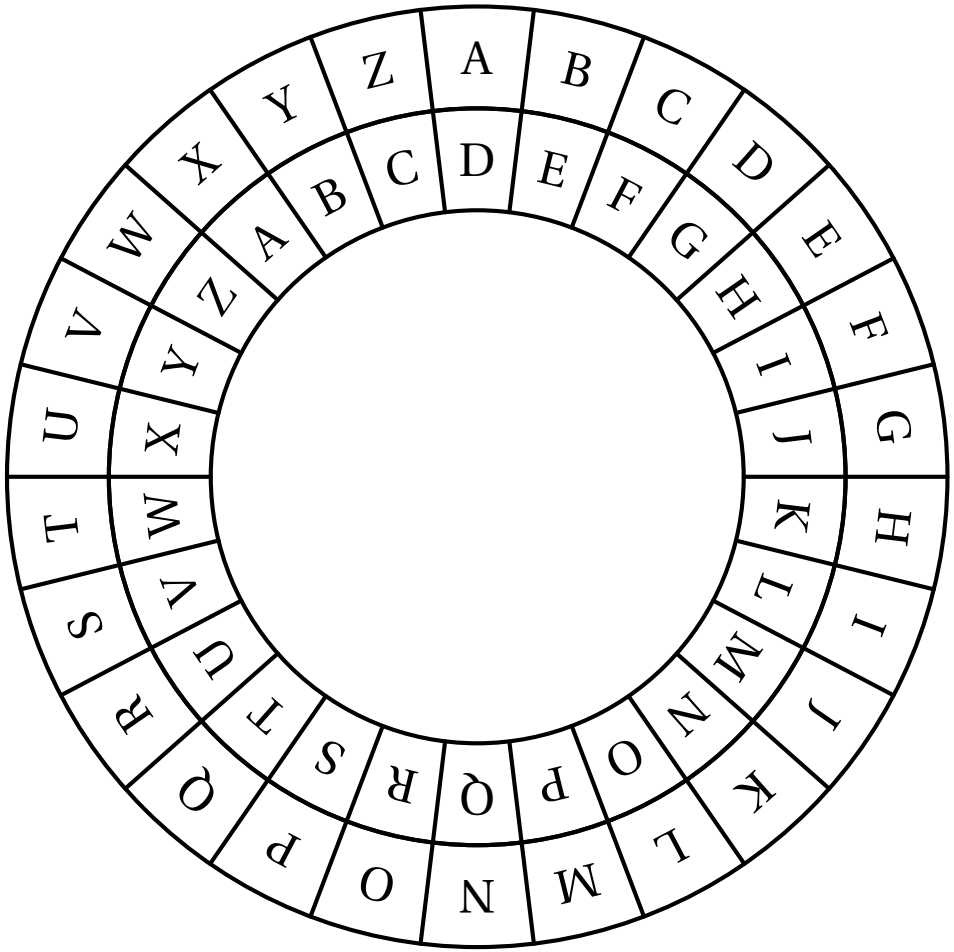
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



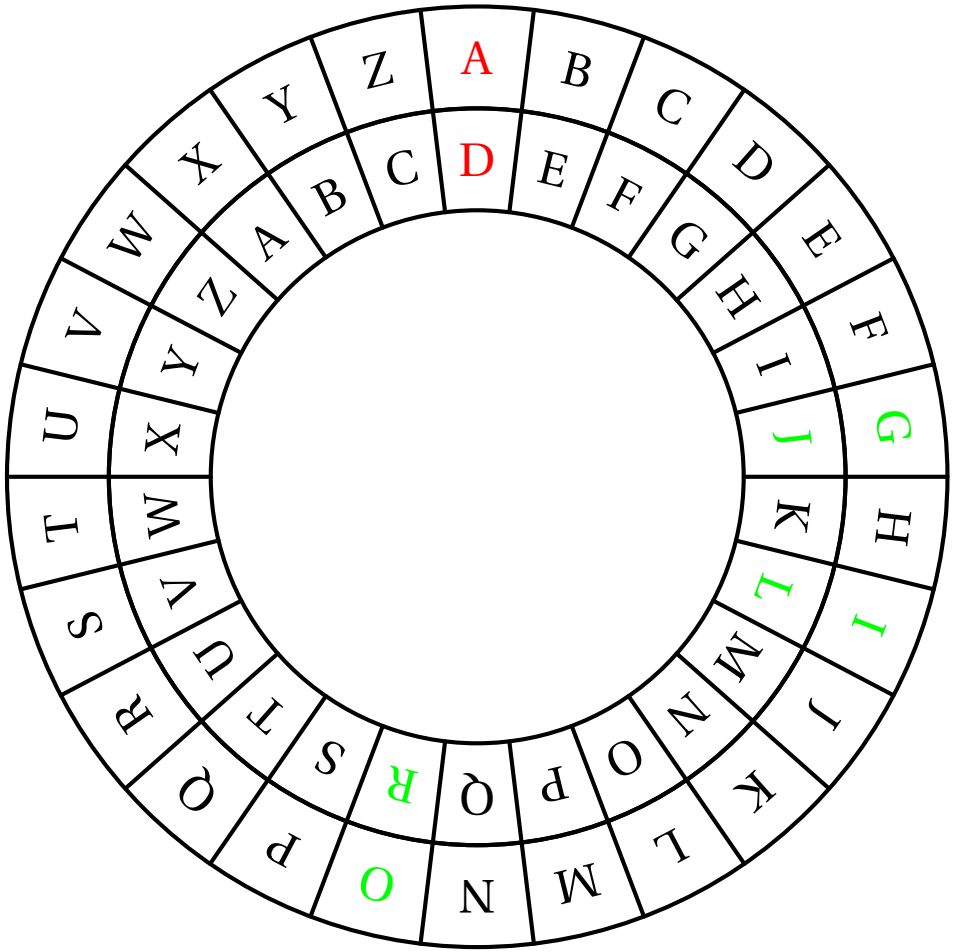
Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)



Disco cifrante: varianti di Cesare

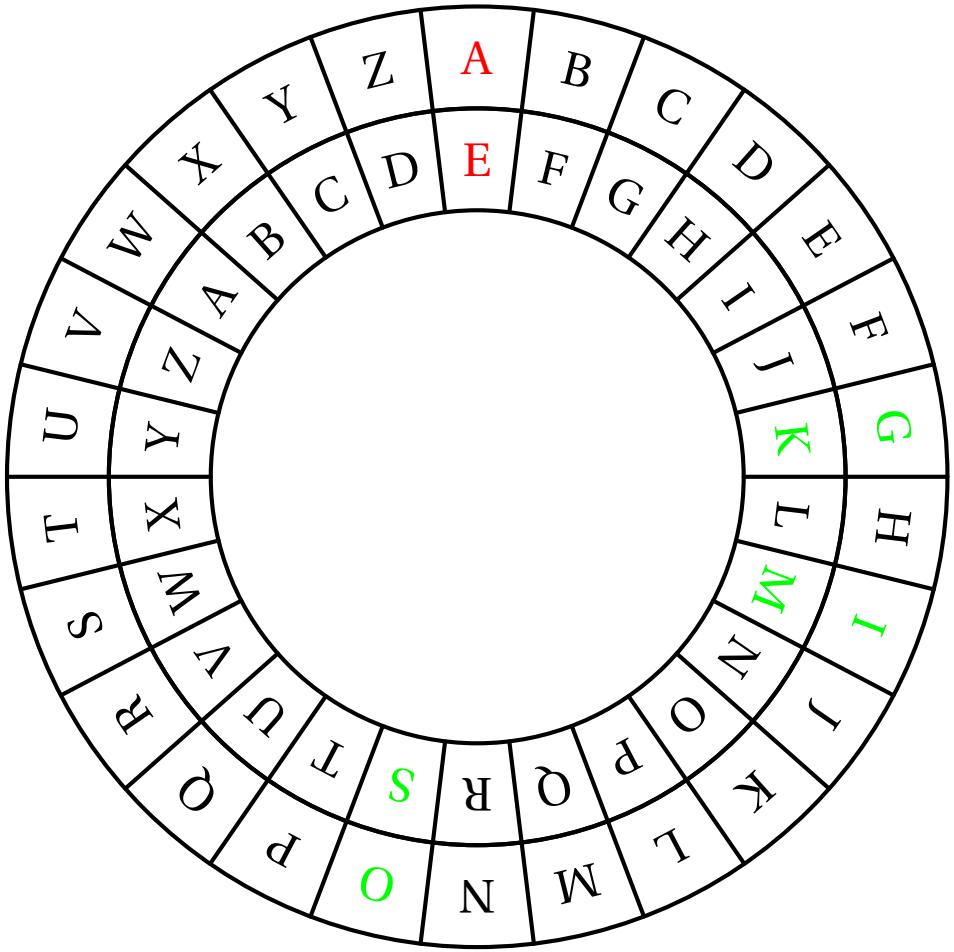
Leon Battista Alberti (1404–1472)



- Chiave D: OGGI → RJJL

Disco cifrante: varianti di Cesare

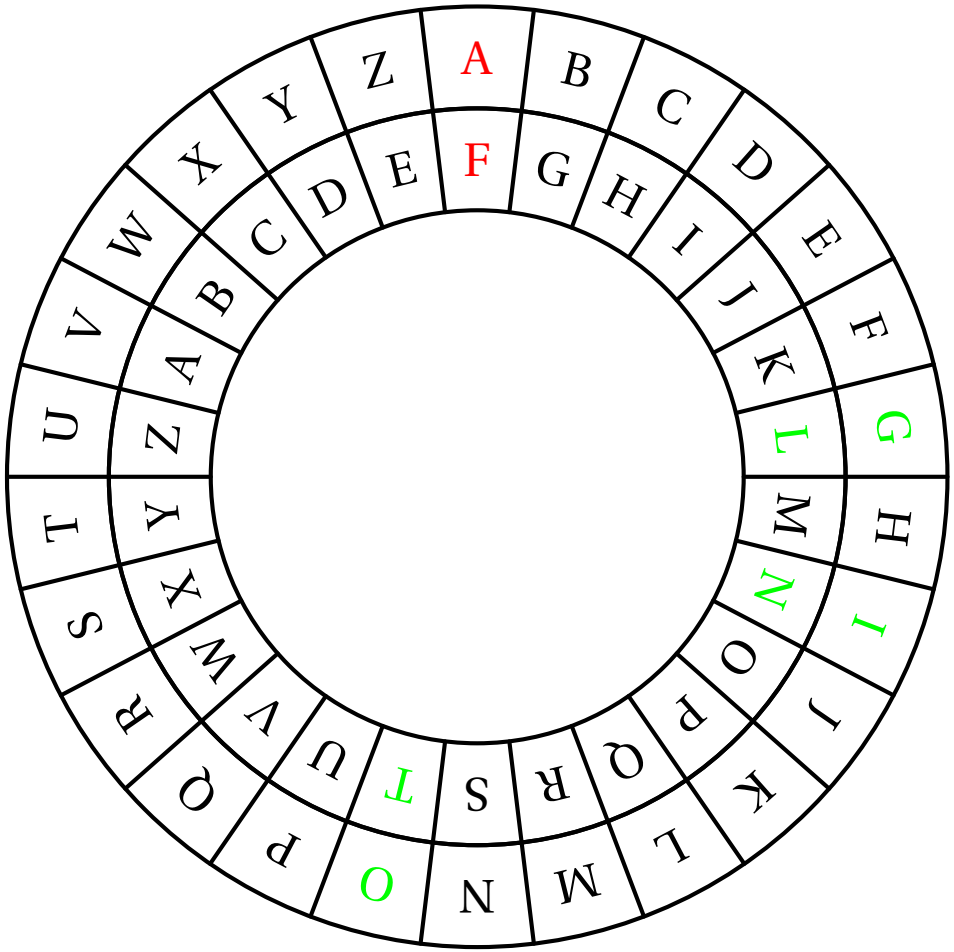
Leon Battista Alberti (1404–1472)



Disco cifrante: varianti di Cesare

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

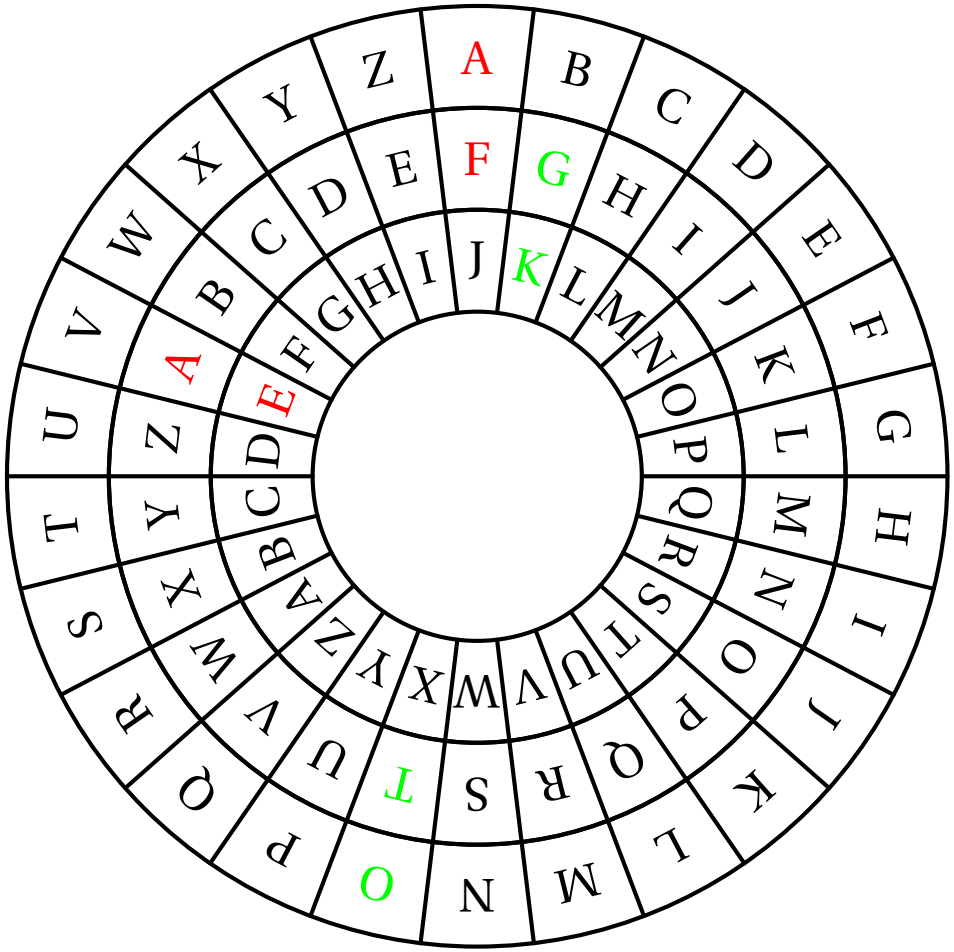
Leon Battista Alberti (1404–1472)



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

Disco cifrante: varianti di Cesare

Leon Battista Alberti (1404–1472)

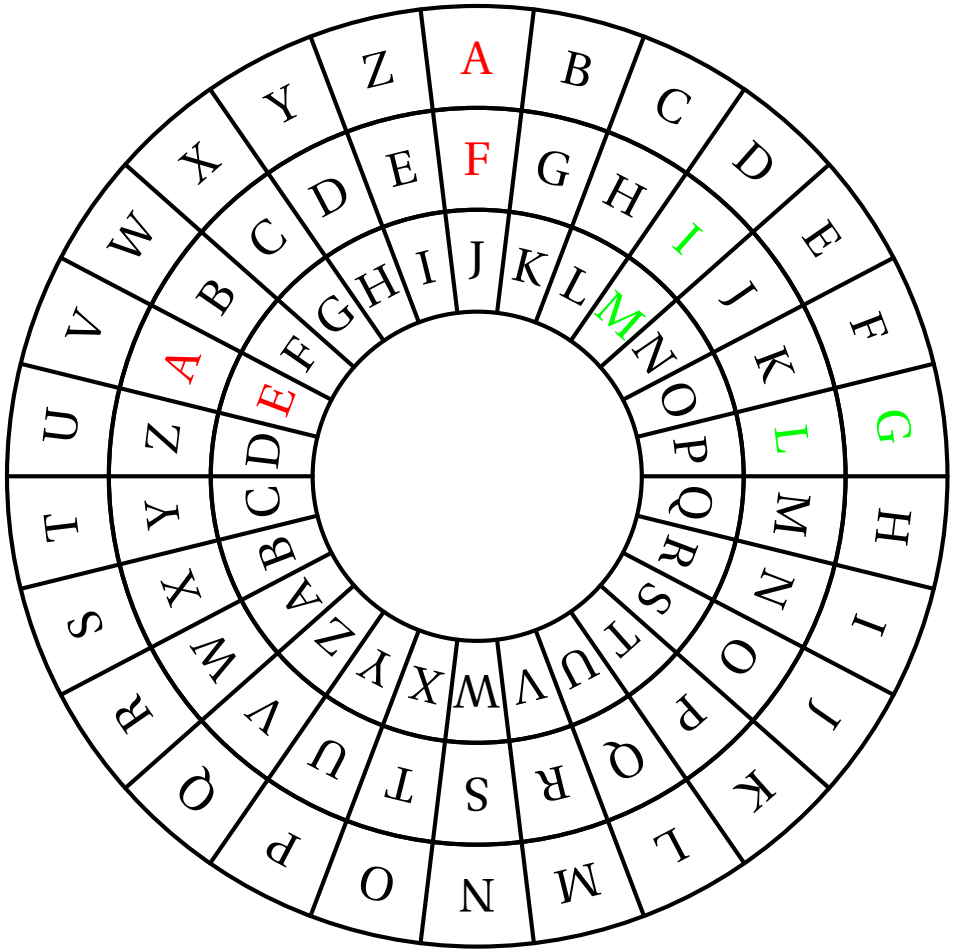


- Chiave D: OGGI → RJJL
- Chiave E: OGGI → SKKM
- Chiave F: OGGI → TLLN

- 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)

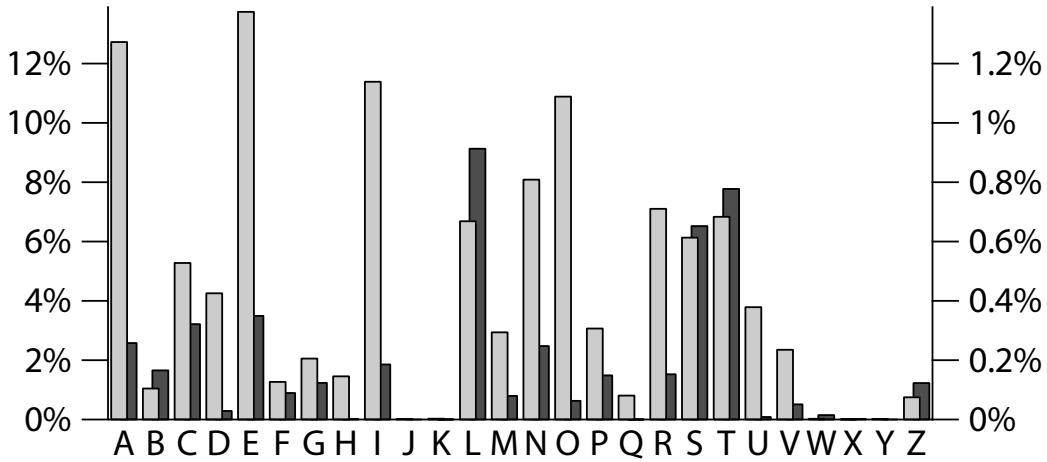
Principio di Kerkhoffs Un sistema deve essere sicuro anche se l'intero sistema, eccetto la chiave, è pubblico

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

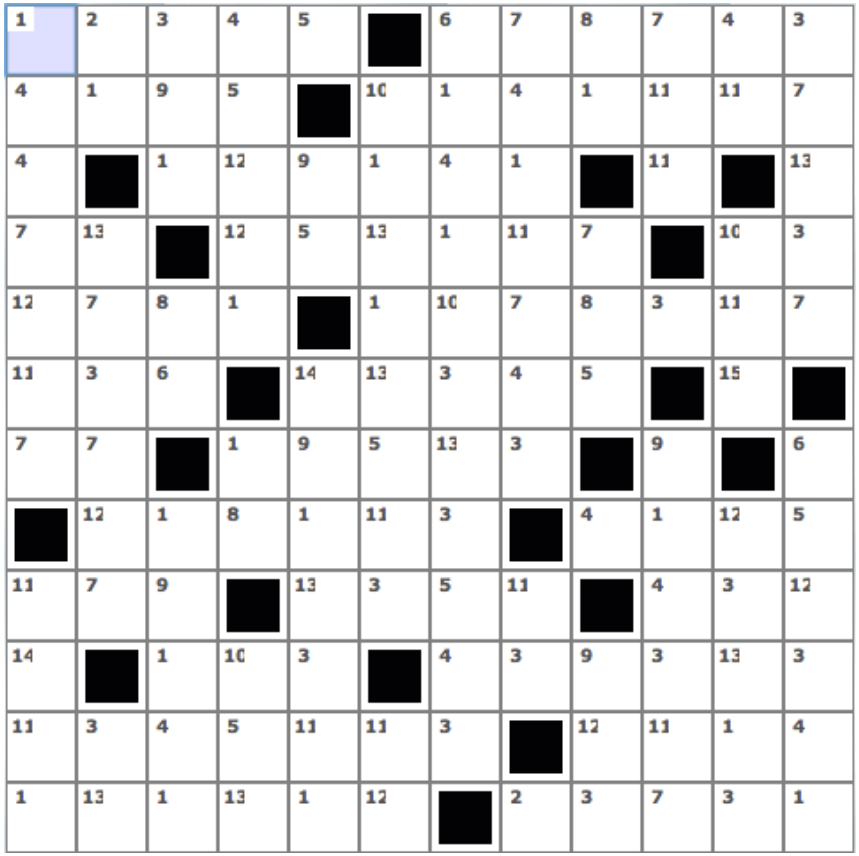


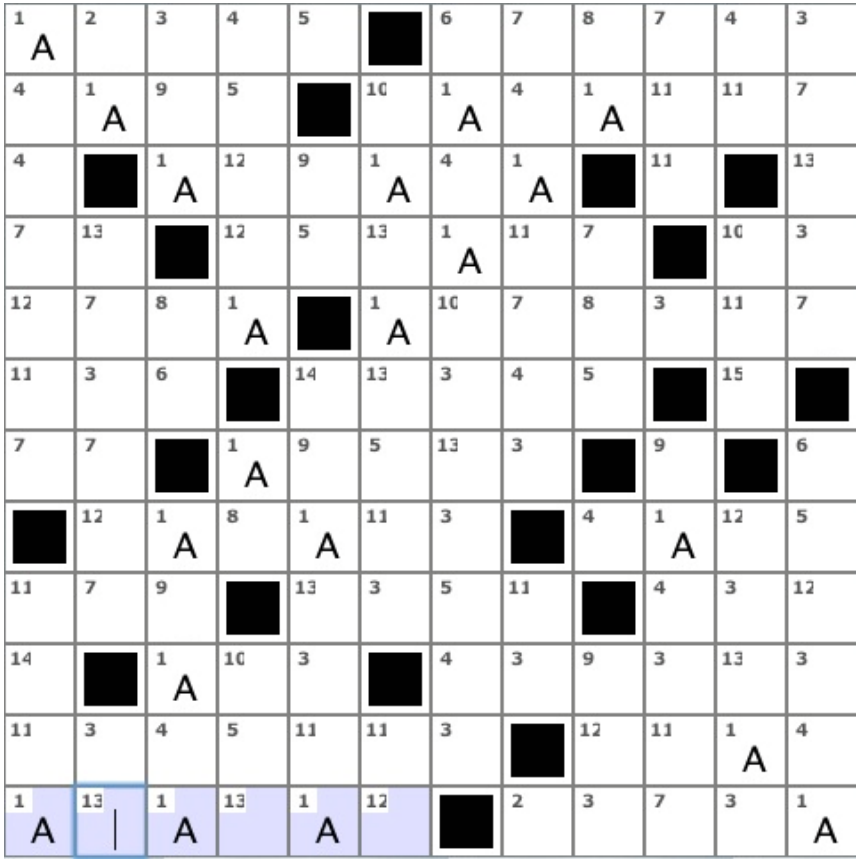
Frequenza delle lettere in italiano, in chiaro a sinistra e, a destra, delle doppie

Sostituzione

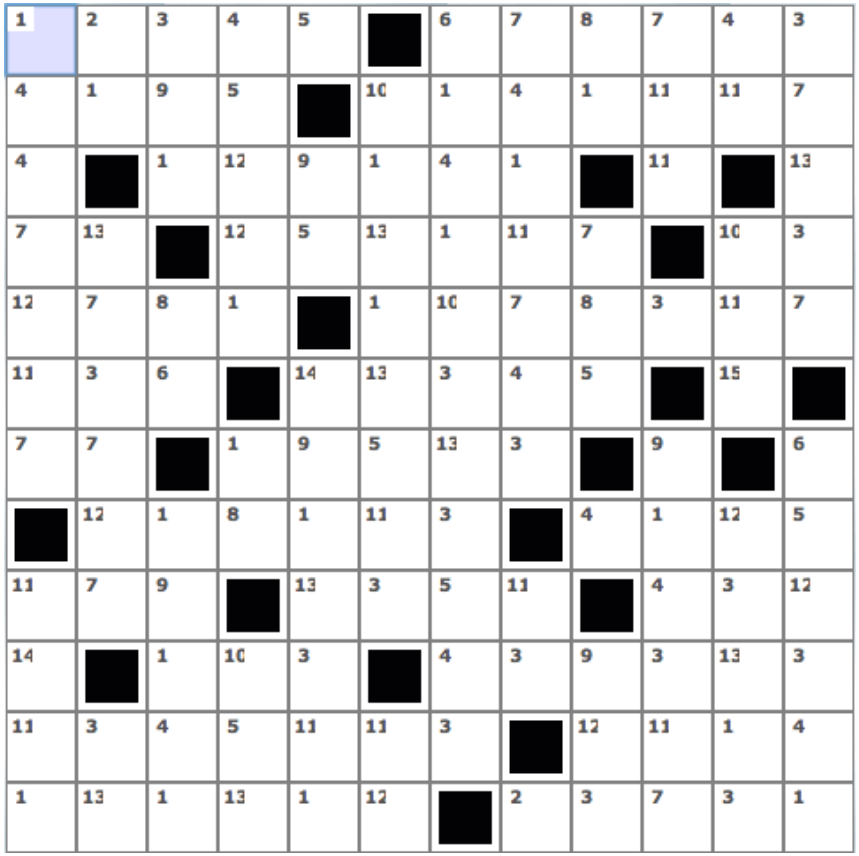
1	2	3	4	5	■	6	7	8	7	4	3
4	1	9	5	■	10	1	4	1	11	11	7
4	■	1	12	9	1	4	1	■	11	■	13
7	13	■	12	5	13	1	11	7	■	10	3
12	7	8	1	■	1	10	7	8	3	11	7
11	3	6	■	14	13	3	4	5	■	15	■
7	7	■	1	9	5	13	3	■	9	■	6
■	12	1	8	1	11	3	■	4	1	12	5
11	7	9	■	13	3	5	11	■	4	3	12
14	■	1	10	3	■	4	3	9	3	13	3
11	3	4	5	11	11	3	■	12	11	1	4
1	13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

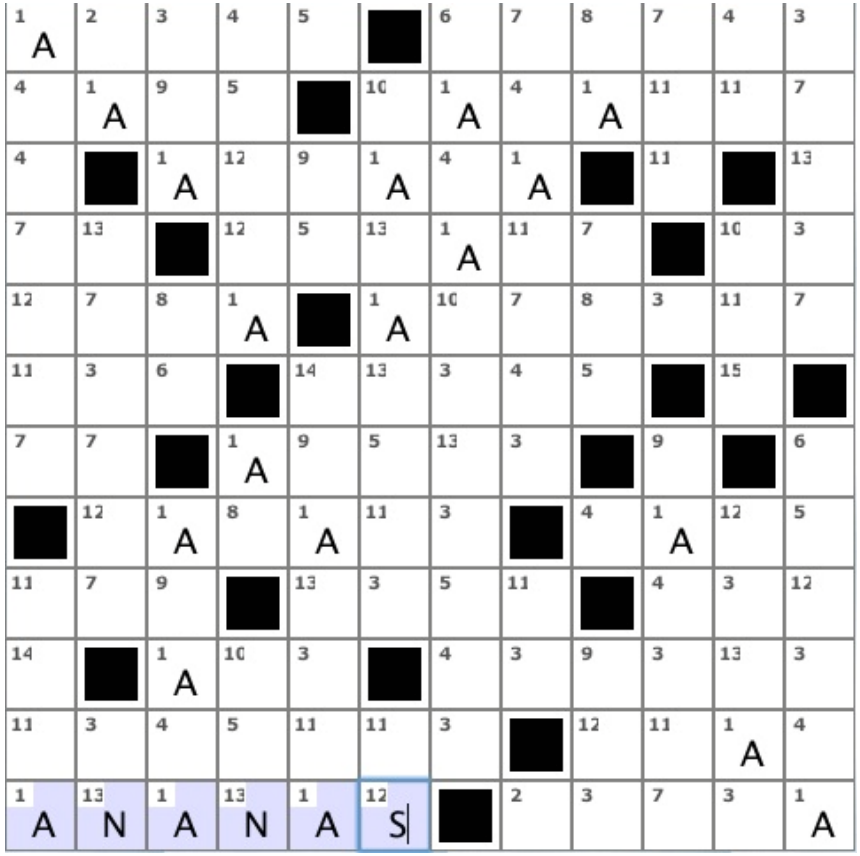
Sostituzione



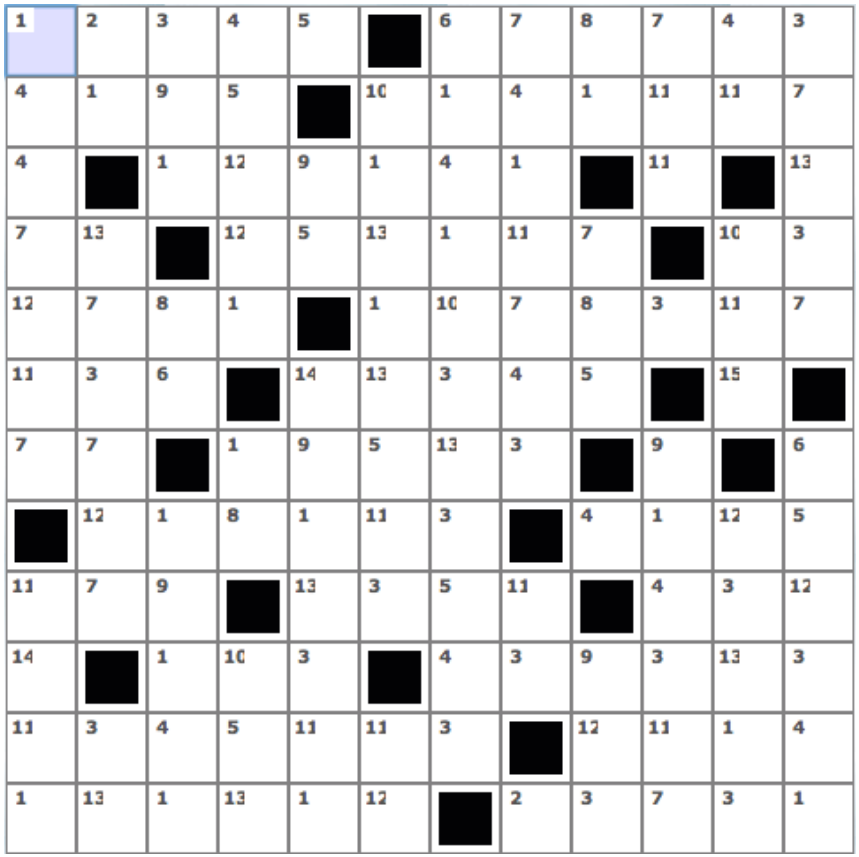


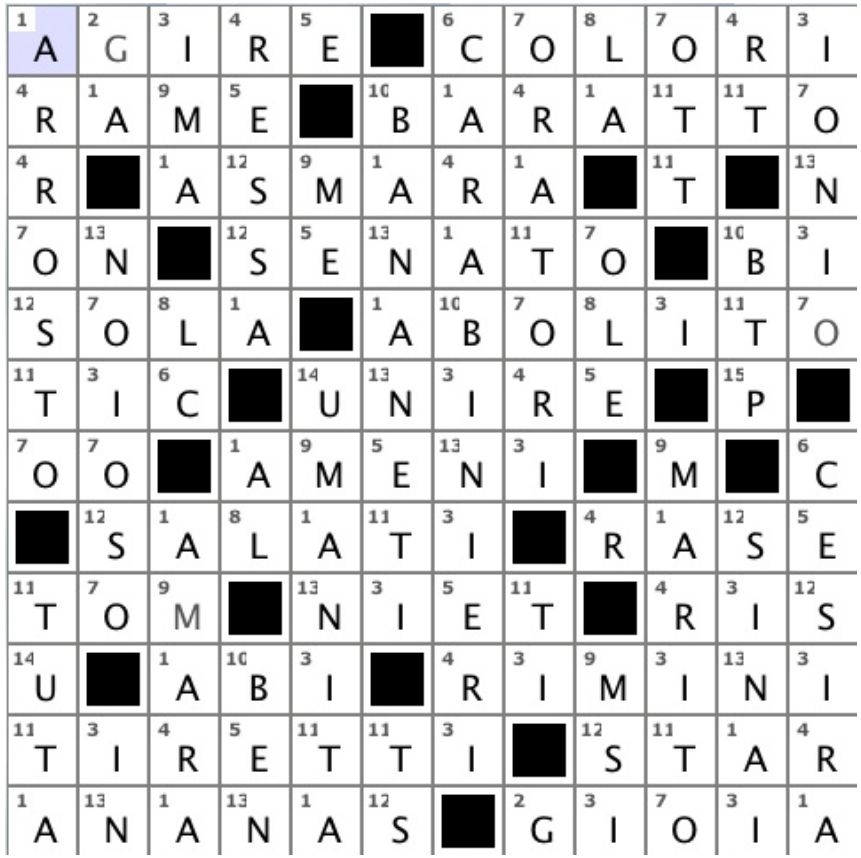
Sostituzione





Sostituzione





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

DES

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

DES

- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione

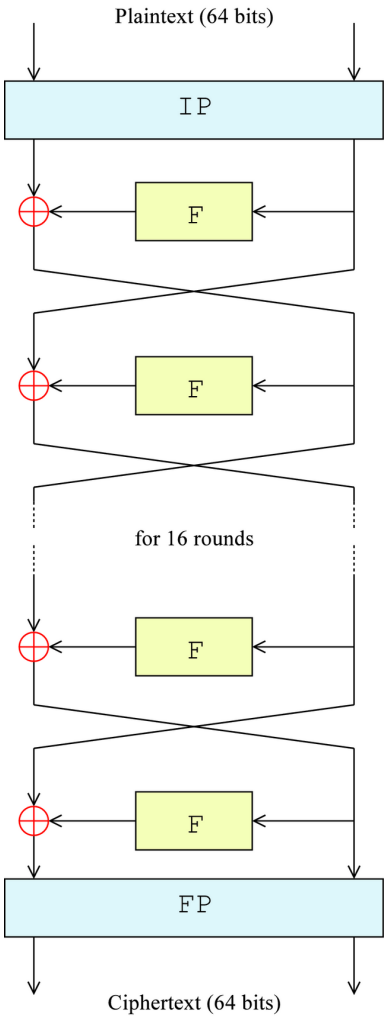
DES

- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione

DES

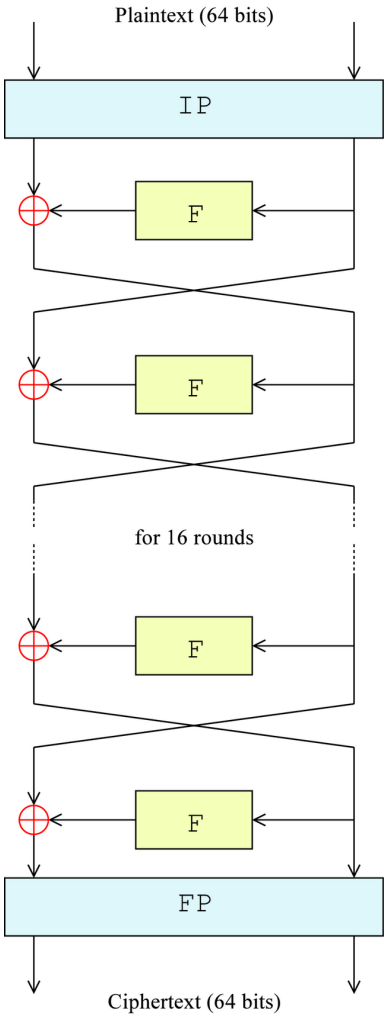
- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione
  - somma della chiave

DES



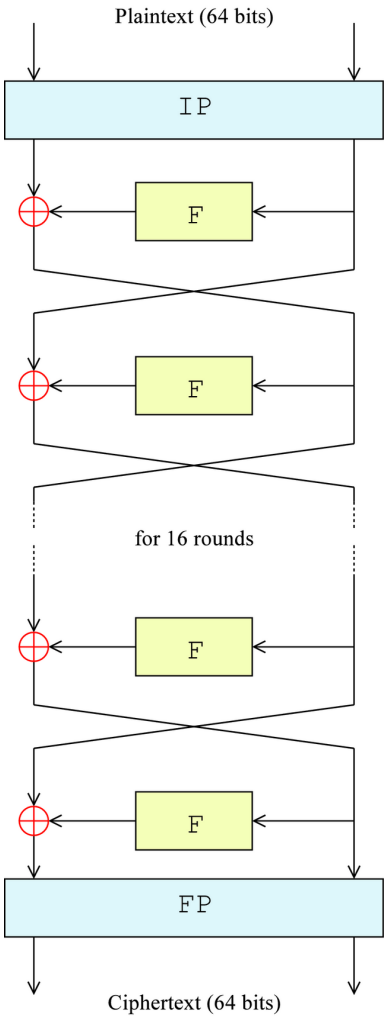
- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione
  - somma della chiave
- Data Encryption Standard, 1976

DES



- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione
  - somma della chiave
- Data Encryption Standard, 1976
  - Sedici iterazioni

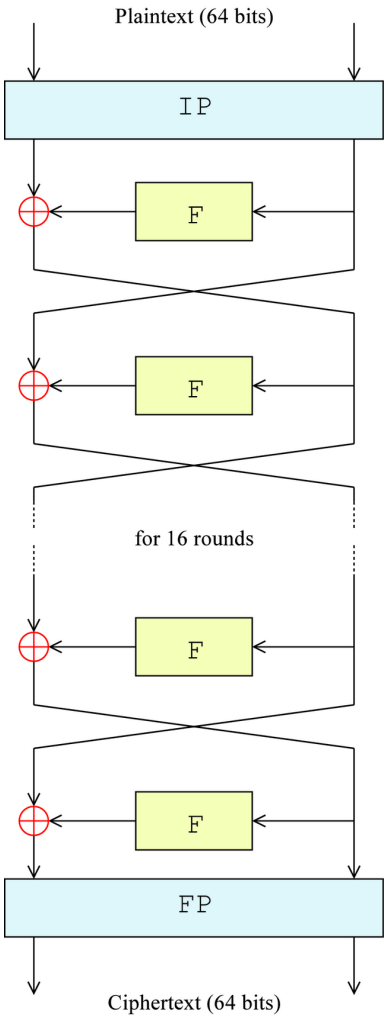
DES



- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione
  - somma della chiave
- Data Encryption Standard, 1976
  - Sedici iterazioni
  - 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



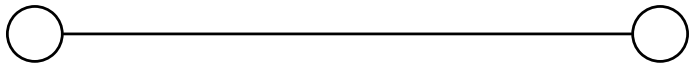
- La crittografia moderna è una combinazione, ripetuta più e più volte, di
  - sostituzione = confusione
  - trasposizione = diffusione
  - somma della chiave
- Data Encryption Standard, 1976
  - Sedici iterazioni
  - Facilmente attaccabile: solo 2^{56} chiavi

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!

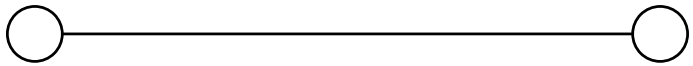
Il problema delle chiavi

- Per ogni coppia che comunica: una chiave

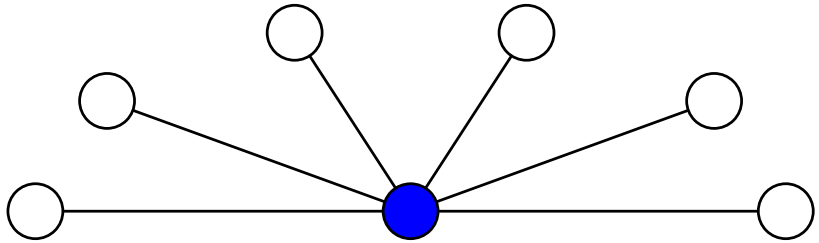


Il problema delle chiavi

- Per ogni coppia che comunica: una chiave

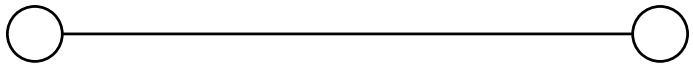


- n parti che comunicano con un sito centrale: n chiavi

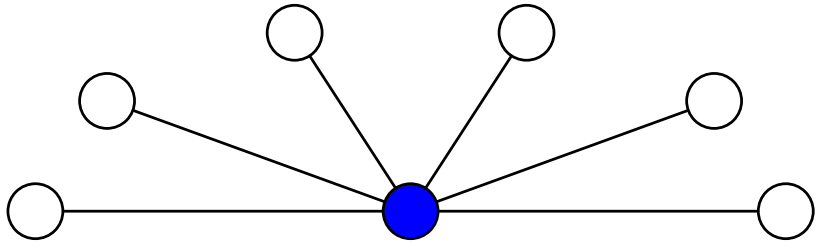


Il problema delle chiavi

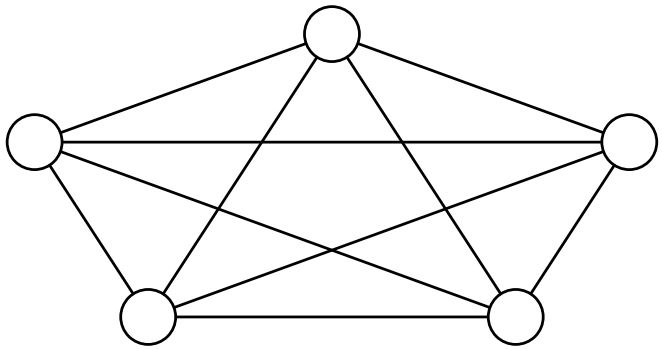
- Per ogni coppia che comunica: una chiave



- 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

- Scambio di chiavi di Diffie–Hellman (1976)

Scambiare chiavi in pubblico

- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo p.

Scambiare chiavi in pubblico

- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B

Scambiare chiavi in pubblico

- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo 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

- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo 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

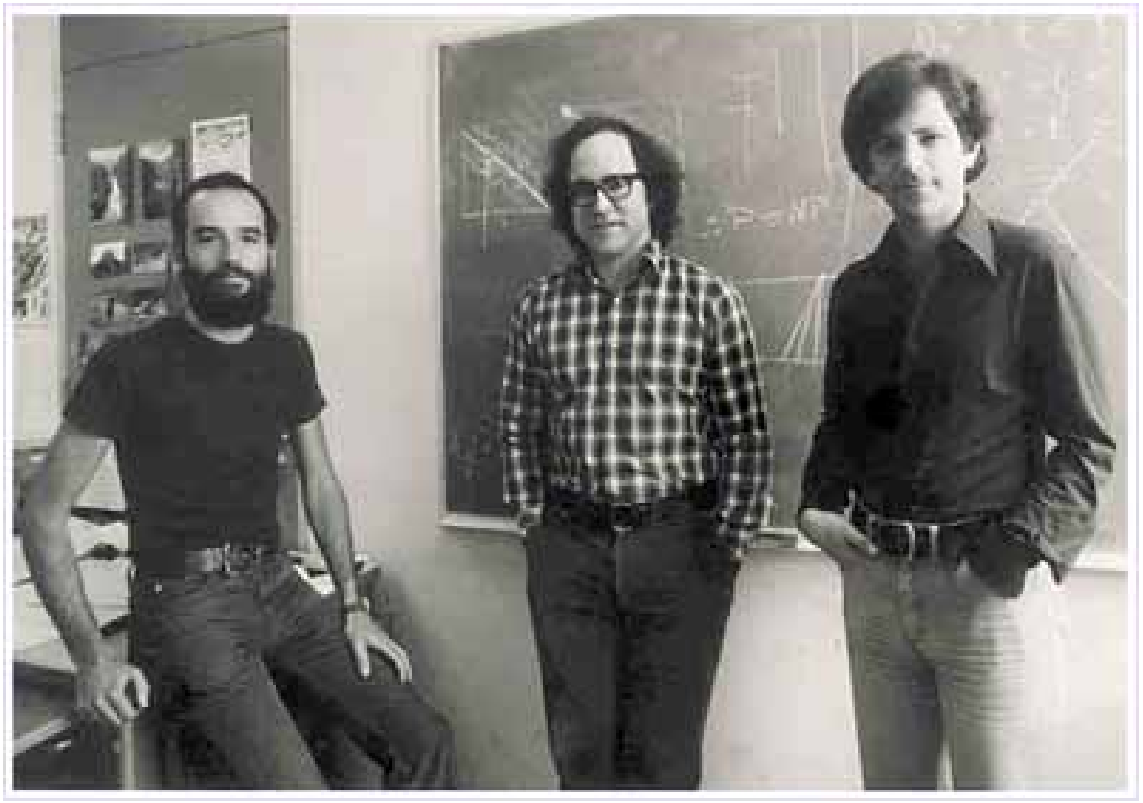
- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo p.
  - Andrea e Barbara scelgono ciascuno un intero a caso n_A e n_B
  - Andrea e Barbara si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$
  - Andrea e Barbara hanno condiviso il segreto $2^{n_A n_B}$
- Idea: noto $2^n \bmod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

Scambiare chiavi in pubblico

- Scambio di chiavi di Diffie–Hellman (1976)
  - Fissiamo un numero primo 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.

Perché?

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

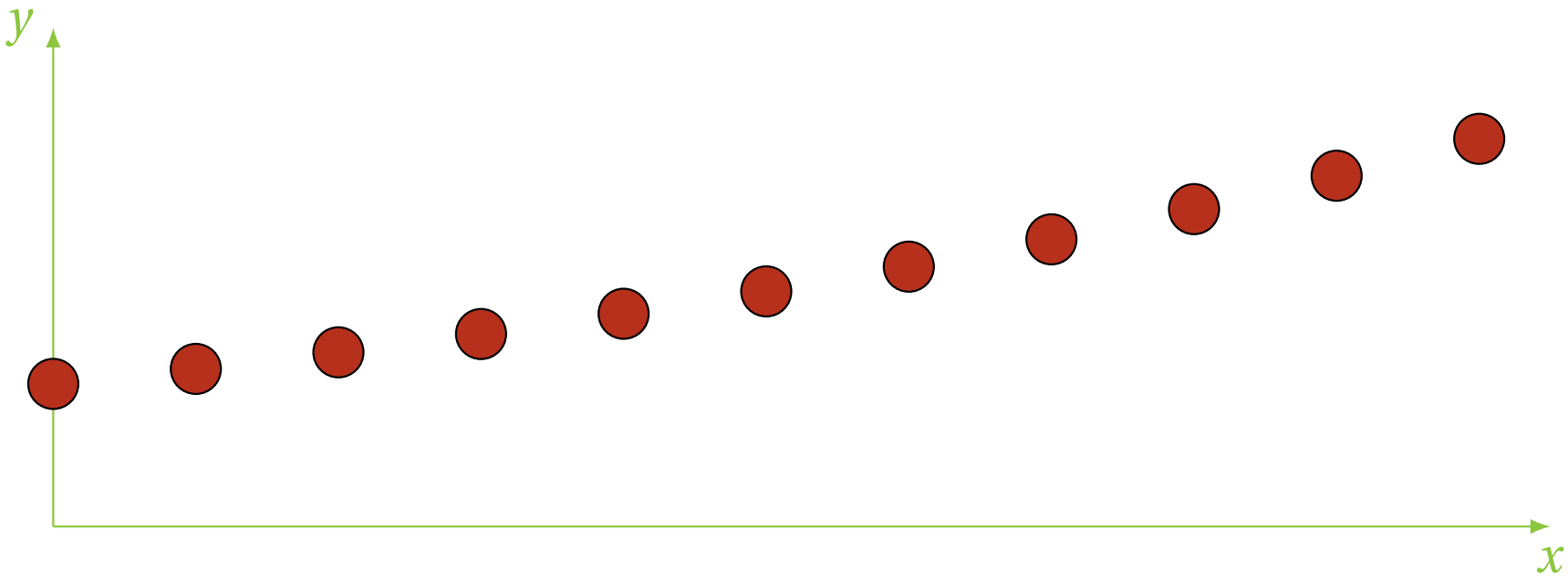
Problema

Didatticamente non funziona

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

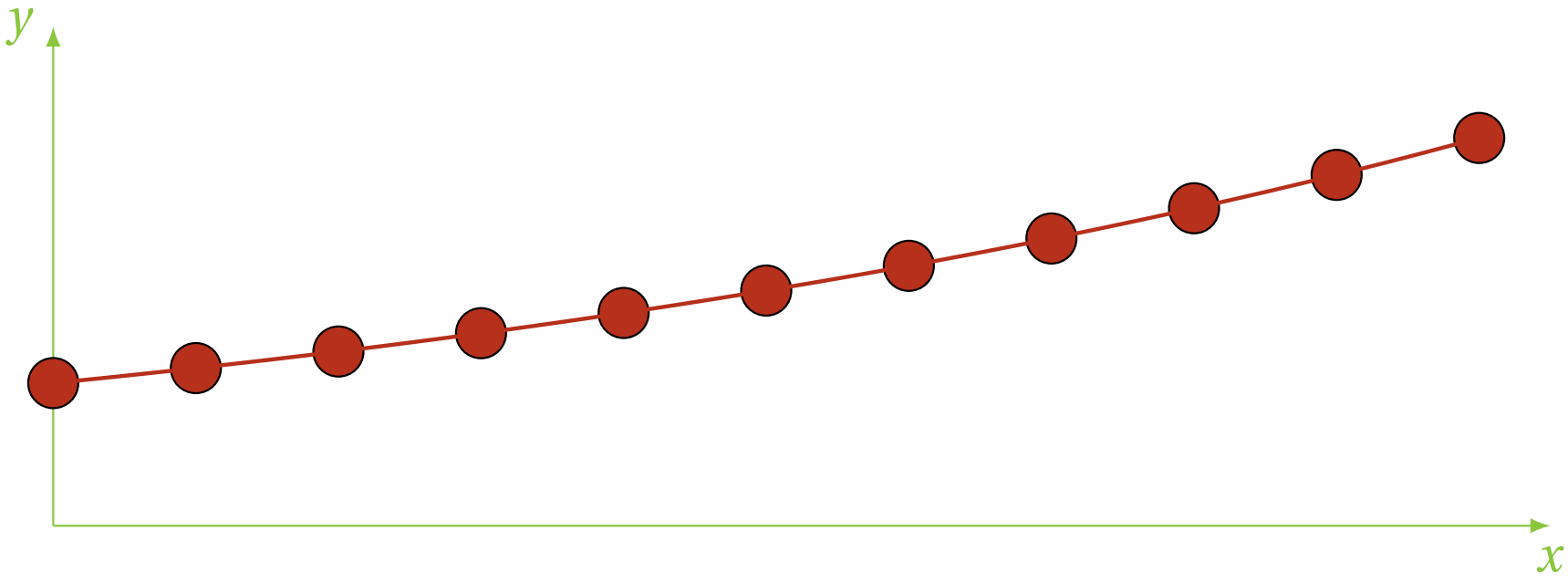
Logaritmo continuo

Lo stesso problema su **R** è banale



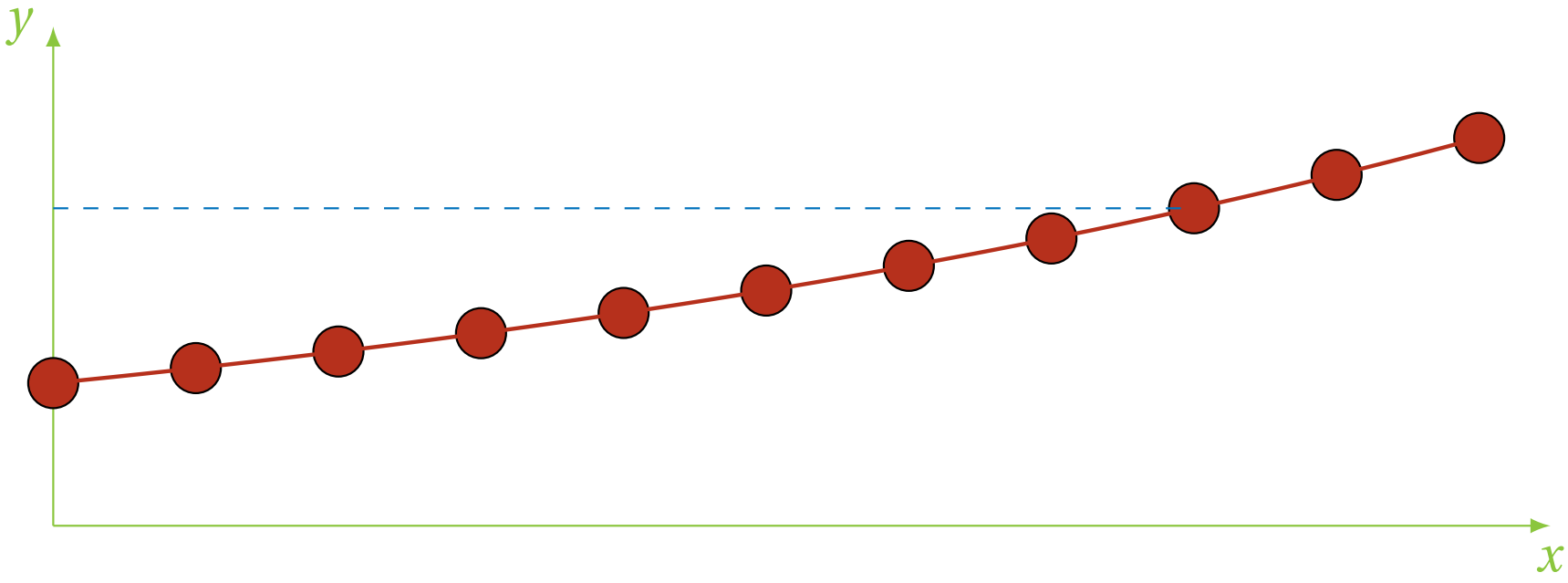
Logaritmo continuo

Lo stesso problema su **R** è banale



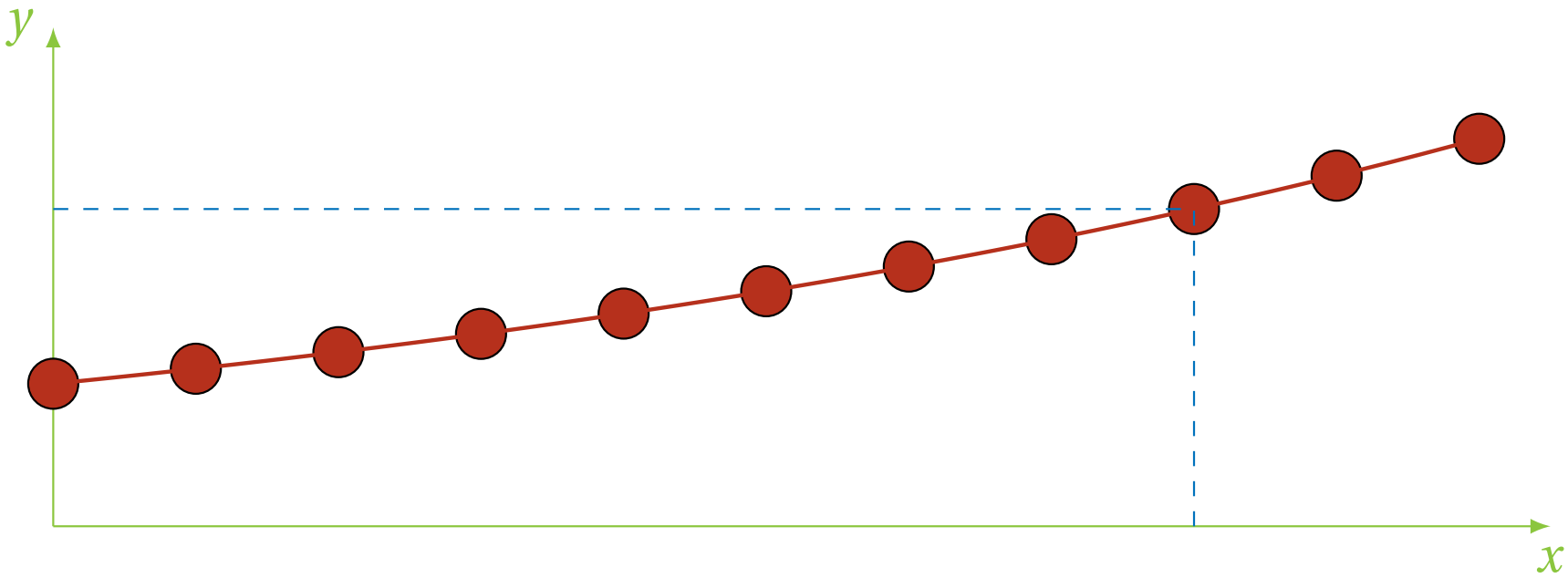
Logaritmo continuo

Lo stesso problema su **R** è banale



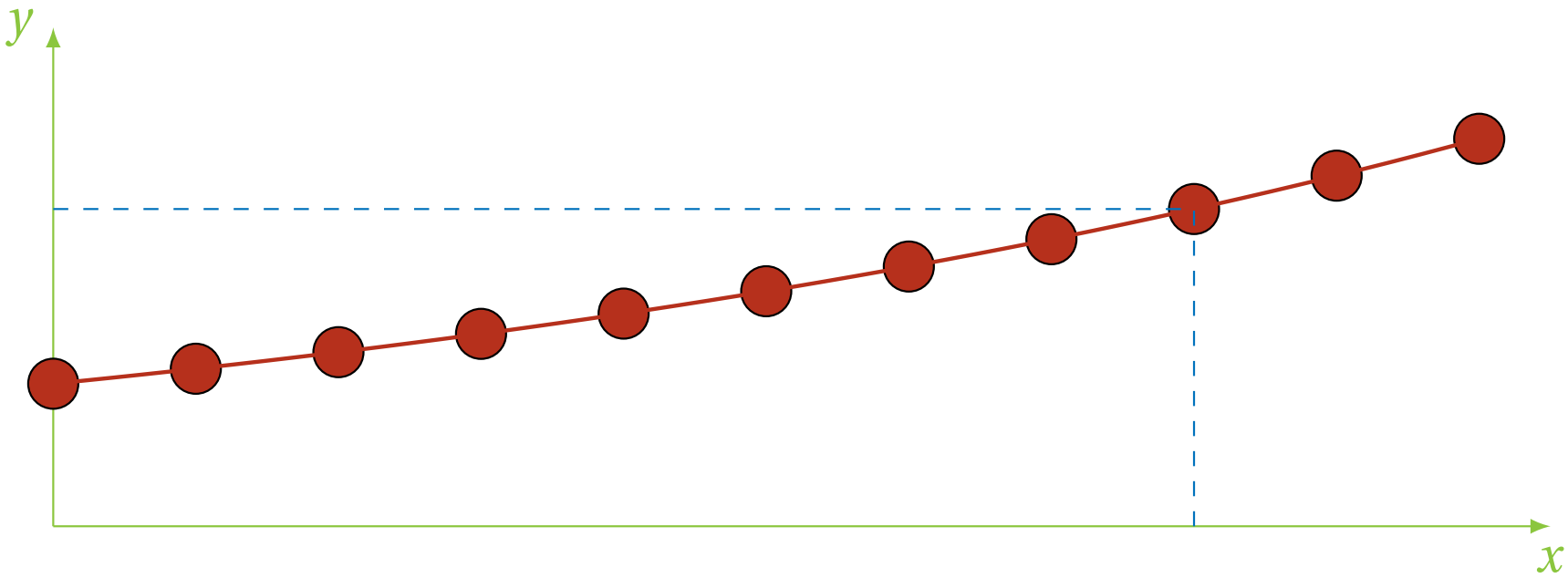
Logaritmo continuo

Lo stesso problema su **R** è banale



Logaritmo continuo

Lo stesso problema su **R** è banale



$$\ln(x) = \sum_{n=1}^{+\infty} \frac{1}{2n+1} \left(\frac{x^2-1}{x^2+1} \right)^{2n+1}$$

Potenze modulo 5

Come si comporta g^α mod n al variare di α?
Fissiamo $n = 5$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	3	1	2	4	3

Potenze modulo 5

Come si comporta g^α mod n al variare di α?
Fissiamo $n = 5$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	3	1	2	4	3

Le potenze si ripetono: se $2^s \equiv 1$ allora

$$2^{s+1} \equiv 2^s \cdot 2 \equiv 2, \qquad 2^{s+a} \equiv 2^s \cdot 2^a \equiv 2^a, \qquad 2^{ks+a} \equiv \left(2^s\right)^k \cdot 2^a \equiv 2^a$$

Potenze modulo 5

Come si comporta $g^\alpha \bmod n$ al variare di α?
Fissiamo $n = 5$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	3	1	2	4	3

Le potenze si ripetono: se $2^s \equiv 1$ allora

$$2^{s+1} \equiv 2^s \cdot 2 \equiv 2, \qquad 2^{s+a} \equiv 2^s \cdot 2^a \equiv 2^a, \qquad 2^{ks+a} \equiv \left(2^s\right)^k \cdot 2^a \equiv 2^a$$

In altre parole: se $g^s \equiv 1$ con $s > 0$ allora gli esponenti sono in realtà definiti modulo s.

Definizione

Chiamiamo ordine di g mod n il minimo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$.

Potenze modulo 6

Fissiamo $n = 6$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	2	4	2	4	2

Potenze modulo 6

Fissiamo $n = 6$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	2	4	2	4	2

Quindi non esiste nessun intero $s > 0$ tale che $2^s \equiv 1 \bmod 6$.

Potenze modulo 6

Fissiamo $n = 6$ e $g = 2$. Abbiamo

α	0	1	2	3	4	5	6	7
2^α	1	2	4	2	4	2	4	2

Quindi non esiste nessun intero $s > 0$ tale che $2^s \equiv 1 \bmod 6$.

Domanda

Cosa sta succedendo?

Potenze modulo 7

Fissiamo $n = 7$. Allora:
Le potenze di 2 sono: $1, 2, 4, 1, 2, \ldots$
Le potenze di 3 sono: $1, 3, 2, 6, 4, 5, 1, \ldots$
Le potenze di 4 sono: $1, 4, 2, 1, \ldots$
Le potenze di 5 sono: $1, 5, 4, 6, 2, 3, 1, \ldots$
Le potenze di 6 sono: $1, 6, 1, \ldots$

Potenze modulo 7

Fissiamo $n = 7$. Allora:
Le potenze di 2 sono: $1, 2, 4, 1, 2, \ldots$
Le potenze di 3 sono: $1, 3, 2, 6, 4, 5, 1, \ldots$
Le potenze di 4 sono: $1, 4, 2, 1, \ldots$
Le potenze di 5 sono: $1, 5, 4, 6, 2, 3, 1, \ldots$
Le potenze di 6 sono: $1, 6, 1, \ldots$
3 e 5 generano tutte le classi non nulle, gli altri no. Diciamo che 3 e 5 sono generatori.

Potenze modulo 10

Le potenze di 2 sono: $1, 2, 4, 8, 6, 2, 4, 8, 6, 2 \ldots$
Le potenze di 3 sono: $1, 3, 9, 7, 1, \ldots$
Le potenze di 4 sono: $1, 4, 6, 4, 6, 4, \ldots$
Le potenze di 5 sono: $1, 5, 5, 5, \ldots$
Le potenze di 6 sono: $1, 6, 6, 6, \ldots$
Le potenze di 7 sono: $1, 7, 9, 3, 1, \ldots$
Le potenze di 8 sono: $1, 8, 4, 2, 6, 8, 4, 2, 6, 8, \ldots$
Le potenze di 9 sono: $1, 9, 1, \ldots$

Potenze modulo 11

Le potenze di 2 sono: $1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, \ldots$
Le potenze di 3 sono: $1, 3, 9, 5, 4, 1, \ldots$
Le potenze di 4 sono: $1, 4, 5, 9, 3, 1, \ldots$
Le potenze di 5 sono: $1, 5, 3, 4, 9, 1, \ldots$
Le potenze di 6 sono: $1, 6, 3, 7, 9, 10, 5, 8, 4, 2, 1, \ldots$
Le potenze di 7 sono: $1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1, \ldots$
Le potenze di 8 sono: $1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1, \ldots$
Le potenze di 9 sono: $1, 9, 4, 3, 5, 1, \ldots$
Le potenze di 10 sono: $1, 10, 1, \ldots$

Potenze modulo 13

Le potenze di 2 sono: $1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, \ldots$
Le potenze di 3 sono: $1, 3, 9, 1, \ldots$
Le potenze di 4 sono: $1, 4, 3, 12, 9, 10, 1, \ldots$
Le potenze di 5 sono: $1, 5, 12, 8, 1, \ldots$
Le potenze di 6 sono: $1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, \ldots$
Le potenze di 7 sono: $1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, \ldots$
Le potenze di 8 sono: $1, 8, 12, 5, 1, \ldots$
Le potenze di 9 sono: $1, 9, 3, 1, \ldots$
Le potenze di 10 sono: $1, 10, 9, 12, 3, 4, 1, \ldots$
Le potenze di 11 sono: $1, 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1, \ldots$
Le potenze di 12 sono: $1, 12, 1, \ldots$

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

- esiste l'ordine se e solo se g, n sono relativamente primi

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

- esiste l'ordine se e solo se g, n sono relativamente primi
- $o_n(n-1) = 2$

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

- esiste l'ordine se e solo se g, n sono relativamente primi
- $o_n(n-1) = 2$
- se n è primo, $o_n(g)$ divide $n-1$

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

- esiste l'ordine se e solo se g, n sono relativamente primi
- $o_n(n-1) = 2$
- se n è primo, $o_n(g)$ divide $n-1$
- se n è primo, $g^{n-1} \equiv 1 \bmod n$ per ogni $g \not\equiv 0 \bmod n$

Un po' di congetture

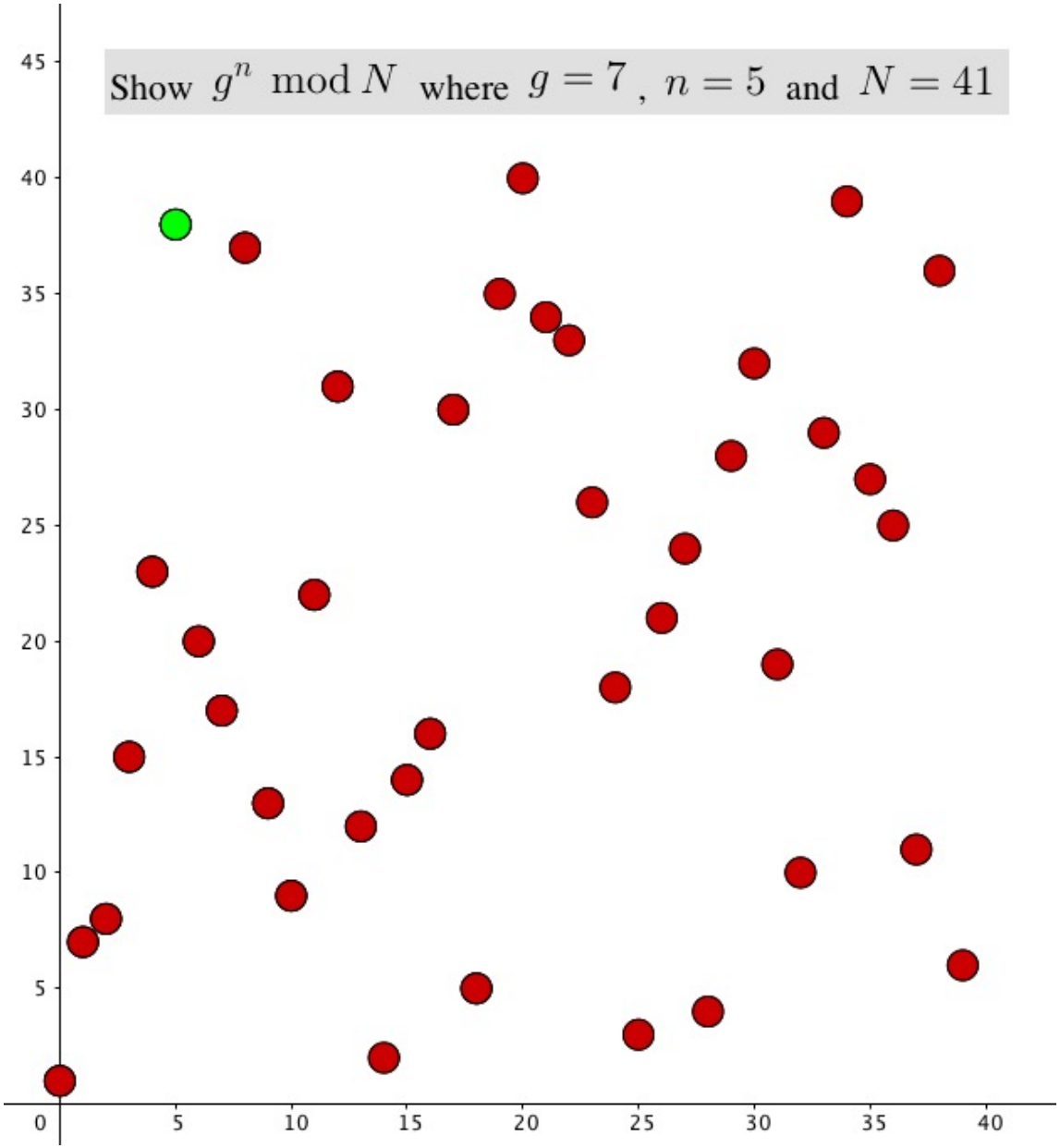
Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

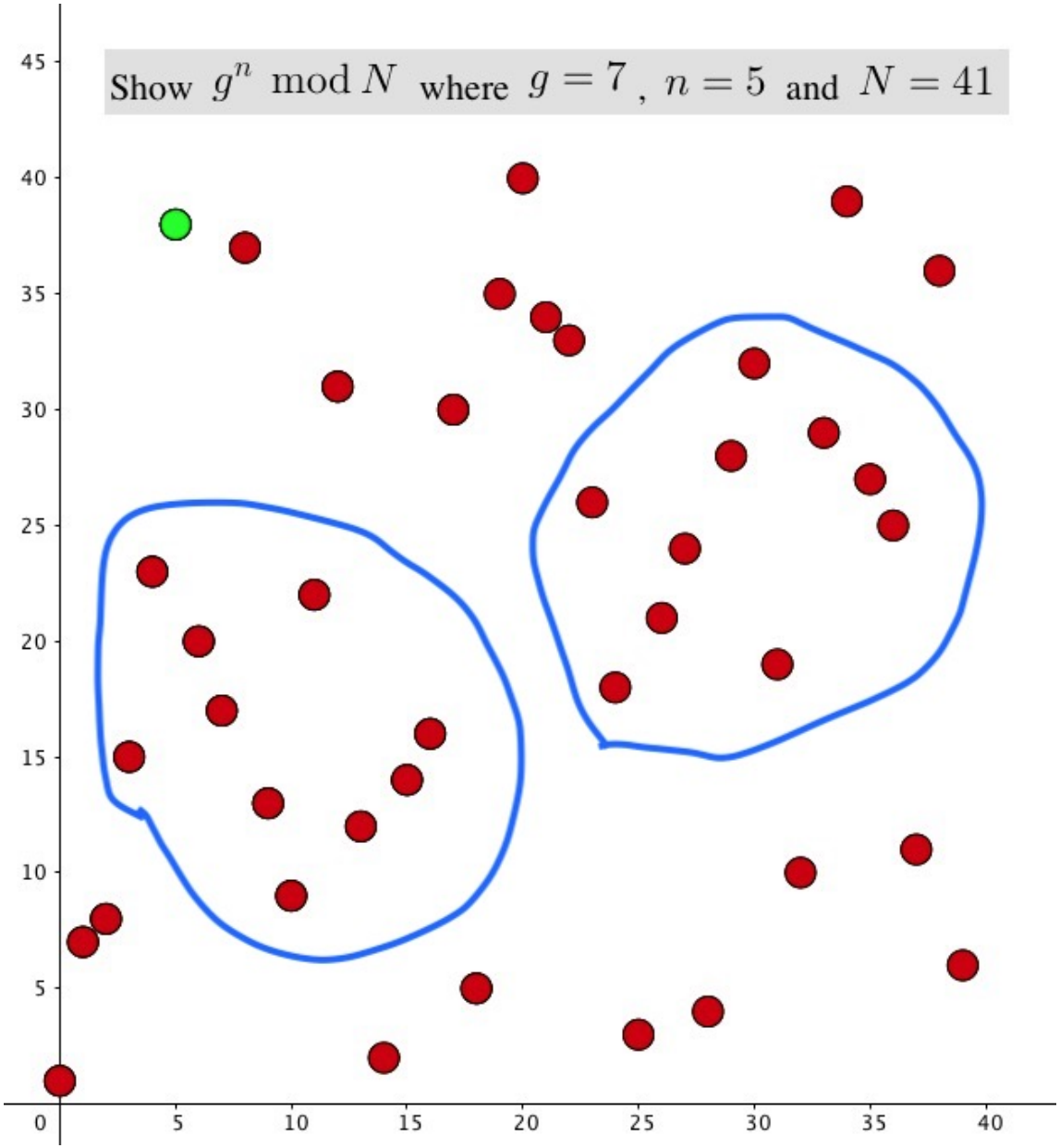
- esiste l'ordine se e solo se g, n sono relativamente primi
- $o_n(n-1) = 2$
- se n è primo, $o_n(g)$ divide $n-1$
- se n è primo, $g^{n-1} \equiv 1 \bmod n$ per ogni $g \not\equiv 0 \bmod n$
- se n è primo, $g^n \equiv g \bmod n$ per ogni g

Un po' di congetture

Definiamo l'ordine $o_n(g)$ di g mod n come il più piccolo intero $s > 0$ tale che $g^s \equiv 1 \bmod n$. Notiamo che l'ordine non esiste sempre!
Avremo che

- esiste l'ordine se e solo se g, n sono relativamente primi
- $o_n(n-1) = 2$
- se n è primo, $o_n(g)$ divide $n-1$
- se n è primo, $g^{n-1} \equiv 1 \bmod n$ per ogni $g \not\equiv 0 \bmod n$
- se n è primo, $g^n \equiv g \bmod n$ per ogni g
- se $s = o_n(g)$, allora $g \cdot g^{s-1} \equiv 1 \bmod n$; cioè $g^{-1} \equiv g^{s-1} \bmod n$


Show $g^n \bmod N$ where $g = 7$, $n = 5$ and $N = 41$
45
40
35
30
25
20
15
10
5
0
5
10
15
20
25
30
35
40


Show $g^n \bmod N$ where $g = 7$, $n = 5$ and $N = 41$
45
40
35
30
25
20
15
10
5
0
5
10
15
20
25
30
35
40

Logaritmo discreto

Definition (logaritmo modulare)

c è il logaritmo di a in base b modulo n se

$$a \equiv b^c \bmod n$$

Fatti

- c non è un elemento di $\mathbf{Z}/n\mathbf{Z}$
- Se n è primo, il logaritmo modulo n è definito modulo $n-1$

Quindi

Il logaritmo è una funzione da un insieme in uno totalmente diverso!

Il Problema del Logaritmo Discreto

DLP

Il problema del logaritmo discreto è:

- dato n primo
- dato una classe di resto g mod n con $o(g) = n-1$
- dato un qualsiasi elemento $x \in \mathbf{Z}/n\mathbf{Z}$ con $x \not\equiv 0 \mod n$

Trovare c tale che $x \equiv g^x \mod n$

Fatto

Il Problema del logaritmo discreto è molto difficile

Possiamo attaccarlo per forza bruta, ma ...

Calcolo dell'indice

Obiettivo

Vogliamo calcolare $\log_7(26 \bmod 41)$.

Idea

- Ricordiamo che $\log_7$ è una funzione a valori $\bmod 40$
- Troviamo potenze di 7 che si fattorizzano in primi piccoli
- Calcoliamo $\log_7$ per tutti i primi piccoli, usando l'algebra lineare $\bmod 40$
- Cerchiamo α tale che $7^\alpha \cdot 26$ si fattorizza in primi piccoli
- Ricaviamo $\log_7(26)$

$7^2 \equiv 49 \equiv 8 = 2^3 \bmod 41$, perciò $2 = 3\log_7(2)$

quindi $\log_7(2) \equiv 2/3 \equiv 14 \bmod 40$

$7^{32} \equiv 10 \equiv 2 \cdot 5 \bmod 41$, perciò $32 = \log_7(2) + \log_7(5)$

quindi $\log_7(5) \equiv 32 - \log_7(2) \equiv 18 \bmod 40$

$7^{21} \equiv 34 \equiv 2 \cdot 17 \bmod 41$, primo grande

$7^{13} \equiv 12 \equiv 2^2 \cdot 3 \bmod 41$, perciò $13 = 2\log_7(2) + \log_7(3)$

quindi $\log_7(3) \equiv 13 - 2\log_7(2) \equiv 25 \bmod 40$

Abbiamo

$\log_7(2) \equiv 14 \bmod 40, \quad \log_7(3) \equiv 25 \bmod 40, \quad \log_7(5) \equiv 18 \bmod 40$

Vogliamo

α tale che $7^\alpha \cdot 26$ abbia fattori primi $2, 3, 5$

$7^{18} \cdot 26 \equiv 7$

$7^{21} \cdot 26 \equiv 23$

$7^{12} \cdot 26 \equiv 27 \equiv 3^3$, quindi

$$12\log_7(7) + \log_7(26) \equiv 3\log_7(3) \bmod 40$$

$$\log_7(26) \equiv 12 - 3 \cdot 25 \equiv 23 \bmod 40$$

Costo

Il calcolo dell'indice è ancora troppo lento, se p ha almeno un migliaio di cifre.

Esercizio

- Vogliamo ora calcolare $\log_2(42 \bmod 101)$ e $\log_2(91 \bmod 101)$
- Calcoliamo le potenze di 2 mod 101 in modo da ottenere relazioni lineari $\bmod 100$ da cui ricavare $\log_2(3), \log_2(5), \log_2(7)$.
- Poiché $42 = 2 \cdot 3 \cdot 7$ abbiamo che $\log_2(42) = \ldots$
- $91 = 7 \cdot 13$ e non conosciamo $\log_2(13)$, quindi calcoliamo $2^\alpha \cdot 91$ con α casuale in modo da ottenere una fattorizzazione in primi piccoli.