Cifrare messaggi dividendo con il resto: Congruenze modulari e RSA

Matteo Misurati

University of Ferrara

Stage di Matematica 2024, 14 Luglio

Il problema del nascondere i messaggi

(Crittografia vs. Steganografia)

Crittografia

- Il messaggio da nascondere viene alterato attraverso una procedura reversibile, rendendolo illeggibile.

Il problema del nascondere i messaggi

(Crittografia vs. Steganografia)

Crittografia

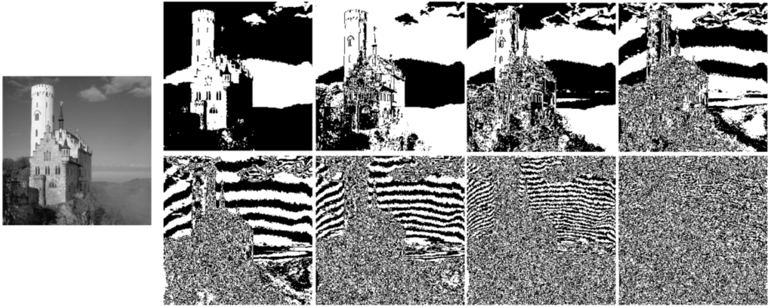
- Il messaggio da nascondere viene alterato attraverso una procedura reversibile, rendendolo illeggibile.

Steganografia

- L'esistenza stessa del messaggio viene nascosta.
- Il messaggio viene nascosto all'interno di qualche altra informazione

Esempio di steganografia

É possibile nascondere dei messaggi alterando il bit meno significativo di un'immagine digitale.



Rappresentazione dei bit via via meno significativi di un'immagine in bianco e nero. Ogni pixel è determinato da 1 byte, ossia 8 bit. E.g. 0010 1010

Oggi ci concentreremo sulla crittografia.

Come cifrare un messaggio

- Si suddivide il messaggio da cifrare in blocchi, composti da unità fondamentali.

Come cifrare un messaggio

- Si suddivide il messaggio da cifrare in blocchi, composti da unità fondamentali.
- Ad esempio, le unità possono essere singole lettere o, nel caso di messaggi digitali, bit, byte o gruppi di byte.

Come cifrare un messaggio

- Si suddivide il messaggio da cifrare in blocchi, composti da unità fondamentali.
- Ad esempio, le unità possono essere singole lettere o, nel caso di messaggi digitali, bit, byte o gruppi di byte.
- Il cifrario agisce su ogni blocco in modo indipendente dagli altri blocchi.

Come cifrare un messaggio

- Si suddivide il messaggio da cifrare in blocchi, composti da unità fondamentali.
- Ad esempio, le unità possono essere singole lettere o, nel caso di messaggi digitali, bit, byte o gruppi di byte.
- Il cifrario agisce su ogni blocco in modo indipendente dagli altri blocchi.
- Su un blocco si possono applicare due trasformazioni: la *sostituzione* o la *trasposizione*.

Come cifrare un messaggio

- Si suddivide il messaggio da cifrare in blocchi, composti da unità fondamentali.
- Ad esempio, le unità possono essere singole lettere o, nel caso di messaggi digitali, bit, byte o gruppi di byte.
- Il cifrario agisce su ogni blocco in modo indipendente dagli altri blocchi.
- Su un blocco si possono applicare due trasformazioni: la *sostituzione* o la *trasposizione*.
- Entrambe le operazioni possono dipendere o meno da *chiavi di cifratura*.

Sostituzione Vs. Trasposizione

- **La trasposizione**: opera una *permutazione* tra le unità del blocco; queste rimangono le stesse, ma il loro ordine è alterato.

Sostituzione Vs. Trasposizione

- **La trasposizione**: opera una *permutazione* tra le unità del blocco; queste rimangono le stesse, ma il loro ordine è alterato.
- **La sostituzione**: trasforma ciascun blocco in un blocco formato da elementi diversi rispetto a quelli originali.

Sostituzione Vs. Trasposizione

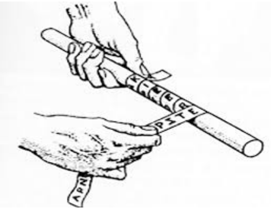
- **La trasposizione**: opera una *permutazione* tra le unità del blocco; queste rimangono le stesse, ma il loro ordine è alterato.
- **La sostituzione**: trasforma ciascun blocco in un blocco formato da elementi diversi rispetto a quelli originali.

Sostituzione Vs. Trasposizione

- **La trasposizione**: opera una *permutazione* tra le unità del blocco; queste rimangono le stesse, ma il loro ordine è alterato.
- **La sostituzione**: trasforma ciascun blocco in un blocco formato da elementi diversi rispetto a quelli originali.

Vediamo adesso esempi per ciascuna operazione, presi dall'antichità.

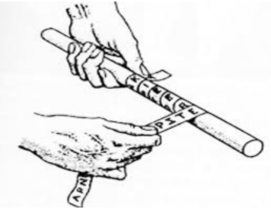
Esempio: la Scitala



La scitala è un cifrario che agisce per **trasposizione**.

- Secondo la tradizione, è un sistema di cifratura di messaggi, utilizzato da generali e magistrati spartani.

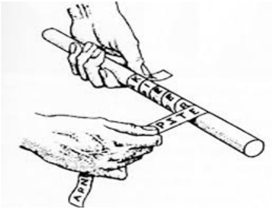
Esempio: la Scitala



La scitala è un cifrario che agisce per **trasposizione**.

- Secondo la tradizione, è un sistema di cifratura di messaggi, utilizzato da generali e magistrati spartani.
- Una stricia di pergamena lunga e stretta viene avvolta attorno a un bastone con un diametro specifico.

Esempio: la Scitala



La scitala è un cifrario che agisce per **trasposizione**.

- Secondo la tradizione, è un sistema di cifratura di messaggi, utilizzato da generali e magistrati spartani.
- Una stricia di pergamena lunga e stretta viene avvolta attorno a un bastone con un diametro specifico.
- Viene quindi scritto un messaggio sulla pergamena. Solo chi possiede un bastone dello stesso diametro del bastone originale può leggere il messaggio.

Esempio: la Scitala

Possiamo visualizzare il funzionamento del cifrario utilizzando una tabella. Proviamo a cifrare la parola *Debugging*.

		D	E	B		
		U	G	G		
		I	N	G		

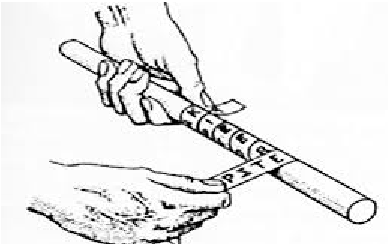
Esempio: la Scitala

Possiamo visualizzare il funzionamento del cifrario utilizzando una tabella. Proviamo a cifrare la parola *Debugging*.

		D	E	B		
		U	G	G		
		I	N	G		

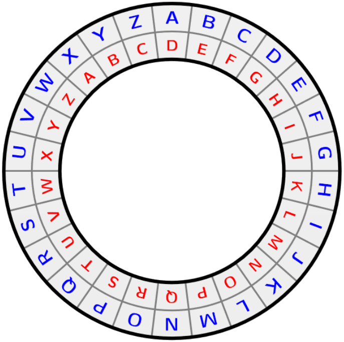
"Srotolando" la striscia di pergamena, rappresentata dalle colonne della tabella, otteniamo il messaggio cifrato:

...	D	U	I	...	E	G	N	...	B	G	G	...



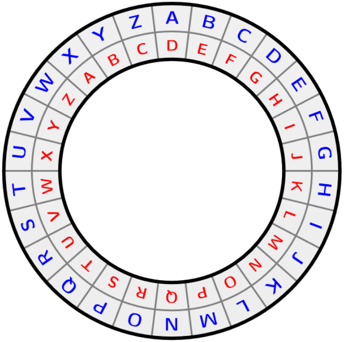
Esempio: il cifrario di Cesare

Un esempio di cifrario che opera per **sostituzione** è il cifrario di Cesare: ciascuna delle lettere viene sostituita dall'n-esima lettera successiva, con n tra 1 e 25, considerando A come la lettera successiva alla Z.



Esempio: il cifrario di Cesare

Un esempio di cifrario che opera per **sostituzione** è il cifrario di Cesare: ciascuna delle lettere viene sostituita dall'n-esima lettera successiva, con n tra 1 e 25, considerando A come la lettera successiva alla Z.



Ecco un esempio di utilizzo del cifrario di Cesare, partendo da una "rotazione" di 3 posizioni:

IACTA ALEA EST

$\downarrow$

LDFWD DOHD HVW

Monoalfabetico vs. Polialfabetico

Il cifrario di Cesare è detto monoalfabetico.

- **Cifrari monoalfabetici:** all'interno di uno stesso blocco, la stessa unità viene trasformata sempre nello stesso modo.

Monoalfabetico vs. Polialfabetico

Il cifrario di Cesare è detto monoalfabetico.

- **Cifrari monoalfabetici:** all'interno di uno stesso blocco, la stessa unità viene trasformata sempre nello stesso modo.
- **Cifrari polialfabetici:** all'interno dello stesso blocco due unità uguali possono essere trasformate in modo diverso.

Monoalfabetico vs. Polialfabetico

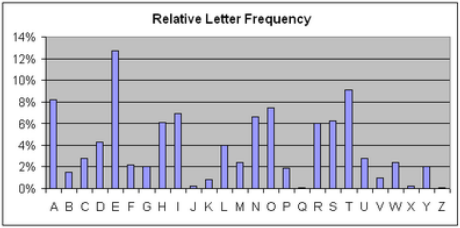
Il cifrario di Cesare è detto monoalfabetico.

- **Cifrari monoalfabetici:** all'interno di uno stesso blocco, la stessa unità viene trasformata sempre nello stesso modo.
- **Cifrari polialfabetici:** all'interno dello stesso blocco due unità uguali possono essere trasformate in modo diverso.

I cifrari monoalfabetici hanno una debolezza fondamentale:

Analisi delle frequenze

- Viene sviluppata nei paesi arabi nel corso dell'800.
- Viene applicata in ambito crittografico per la prima volta da al-Kindi (801-873).
- Consiste nel calcolare la frequenza di determinate lettere in una determinata lingua, e nel confrontare le percentuali ottenute con la frequenza dei simboli in un testo cifrato.
- Permette di violare ogni cifrario monoalfabetico, ma è utile per analizzare anche cifrari più complessi.



Frequenza delle varie lettere nella lingua Inglese.

Cifrari polialfabetici

- Sviluppati per avere una cifratura resistente all'analisi delle frequenze.

Cifrari polialfabetici

- Sviluppati per avere una cifratura resistente all'analisi delle frequenze.
- L'idea della sostituzione polialfabetica nasce nel 1466 per mano di Battista Alberti.
- Una versione migliorata del disco cifrante di Alberti passerà alla storia come cifrario di Vigenère.

Cifrari polialfabetici

- Sviluppati per avere una cifratura resistente all'analisi delle frequenze.
- L'idea della sostituzione polialfabetica nasce nel 1466 per mano di Battista Alberti.
- Una versione migliorata del disco cifrante di Alberti passerà alla storia come cifrario di Vigenère.
- Il cifrario usa una chiave di cifratura per criptare e decriptare i messaggi.

Cifrari polialfabetici

- Sviluppati per avere una cifratura resistente all'analisi delle frequenze.
- L'idea della sostituzione polialfabetica nasce nel 1466 per mano di Battista Alberti.
- Una versione migliorata del disco cifrante di Alberti passerà alla storia come cifrario di Vigenère.
- Il cifrario usa una chiave di cifratura per criptare e decriptare i messaggi.
- Rimarrà inviolato fino alla seconda metà del diciannovesimo secolo.

Congruenze modulari

M.Misurati

Cifrario di Vigenère 1

Guardiamo insieme come funziona il cifrario di Vigenère, cifrando la parola "BOZZOLO" usando "POI" come chiave.

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

B	O	Z	Z	O	L	O
P	O	I	P	O	I	P

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

B	O	Z	Z	O	L	O
P	O	I	P	O	I	P
Q	C	H	O	C	T	D

L'importanza della chiave

- Non è possibile decifrare un messaggio cifrato con il cifrario di Vigenère con un'analisi delle frequenze semplice.

L'importanza della chiave

- Non è possibile decifrare un messaggio cifrato con il cifrario di Vigenère con un'analisi delle frequenze semplice.
- É comunque possibile forzare il cifrario di Vigenère se il messaggio è molto più lungo della chiave.

L'importanza della chiave

- Non è possibile decifrare un messaggio cifrato con il cifrario di Vigenère con un'analisi delle frequenze semplice.
- É comunque possibile forzare il cifrario di Vigenère se il messaggio è molto più lungo della chiave.
- Intuita la lunghezza della chiave, si considerano le lettere associate a ogni lettera della chiave come un messaggio a sé, poi si usa l'analisi delle frequenze.

L'importanza della chiave

- Non è possibile decifrare un messaggio cifrato con il cifrario di Vigenère con un'analisi delle frequenze semplice.
- É comunque possibile forzare il cifrario di Vigenère se il messaggio è molto più lungo della chiave.
- Intuita la lunghezza della chiave, si considerano le lettere associate a ogni lettera della chiave come un messaggio a sé, poi si usa l'analisi delle frequenze.
- Questo attacco non è possibile se la chiave è lunga quanto il messaggio.

L'importanza della chiave

- Non è possibile decifrare un messaggio cifrato con il cifrario di Vigenère con un'analisi delle frequenze semplice.
- É comunque possibile forzare il cifrario di Vigenère se il messaggio è molto più lungo della chiave.
- Intuita la lunghezza della chiave, si considerano le lettere associate a ogni lettera della chiave come un messaggio a sé, poi si usa l'analisi delle frequenze.
- Questo attacco non è possibile se la chiave è lunga quanto il messaggio.
- Altre debolezze, per motivi analoghi, si verificano se la chiave non è casuale o la chiave viene utilizzata per cifrare più messaggi.

Cifrario di Vernam

Il cifrario di Vernam (1917), detto anche OTP (One Time Password) si ottiene imponendo le seguenti condizioni sul cifrario di Vigenère:

Cifrario di Vernam

Il cifrario di Vernam (1917), detto anche OTP (One Time Password) si ottiene imponendo le seguenti condizioni sul cifrario di Vigenère:

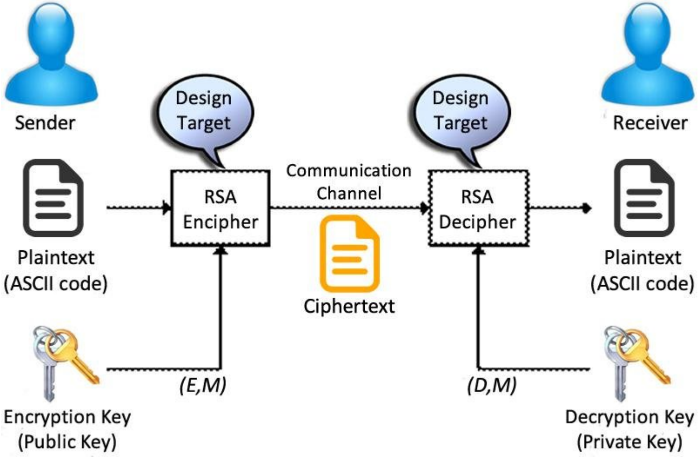
- La chiave deve essere lunga come il messaggio.
- La chiave deve essere casuale.
- La chiave deve essere usata una volta sola.

Problema della distribuzione delle password 1

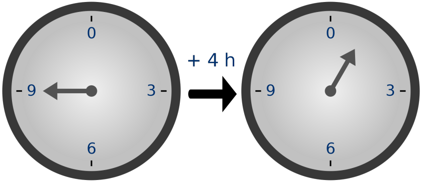
Una soluzione: macchine cifranti

Problema della distribuzione delle password 2

Un'altra soluzione: cifrari a chiave pubblica, tra i quali l'RSA (1977: R. Rivest, A. Shamir, L. Adleman).

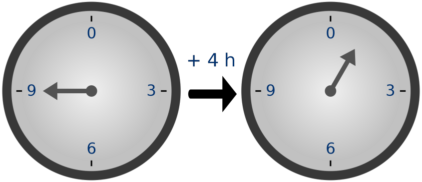


Aritmetica modulare 1



Proviamo a ragionare matematicamente su cosa succede quando pensiamo alle ore di una giornata su un orologio.

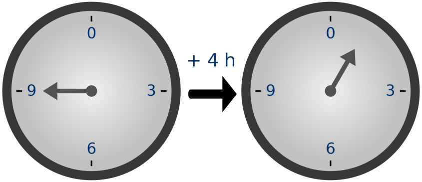
Aritmetica modulare 1



Proviamo a ragionare matematicamente su cosa succede quando pensiamo alle ore di una giornata su un orologio.

- Alcune coppie di ore sono rappresentate nello stesso modo: e.g. 10 e 22, 7 e 19 o 2 e 14.

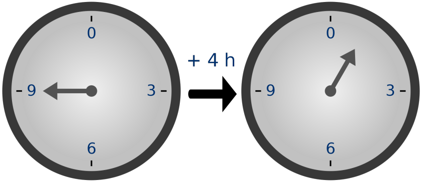
Aritmetica modulare 1



Proviamo a ragionare matematicamente su cosa succede quando pensiamo alle ore di una giornata su un orologio.

- Alcune coppie di ore sono rappresentate nello stesso modo: e.g. 10 e 22, 7 e 19 o 2 e 14.
- Mandando avanti l'orologio di n ore, si ottiene sempre un numero tra 0 e 11, i numeri "girano", al posto di avanzare.

Aritmetica modulare 1



Proviamo a ragionare matematicamente su cosa succede quando pensiamo alle ore di una giornata su un orologio.

- Alcune coppie di ore sono rappresentate nello stesso modo: e.g. 10 e 22, 7 e 19 o 2 e 14.
- Mandando avanti l'orologio di n ore, si ottiene sempre un numero tra 0 e 11, i numeri "girano", al posto di avanzare.
- Cosa regola matematicamente queste proprietà? Due ore sono rappresentate nello stesso modo su un orologio se e solo se, divise per 12, danno lo stesso resto.

Aritmetica modulare 2

$$10 = 0 \cdot 12 + 10 \quad \text{e} \quad 22 = 1 \cdot 12 + 10$$

In linguaggio matematico, diciamo che 10 e 22 sono congrui modulo 12; in notazione:

$$10 \equiv 22 \pmod{12}$$

Aritmetica modulare 2

$$10 = 0 \cdot 12 + 10 \quad \text{e} \quad 22 = 1 \cdot 12 + 10$$

In linguaggio matematico, diciamo che 10 e 22 sono congrui modulo 12; in notazione:

$$10 \equiv 22 \pmod{12}$$

In generale, diciamo che, dati tre numeri interi a,b e n, a e b sono congrui modulo n se n divide $a - b$.

Aritmetica modulare 2

$$10 = 0 \cdot 12 + 10 \quad \text{e} \quad 22 = 1 \cdot 12 + 10$$

In linguaggio matematico, diciamo che 10 e 22 sono congrui modulo 12; in notazione:

$$10 \equiv 22 \pmod{12}$$

In generale, diciamo che, dati tre numeri interi a,b e n, a e b sono congrui modulo n se n divide $a - b$.
Si può dimostrare che:

$$r_a = r_b \text{ se e solo se } n \text{ divide } a - b$$

Aritmetica modulare 3

Guardiamo qualche esempio:

- $15 \equiv 7 \pmod 2$
- $4 \equiv 29 \equiv -1 \pmod 5$
- $3 \equiv 103 \equiv 1003 \pmod{100}$

Aritmetica modulare 3

Guardiamo qualche esempio:

- $15 \equiv 7 \pmod 2$
- $4 \equiv 29 \equiv -1 \pmod 5$
- $3 \equiv 103 \equiv 1003 \pmod{100}$

Guardiamo qualche proprietà:

- $a = b \implies a \equiv b \pmod n$
- $100 \equiv 4 \cdot 21 + 16 \equiv 4 \cdot 0 + 16 \equiv 16 \pmod{21}$
- $-3 \equiv 0 - 3 \equiv 7 - 3 \equiv 4 \pmod 7$
- $3x \equiv 1 \pmod 7 \iff x \equiv 3^{-1} \equiv 5 \pmod 7$, poiché 3 e 7 sono coprimi

Algoritmo euclideo esteso 1

- In genere, quando vogliamo calcolare il massimo comune divisore tra due numeri interi, procediamo in questo modo:
- scomponiamo i due numeri in fattori primi $\rightarrow$ scegliamo i fattori comuni, con l'esponente più basso.
- $24 = 2^3 \cdot 3,\ 30 = 2 \cdot 3 \cdot 5 \quad \longrightarrow \quad \mathrm{MCD}(24, 30) = 6$

Algoritmo euclideo esteso 1

- In genere, quando vogliamo calcolare il massimo comune divisore tra due numeri interi, procediamo in questo modo:
- scomponiamo i due numeri in fattori primi $\rightarrow$ scegliamo i fattori comuni, con l'esponente più basso.
- $24 = 2^3 \cdot 3$, $30 = 2 \cdot 3 \cdot 5 \quad \longrightarrow \quad \mathrm{MCD}(24, 30) = 6$

Tuttavia, questo approccio è inadatto a calcolare il massimo comune divisore tra numeri molto grandi.
Scomporre numeri grandi in fattori primi in modo efficiente è un problema difficile da risolvere!

$$\mathrm{MCD}(699870, 4935) = ???$$

Algoritmo euclideo esteso 1

- In genere, quando vogliamo calcolare il massimo comune divisore tra due numeri interi, procediamo in questo modo:
- scomponiamo i due numeri in fattori primi $\rightarrow$ scegliamo i fattori comuni, con l'esponente più basso.
- $24 = 2^3 \cdot 3$, $30 = 2 \cdot 3 \cdot 5 \quad \longrightarrow \quad \mathrm{MCD}(24, 30) = 6$

Tuttavia, questo approccio è inadatto a calcolare il massimo comune divisore tra numeri molto grandi.
Scomporre numeri grandi in fattori primi in modo efficiente è un problema difficile da risolvere!

$$\mathrm{MCD}(699870, 4935) = ???$$

L'algoritmo si basa sulla seguente importante proprietà: se la divisione tra a e b da resto r, allora

$$MCD(a, b) = MCD(b, r)$$

Algoritmo euclideo esteso 2

L'algoritmo euclideo risolve questo problema, permettendo di calcolare il massimo comune divisore in modo efficiente, bypassando la necessità di scomporre in fattori primi.

Algoritmo euclideo esteso 2

L'algoritmo euclideo risolve questo problema, permettendo di calcolare il massimo comune divisore in modo efficiente, bypassando la necessità di scomporre in fattori primi.

- Supponiamo di voler trovare il MCD tra due interi a e b.

Algoritmo euclideo esteso 2

L'algoritmo euclideo risolve questo problema, permettendo di calcolare il massimo comune divisore in modo efficiente, bypassando la necessità di scomporre in fattori primi.

- Supponiamo di voler trovare il MCD tra due interi a e b.
- L'algoritmo costruisce una sequenza decrescente finita di numeri interi partendo da a e b:
  $r_0 = a,\ r_1 = b,\ r_2, \dots,\ r_{n-1},\ r_n,\ r_{n+1} = 0.$

Algoritmo euclideo esteso 2

L'algoritmo euclideo risolve questo problema, permettendo di calcolare il massimo comune divisore in modo efficiente, bypassando la necessità di scomporre in fattori primi.

- Supponiamo di voler trovare il MCD tra due interi a e b.
- L'algoritmo costruisce una sequenza decrescente finita di numeri interi partendo da a e b:
  $r_0 = a,\ r_1 = b,\ r_2, \dots,\ r_{n-1},\ r_n,\ r_{n+1} = 0.$
- La successione termina quanto viene raggiunto lo $0 = r_{n+1}$: r_n è il massimo comune divisore tra a e b.

Algoritmo euclideo esteso 2

L'algoritmo euclideo risolve questo problema, permettendo di calcolare il massimo comune divisore in modo efficiente, bypassando la necessità di scomporre in fattori primi.

- Supponiamo di voler trovare il MCD tra due interi a e b.
- L'algoritmo costruisce una sequenza decrescente finita di numeri interi partendo da a e b:
  $r_0 = a,\ r_1 = b,\ r_2, \ldots,\ r_{n-1},\ r_n,\ r_{n+1} = 0.$
- La successione termina quanto viene raggiunto lo $0 = r_{n+1}$: r_n è il massimo comune divisore tra a e b.
- Oltre a generare la successione, l'algoritmo costruisce anche due coefficienti interi, x e y, tali che

$$x \cdot a + y \cdot b = \mathrm{MCD}(a, b)$$

  questa uguaglianza è nota come l'Identità di Bézout, ed è alla base di molti risultati nell'aritmetica modulare.

Algoritmo euclideo esteso 3

Vediamo ora come l'algoritmo euclideo produce la sequenza $r_0, r_1, r_2, \ldots, \ r_{n-1}, \ r_n, \ r_{n+1} = 0$ partendo da due interi a e b.

- $r_0 = a$ e $r_1 = b$ (Non importa l'ordine!)

Algoritmo euclideo esteso 3

Vediamo ora come l'algoritmo euclideo produce la sequenza $r_0, r_1, r_2, \ldots, \ r_{n-1}, \ r_n, \ r_{n+1} = 0$ partendo da due interi a e b.

- $r_0 = a$ e $r_1 = b$ (Non importa l'ordine!)
- Ogni r_i, con $i \geq 2$, si ottiene come resto nella divisione tra r_{i-2} e r_{i-1}:

$$r_{i-2} = q_i \cdot r_{i-1} + r_i$$

Algoritmo euclideo esteso 3

Vediamo ora come l'algoritmo euclideo produce la sequenza $r_0, r_1, r_2, \dots, \ r_{n-1}, \ r_n, \ r_{n+1} = 0$ partendo da due interi a e b.

- $r_0 = a$ e $r_1 = b$ (Non importa l'ordine!)
- Ogni r_i, con $i \geq 2$, si ottiene come resto nella divisione tra r_{i-2} e r_{i-1}:

$$r_{i-2} = q_i \cdot r_{i-1} + r_i$$

- "Riordinando" queste divisioni con il resto, si ricava l'identità di Bézout

$$x \cdot r_0 + y \cdot r_1 = \mathrm{MCD}(r_0, r_1)$$

Vediamo adesso qualche esempio.

Algoritmo euclideo: Esempio

Calcoliamo l'MCD e l'identità di Bézout tra 472 e 21 :

$$\begin{aligned} 472 &= 22 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 + 0 \end{aligned}$$

Abbiamo trovato che $\mathrm{MCD}(472, 21) = 1$.

Algoritmo euclideo: Esempio

Calcoliamo l'MCD e l'identità di Bézout tra 472 e 21 :

$$\begin{aligned} 472 &= 22 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 + 0 \end{aligned}$$

Abbiamo trovato che $\mathrm{MCD}(472, 21) = 1$.Inoltre:

$$\begin{aligned} 472 &= 22 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \end{aligned} \iff \begin{aligned} 472 - 22 \cdot 21 &= 10 \\ 21 - 2 \cdot 10 &= 1 \end{aligned}$$

Algoritmo euclideo: Esempio

Calcoliamo l'MCD e l'identità di Bézout tra 472 e 21 :

$$\begin{aligned} 472 &= 22 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 + 0 \end{aligned}$$

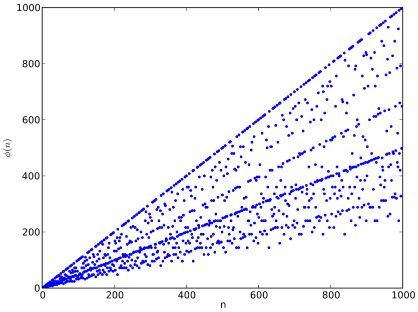
Abbiamo trovato che $\mathrm{MCD}(472, 21) = 1$.Inoltre:

$$\begin{aligned} 472 &= 22 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \end{aligned} \iff \begin{aligned} 472 - 22 \cdot 21 &= 10 \\ 21 - 2 \cdot 10 &= 1 \end{aligned}$$

sostituendo, otteniamo l'identità di Bézout:

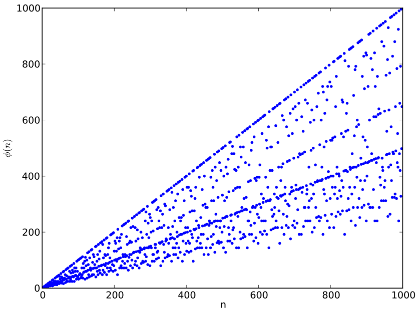
$$\begin{aligned} 1 &= 21 - 2 \cdot 10 = 21 - 2 \cdot (472 - 22 \cdot 21) \\ &= 21 - 2 \cdot 472 + 44 \cdot 21 = 45 \cdot 21 - 2 \cdot 472 \end{aligned}$$

La funzione φ di Eulero



- La funzione $\varphi(n)$ di Eulero conta i numeri tra 1 e n (estremi compresi) che sono primi con n.

La funzione φ di Eulero



- La funzione $\varphi(n)$ di Eulero conta i numeri tra 1 e n (estremi compresi) che sono primi con n.
- Se p è un numero primo, ogni numero tra 1 e $p-1$ non avrà fattori in comune con p. Quindi avremo $\varphi(p) = p - 1$.

La funzione φ di Eulero: proprietà

- La funzione di Eulero è moltiplicativa su numeri primi fra loro. Ciò significa che, dati p e q tali che $\mathrm{MCD}(p, q) = 1$, allora

$$\varphi(pq) \; = \; \varphi(p)\varphi(q).$$

La funzione φ di Eulero: proprietà

- La funzione di Eulero è moltiplicativa su numeri primi fra loro. Ciò significa che, dati p e q tali che $\mathrm{MCD}(p, q) = 1$, allora
$$\varphi(pq) = \varphi(p)\varphi(q).$$
- Questo ci permette di calcolare la funzione di Eulero su ogni intero positivo.

La funzione φ di Eulero: proprietà

- La funzione di Eulero è moltiplicativa su numeri primi fra loro. Ciò significa che, dati p e q tali che $\mathrm{MCD}(p, q) = 1$, allora
$$\varphi(pq) = \varphi(p)\varphi(q).$$
- Questo ci permette di calcolare la funzione di Eulero su ogni intero positivo.
- Ad esempio, proviamo a calcolare il valore di φ su un numero composito:
$$\begin{aligned}\varphi(30) &= \varphi(2 \cdot 3 \cdot 5) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \\ &= (2-1) \cdot (3-1) \cdot (5-1) = 8,\end{aligned}$$
questi otto numeri sono $\{1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29\}$.

Il teorema di Eulero

Teorema

Siano n e a due interi positivi primi fra loro. Allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Il teorema di Eulero

Teorema

Siano n e a due interi positivi primi fra loro. Allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- Questo teorema ci permette di calcolare le potenze modulo un certo numero.

Il teorema di Eulero

Teorema

Siano n e a due interi positivi primi fra loro. Allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- Questo teorema ci permette di calcolare le potenze modulo un certo numero.
- Ci chiediamo quale sia l'ultima cifra di 3^{111}. Allora, applicando il teorema di Eulero, con $\varphi(10) = 4$:

$$\begin{aligned} 3^{111} \equiv& 3^{27\cdot4+3} \equiv (3^{27})^4 3^3 \equiv (3^{27})^{\varphi(10)} 27 \\ \equiv& 27 \equiv 20 + 7 \equiv 7 \pmod{10} \end{aligned}$$

Cifrario RSA

Ora abbiamo tutti gli ingredienti per tornare alla crittografia.

- Il cifrario RSA, introdotto nel 1977, risolve il problema di distribuzione delle chiavi, facendo uso di una chiave pubblica e una privata.

Cifrario RSA

Ora abbiamo tutti gli ingredienti per tornare alla crittografia.

- Il cifrario RSA, introdotto nel 1977, risolve il problema di distribuzione delle chiavi, facendo uso di una chiave pubblica e una privata.
- Poiché le chiavi hanno un ruolo simmetrico, il cifrario può essere usato sia per cifrare messaggi che come firma digitale.

Cifrario RSA

Ora abbiamo tutti gli ingredienti per tornare alla crittografia.

- Il cifrario RSA, introdotto nel 1977, risolve il problema di distribuzione delle chiavi, facendo uso di una chiave pubblica e una privata.
- Poiché le chiavi hanno un ruolo simmetrico, il cifrario può essere usato sia per cifrare messaggi che come firma digitale.
- Si basa sulla difficoltà di fattorizzare un numero molto grande, senza conoscere i suoi fattori primi.

Costruire il cifrario RSA

- Scegliamo in segreto due numeri primi molto grandi p e q (i più grandi possono essere lunghi anche 300 cifre!)

Costruire il cifrario RSA

- Scegliamo in segreto due numeri primi molto grandi p e q (i più grandi possono essere lunghi anche 300 cifre!)
- Calcoliamo $n = pq$ e $\varphi(n) = (p-1)(q-1)$.

Costruire il cifrario RSA

- Scegliamo in segreto due numeri primi molto grandi p e q (i più grandi possono essere lunghi anche 300 cifre!)
- Calcoliamo $n = pq$ e $\varphi(n) = (p-1)(q-1)$.
- Scegliamo un numero e più piccolo di $\varphi(n)$ e coprimo con $\varphi(n)$.

Costruire il cifrario RSA

- Scegliamo in segreto due numeri primi molto grandi p e q (i più grandi possono essere lunghi anche 300 cifre!)
- Calcoliamo $n = pq$ e $\varphi(n) = (p-1)(q-1)$.
- Scegliamo un numero e più piccolo di $\varphi(n)$ e coprimo con $\varphi(n)$.
- Utilizzando l'algoritmo euclideo esteso, calcoliamo l'identità di Bézout tra e e $\varphi(n)$

$$1 = d \cdot e + \lambda \cdot \varphi(n)$$

ottenendo l'intero d.

Costruire il cifrario RSA

- Scegliamo in segreto due numeri primi molto grandi p e q (i più grandi possono essere lunghi anche 300 cifre!)
- Calcoliamo $n = pq$ e $\varphi(n) = (p-1)(q-1)$.
- Scegliamo un numero e più piccolo di $\varphi(n)$ e coprimo con $\varphi(n)$.
- Utilizzando l'algoritmo euclideo esteso, calcoliamo l'identità di Bézout tra e e $\varphi(n)$

$$1 = d \cdot e + \lambda \cdot \varphi(n)$$

  ottenendo l'intero d.
- La coppia (n, e) è la chiave pubblica, che viene distribuita apertamente. (n, d) è la chiave privata.

Il funzionamento del cifrario RSA

Bob conosce la chiave pubblica (n, e) di Alice, e vuole mandarle un messaggio $0 \leq m \leq n - 1$.

- Bob usa la chiave pubblica di Alice per cifrare il messaggio m e calcola c, il resto modulo n della potenza m^e

$$c \equiv m^e \pmod{n}.$$

Il funzionamento del cifrario RSA

Bob conosce la chiave pubblica (n, e) di Alice, e vuole mandarle un messaggio $0 \leq m \leq n - 1$.

- Bob usa la chiave pubblica di Alice per cifrare il messaggio m e calcola c, il resto modulo n della potenza m^e

$$c \equiv m^e \pmod{n}.$$

- Bob invia ad Alice il messaggio cifrato c.

Il funzionamento del cifrario RSA

Bob conosce la chiave pubblica (n, e) di Alice, e vuole mandarle un messaggio $0 \leq m \leq n - 1$.

- Bob usa la chiave pubblica di Alice per cifrare il messaggio m e calcola c, il resto modulo n della potenza m^e

$$c \equiv m^e \pmod{n}.$$

- Bob invia ad Alice il messaggio cifrato c.
- Alice riceve il messaggio cifrato c da Bob e usa la sua chiave privata per calcolare il resto modulo n di c^d, che risulta essere m.

Il funzionamento del cifrario RSA

Bob conosce la chiave pubblica (n, e) di Alice, e vuole mandarle un messaggio $0 \leq m \leq n-1$.

- Bob usa la chiave pubblica di Alice per cifrare il messaggio m e calcola c, il resto modulo n della potenza m^e

$$c \equiv m^e \pmod{n}.$$

- Bob invia ad Alice il messaggio cifrato c.
- Alice riceve il messaggio cifrato c da Bob e usa la sua chiave privata per calcolare il resto modulo n di c^d, che risulta essere m.

Infatti, poiché $1 = de + \lambda\varphi(n)$:

$$c^d \equiv m^{de} \equiv m^{1-\lambda\varphi(n)} \equiv m(m^{-\lambda})^{\varphi(n)} \equiv m \pmod{n}$$

per il teorema di Euclide (ammesso che m sia primo con n).

RSA: esempio 1

Guardiamo un esempio (giocattolo) per capire meglio il funzionamento del cifrario.
Come prima cosa, mettiamoci nei panni di Alice e costruiamo la chiave pubblica e la chiave privata.

RSA: esempio 1

Guardiamo un esempio (giocattolo) per capire meglio il funzionamento del cifrario.
Come prima cosa, mettiamoci nei panni di Alice e costruiamo la chiave pubblica e la chiave privata.

- Alice sceglie due numeri primi: 37 e 29.

RSA: esempio 1

Guardiamo un esempio (giocattolo) per capire meglio il funzionamento del cifrario.
Come prima cosa, mettiamoci nei panni di Alice e costruiamo la chiave pubblica e la chiave privata.

- Alice sceglie due numeri primi: 37 e 29.
- Alice calcola $n = 37 \cdot 29 = 1073$ e $\varphi(1073) = 36 \cdot 28 = 1008$.

RSA: esempio 1

Guardiamo un esempio (giocattolo) per capire meglio il funzionamento del cifrario.
Come prima cosa, mettiamoci nei panni di Alice e costruiamo la chiave pubblica e la chiave privata.

- Alice sceglie due numeri primi: 37 e 29.
- Alice calcola $n = 37 \cdot 29 = 1073$ e $\varphi(1073) = 36 \cdot 28 = 1008$.
- Sceglie $e = 5$, minore e primo rispetto a $\varphi(1073) = 1008$.

RSA: esempio 2

$n = 1073 (= 37 \cdot 29)$, $\varphi(n) = 1008$, $e = 5$.

- Calcola l'identità di Bézout tra 23 e 1008:

$$1008 = 201 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

$$\begin{aligned} 1 = 3 - 2 &= 3 - 5 + 3 = 2 \cdot 3 - 5 \\ &= 2(1008 - 201 \cdot 5) - 5 \\ &= 2 \cdot 1008 - 403 \cdot 5 \end{aligned}$$

ottenendo la chiave privata (n, d), con $d = -403$.

Alice comunica a tutti che la sua chiave pubblica è $(n, e) = (1073, 5)$.

RSA: esempio 3

Mettiamoci adesso nei panni di Bob, che vuole mandare segretamente ad Alice il messaggio "HEI". La chiave pubblica di Alice è $(n, e) = (1073, 5)$.

RSA: esempio 3

Mettiamoci adesso nei panni di Bob, che vuole mandare segretamente ad Alice il messaggio "HEI". La chiave pubblica di Alice è $(n, e) = (1073, 5)$.

- Considerando solo le prime 9 lettere dell'alfabeto, usiamo la seguente tabella per convertire il messaggio di Bob in un numero

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9

- Abbiamo quindi "*HEI*" $\rightarrow$ $m = 859$.

RSA: esempio 3

Mettiamoci adesso nei panni di Bob, che vuole mandare segretamente ad Alice il messaggio "HEI". La chiave pubblica di Alice è $(n, e) = (1073, 5)$.

- Considerando solo le prime 9 lettere dell'alfabeto, usiamo la seguente tabella per convertire il messaggio di Bob in un numero

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9

- Abbiamo quindi "*HEI*" $\rightarrow$ $m = 859$.
- A questo punto Bob calcola c, il resto modulo n di m^e.

$$\begin{aligned} c &\equiv 859^e \equiv 859^5 \equiv 859(859^2)^2 \\ &\equiv 859(737,881)^2 \equiv 859(730)^2 \equiv 859 \cdot 692 \\ &\equiv 594428 \equiv 1059 \equiv -14 \pmod{1073} \end{aligned}$$

RSA: esempio 4

- Bob comunica ad Alice il suo messaggio cifrato, inviandole il numero $c = -14$.

RSA: esempio 4

- Bob comunica ad Alice il suo messaggio cifrato, inviandole il numero $c = -14$.
- Per decodificare il messaggio, Alice calcolerà c^d, modulo n:

$$
\begin{aligned}
c^d &\equiv (-14)^{-403} \equiv (-14)^{\varphi(n)}(-14)^{-403} \equiv (-14)^{1008-403} \\
&\equiv (-14)^{605} \equiv -14^{605} \equiv -14^{5\cdot 11^2} \equiv -(14^5)^{11^2} \\
&\equiv -(251^{11})^{11} \equiv -(578)^{11} \equiv -(578)^{11} \equiv -214 \\
&\equiv 1073 - 214 \equiv 859 \pmod{1073}.
\end{aligned}
$$

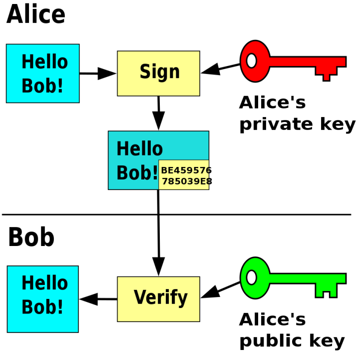
RSA: esempio 4

- Bob comunica ad Alice il suo messaggio cifrato, inviandole il numero $c = -14$.
- Per decodificare il messaggio, Alice calcolerà c^d, modulo n:

$$\begin{aligned} c^d &\equiv (-14)^{-403} \equiv (-14)^{\varphi(n)}(-14)^{-403} \equiv (-14)^{1008-403} \\ &\equiv (-14)^{605} \equiv -14^{605} \equiv -14^{5\cdot 11^2} \equiv -(14^5)^{11^2} \\ &\equiv -(251^{11})^{11} \equiv -(578)^{11} \equiv -(578)^{11} \equiv -214 \\ &\equiv 1073 - 214 \equiv 859 \pmod{1073}. \end{aligned}$$

- A questo punto, Alice ritrova il messaggio di Bob $m = 859$, che leggerà correttamente come "HEI", usando la tabella di prima.

Firma digitale



Il cifrario RSA può essere usato anche per permettere di verificare l'autenticità del mittente di un messaggio.

Firma digitale con RSA

Alice vuole inviare un messaggio a Bob, in modo che Bob sia sicuro della provenienza del messaggio.

Firma digitale con RSA

Alice vuole inviare un messaggio a Bob, in modo che Bob sia sicuro della provenienza del messaggio.

- Alice "firma" il suo messaggio m, cifrandolo con la sua chiave privata. Calcola $f \equiv m^d \ (mod\ n)$, poi invia f a Bob.

Firma digitale con RSA

Alice vuole inviare un messaggio a Bob, in modo che Bob sia sicuro della provenienza del messaggio.

- Alice "firma" il suo messaggio m, cifrandolo con la sua chiave privata. Calcola $f \equiv m^d \ (mod \ n)$, poi invia f a Bob.
- Bob riceve il messaggio da Alice, quindi lo decodifica usando la sua chiave pubblica, recuperando così m:

$$m \equiv f^e \ (mod \ n).$$

Poiché Bob riesce a leggere il messaggio, è sicuro venga proprio da Alice.

Firma digitale con RSA

Alice vuole inviare un messaggio a Bob, in modo che Bob sia sicuro della provenienza del messaggio.

- Alice "firma" il suo messaggio m, cifrandolo con la sua chiave privata. Calcola $f \equiv m^d \ (mod\ n)$, poi invia f a Bob.
- Bob riceve il messaggio da Alice, quindi lo decodifica usando la sua chiave pubblica, recuperando così m:

$$m \equiv f^e \ (mod\ n).$$

  Poiché Bob riesce a leggere il messaggio, è sicuro venga proprio da Alice.

- Questo funziona perché, nell'RSA, chiave pubblica e chiave privata hanno un ruolo simmetrico:

$$m^{de} \equiv m^{1-\lambda\varphi(n)} \equiv m \ (mod\ n).$$

Fine

Grazie per l'attenzione!

Ringrazio i professori Fabio Stumbo e Paolo Codecà per avere ispirato questa presentazione.

Quiz finale

Lo trovate seguendo il QR code: