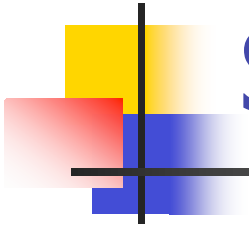
clic per iniziare...

- Anna Rita Strazioso
- Fabrizio Piacenza
- Valentina Ventriglia



Struttura

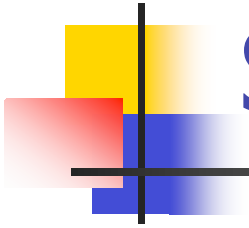
1) Introduzione:
   a cura di Fabrizio Piacenza
2) Generazione chiavi & Test di primalità:
   a cura di Anna Rita Strazioso
3) Cifratura & Decifratura con esempi:
   a cura di Valentina Ventriglia
4) Dimostrazione:
   a cura di Fabrizio Piacenza

Personaggi

Kyle (mittente)

Cartman (destinatario)

Dark (Crittoanalista)



Struttura

1) Introduzione:
   a cura di Fabrizio Piacenza
2) Generazione chiavi & Test di primalità:
   a cura di Anna Rita Strazioso
3) Cifratura & Decifratura con esempi:
   a cura di Valentina Ventriglia
4) Dimostrazione:
   a cura di Fabrizio Piacenza

Introduzione

- L'RSA nasce nel 1977 come acronimo dei cognomi dei loro inventori: Rivest-Shamir-Adleman
- È una svolta nella Crittologia essendo il primo cifrario a NON usare una chiave segreta e simmetrica ma una

CHIAVE PUBBLICA

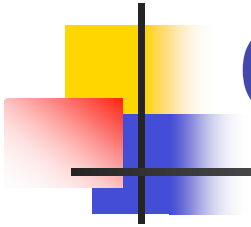
Perché tale necessità?

Lo scopo per cui è stato inventato questo metodo, è da ricercarsi nella difficoltà di comunicare la chiave privata di decrittazione al destinatario.

Chiave Privata VS Pubblica (1)

- Nei metodi a chiave simmetrica per comunicare la chiave è necessario accordarsi di persona con il destinatario incontrandosi in un luogo sicuro!!!
- O usare canali di comunicazione sicuri …

Ovvio però che se esistesse un canale di comunicazione sicuro non servirebbe neanche cifrare i messaggi!



Chiave Privata VS Pubblica (2)

- Con l'RSA si utilizza una chiave per la cifratura (pubblica), ma una chiave diversa per riportare il testo in chiaro (privata).
- La prima chiave può anche essere resa pubblica, dato che offre solo la possibilità di cifrare, ma non di decifrare il messaggio.

Proprietà fondamentale

L'RSA ha la sua forza nell'uso di una funzione unidirezionale (one-way) che sfrutta la fattorizzazione dei numeri

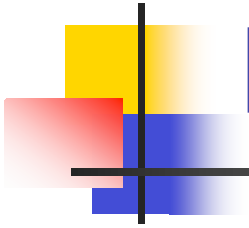
… cioè la cui funzione inversa sia difficilissima da calcolare!!!

Un po' di storia …

- Nel 1976 Diffie ed Hellmann per la prima volta proposero l'idea di una crittografia a chiave pubblica

Un matematico, Ron Rivest, prese sul serio quella proposta e con l'aiuto di Adi Shamir, e Leonard Adleman riuscì a definire un metodo che sfruttasse proprio la chiave pubblica …

RSA



Linea guida

Ogni utente del sistema ha una coppia di chiavi pubbliche che vengono pubblicate da un ente che ne garantisce l'autenticità tanto che ...

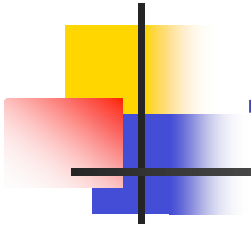
- RSA è usato come:
  - Cifratura (si cifra il msg con la chiave pubblica del destinatario)
  - Firma (si autentica il msg con la propria chiave privata)

Curiosità…

- Samuel Wagstaff, docente di informatica all'Università dell'Indiana, è riuscito a fattorizzare un numero di 167 cifre in centomila ore di tempo computer…

Il numero della prova era:

1637901955805366239217413015467044958
3923965684832704024983781709239694686
3513212041565096492260805419718247075
5579714456896907387777297303883717449030628887379284041



… possibilità …

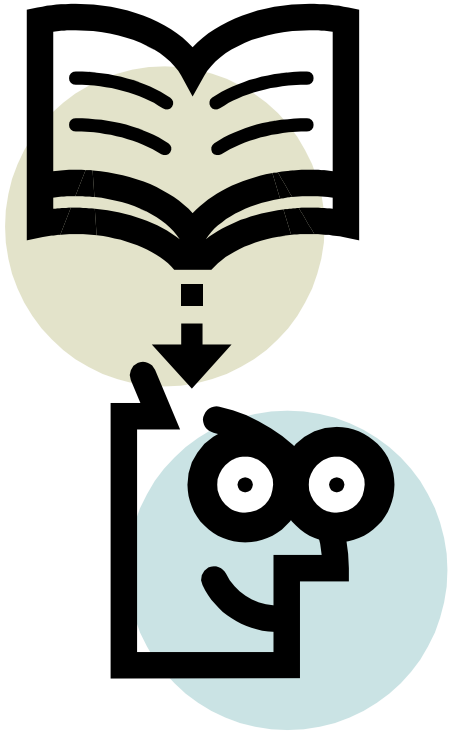
- Questa notizia dovrebbe far riflettere …
- … sarà una buona scelta affidare dati importantissimi ad un metodo che si basa solo sulla lentezza dei calcolatori attuali?
- *Pensiamo alla Legge di Moore (e non parliamo dei computers dei laboratori segreti!)*

… e riflessioni!!!

- È interessante quando detto nel '93 da Wiener, che ha descritto come sia realizzabile un chip da 50 milioni di test al secondo che, in parallelo ad altri 57.000, può condurre un attacco con successo in:
  - 3,5 ore circa. Costo 1 milione $
  - 21 minuti circa. Costo 10 milioni $
  - pochi secondi. Costo 100 milioni $

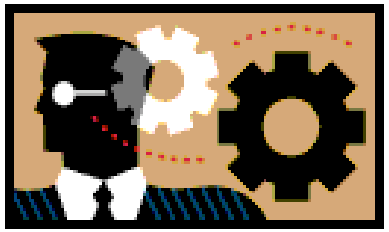
Introduzione

- Entriamo ora più nel dettaglio…

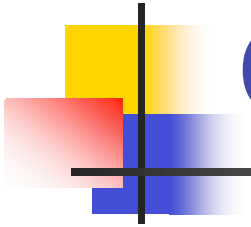


L'idea

L'idea di Rivest: sfruttare la difficoltà di fattorizzare un numero

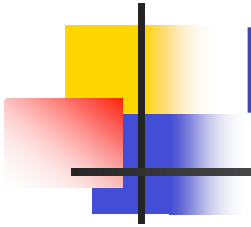


- Infatti, la chiave pubblica è un numero **n** ottenuto moltiplicando due numeri primi **molto grandi** (centinaia di cifre decimali) che restano segreti!!!
- Il sistema si basa su calcoli complicatissimi sfruttando la funzione di Eulero



Come funziona…

- Prendiamo i soliti utenti Kyle e Cartman;
- Se Kyle vuole inviare un messaggio riservato a Cartman, deve prima di tutto andare a cercare sull'elenco le chiavi pubbliche di Cartman.
- Usando questi numeri con una serie di calcoli piuttosto complessi Kyle ottiene il messaggio cifrato da inviare a Cartman.
- Cartman riceve il messaggio e usa la sua chiave segreta per decifrarlo con un calcolo; solo lui conosce questo numero e quindi solo lui può decifrare il messaggio (paradossalmente nemmeno Kyle può decifrare il suo stesso messaggio).

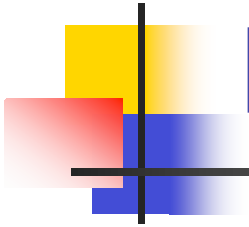


Pro e Contro (1)

- In verità non è dimostrato che sia necessaria la fattorizzazione per forzare RSA …
- … potrebbe esistere un metodo per calcolare la funzione di Eulero _(N) senza conoscere i fattori primi di N!!!
- Ma nessun metodo simile è stato trovato ed RSA resta ad oggi un cifrario inviolato

Attacchi

- Naturalmente è comunque possibile "forzare" l'RSA …
- Una tesina apposita …



Pro e Contro (2)

- Un difetto di RSA è la mole dei calcoli aritmetici che per numeri grandi si traduce in una lentezza della codifica
- Diventano così essenziali:
  - algoritmi veloci per il calcolo,
  - calcolatori sempre più potenti e costosi

Soluzioni miste: l'idea

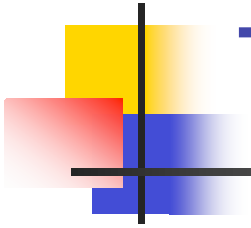
Anche così RSA resta un metodo di cifratura molto più lento (circa mille volte!) degli algoritmi classici come DES

Per questo si usano spesso

SOLUZIONI MISTE

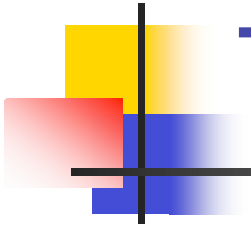
Soluzioni miste: esempio

Esempio: RSA è utilizzato solo per trasmettere la chiave segreta di un DES e il messaggio vero e proprio viene trasmesso appunto con il DES.



Test di primalità

- Un numero si dice **primo** quando è divisibile solo per se stesso e per 1; se possiede altri divisori, si dice che è **composto**
- Escluso dunque il numero 2, tutti i numeri primi sono **dispari**
- Il **controllo della primalità** di un numero è la classificazione di quest'ultimo come primo o come composto



Test di primalità

- La verifica di primalità di un numero n può essere effettuata in vari modi. La scelta è strettamente dipendente dalla dimensione del numero:
  - Numeri piccoli → Teorema di Wilson
  - Numeri grandi → Teorema di Fermat

Teorema di Wilson

- Un numero n è primo se divide <u>senza resto</u>

(n-1)!+1

- Per numeri piccoli, il fattoriale è calcolabile:
  - n=5 → 4!+1=25 → 25/5=5 (resto=0)
  - n=8 → 7!+1=5041 → 5041/8=630,125 (resto≠0)
  - n=19 → 18!+1=6402373705728001 → 6402373705728001/19=336967037143579 (resto=0)

"Piccole difficoltà … "

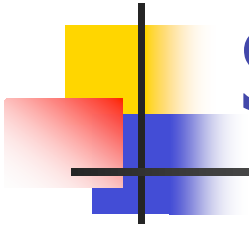
- n=51739721 → 51739720! +1 = → ???

  troppo grande …

Dunque per numeri troppo grandi il teorema di Wilson è IMPRATICABILE!!! …

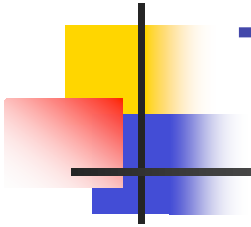
… usiamo un altro algoritmo …

Teorema di Fermat



Struttura

1) Introduzione:
   a cura di Fabrizio Piacenza
2) Generazione chiavi & Test di primalità:
   a cura di Anna Rita Strazioso
3) Cifratura & Decifratura con esempi:
   a cura di Valentina Ventriglia
4) Dimostrazione:
   a cura di Fabrizio Piacenza



Teorema di Fermat

- Un "veloce" algoritmo di controllo della **quasi certa primalità** di numeri molto grandi si basa sul

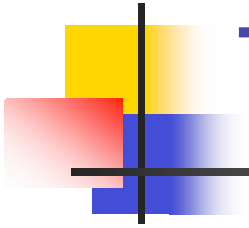
PICCOLO TEOREMA DI FERMAT

Il teorema stabilisce che ***se p è un numero primo, allora per ogni numero naturale b appartenente all'intervallo aperto (0,p):***

$$b^p \bmod p = b$$

Un facile esempio

- Dati 2, 3, 5 (primi) verifichiamone la primalità
  - 2 → $1^2 \bmod 2 = 1$
  - 3 → $1^3 \bmod 3 = 1$, $2^3 \bmod 3 = 2$
  - 5 → $1^5 \bmod 5 = 1$, $2^5 \bmod 5 = 2$, $3^5 \bmod 5 = 3$, $4^5 \bmod 5 = 4$



Teorema di Fermat

- Di conseguenza:

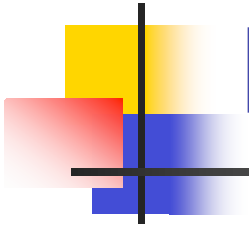
  se esiste un numero naturale b appartenente all'intervallo aperto (0,p), per il quale:

  $$b^p \bmod p \neq b$$

  allora p è un numero composto

Se p non è primo …

- Così ad esempio per il numero *p=4* (non primo) è:
  - 4  $1^4 \bmod 4 = 1$
    $2^4 \bmod 4 = 0$
    $3^4 \bmod 4 = 1$
- per cui 4 è composto (c.v.d.)



Deduzioni ...!!!

- E' lecito a questo punto chiedersi:
  - ***se per ogni b, appartenente all'intervallo aperto (0,p), è***

$$b^p \bmod p = b$$

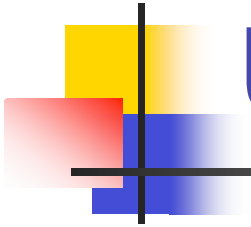
- Si può affermare che p è primo?

Purtroppo NO !!!

Perché NO?

- Esistono infatti numeri composti come:
  - *15* (il prodotto di *3 e* 5)

  che, in relazione al piccolo teorema di Fermat, ***si comportano come se fossero primi , ma non lo sono***
- Tali numeri sono i **numeri di Carmichael**
- ***Poi ci sono numeri,(pseudoprimi),che si comportano come numeri primi, ma non per tutti i valori di b dell'intervallo aperto (0,p).***



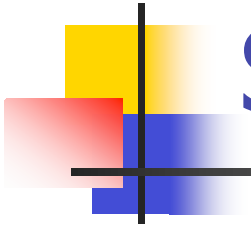
Un esempio

- Il numero composto ***15*** (il prodotto di *3* e *5*), è uno ***pseudoprimo***

$1^{15} \bmod 15 = 1$
$3^{15} \bmod 15 = 12$
$5^{15} \bmod 15 = 5$
$7^{15} \bmod 15 = 13$
$9^{15} \bmod 15 = 9$
$11^{15} \bmod 15 = 11$
$13^{15} \bmod 15 = 7$

$2^{15} \bmod 15 = 8$
$4^{15} \bmod 15 = 4$
$6^{15} \bmod 15 = 6$
$8^{15} \bmod 15 = 2$
$10^{15} \bmod 15 = 10$
$12^{15} \bmod 15 = 3$
$14^{15} \bmod 15 = 14$

In tutto dunque ***8 basi su 14***



Statistiche

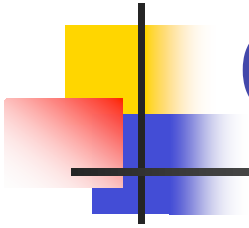
- Senza scendere nei dettagli, si analizzano le basi di 15 e, calcolando le probabilità parziali sulle basi stesse, si ottiene la probabilità che il numero pseudoprimo ***non venga riconosciuto come numero composto*** dal test di Fermat

8/14=0,57	*7/13=0,54*	*6/12=0,5*
5/11=0,45	*4/10=0,4*	*3/9=0,3*
2/8=0,25	*1/7=0,14*	

Che, come si vede, ***tendono a decrescere***

Analisi delle statistiche

- E' importante a questo punto chiedersi:
  - se il ***numero pseudoprimo 15*** non viene riconosciuto come numero composto (ad es.) per 4 volte consecutive, che probabilità ha di superare ***per la quinta volta*** il test di Fermat?
- La risposta è:
  0,07=*0,57*0.54*0.5*0,45* → **7%**

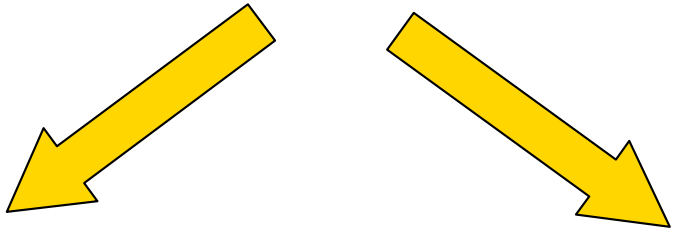


Conclusioni

- Per il calcolo corretto delle probabilità bisogna analizzare ***circa la metà delle basi comprese nell'intervallo aperto (0,p)***
- Si può concludere che, ***se è sempre verificato Fermat***, p ***quasi certamente è un numero primo***

Struttura dell'RSA

- L'analisi dell'algoritmo potrebbe essere suddivisa in 2 parti:

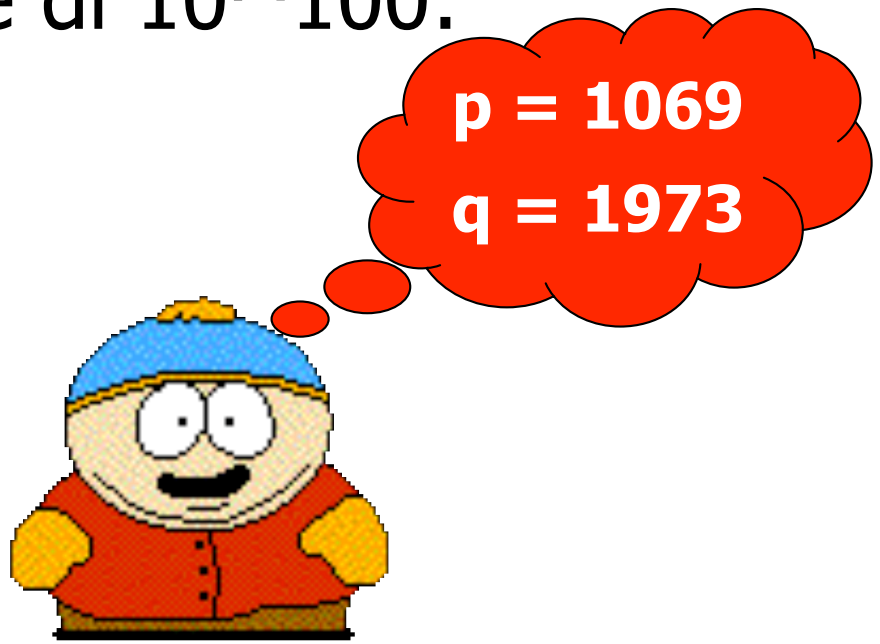


Generazione coppia di chiavi

Utilizzo coppia di chiavi

Esempio (generazione coppia di chiavi)

- Cartman genera due numeri primi distinti **p** e **q**, di valore consigliato maggiore di 10^100:



… continua …

- Cartman calcola il prodotto dei due numeri primi ottenendo il numero n

n = p * q

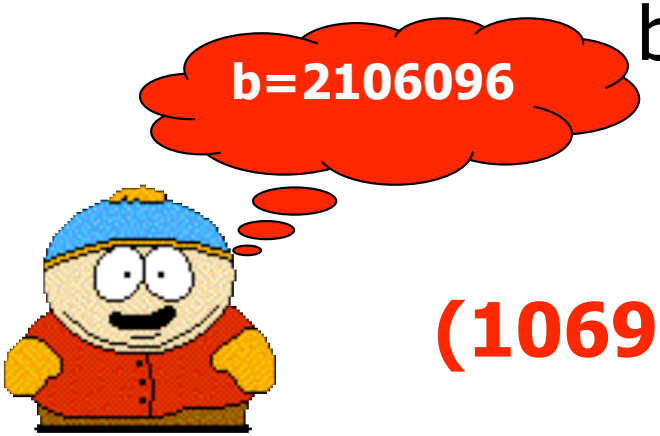
n = 1069 *1973 = 2109137

- **n è la PRIMA CHIAVE PUBBLICA**

...continua ...

- Cartman calcola **b**,la funzione di Eulero di n:
  - Cioè il numero di naturali minori di n e primi con n!

b = _(n) = (p-1)*(q-1)



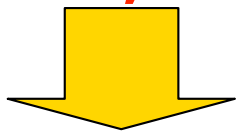
b = _(2109137) =
(1069-1)*(1973-1) = 2106096

- **b è la CHIAVE SEGRETA**
- Ora p e q vengono distrutti.

...continua ...

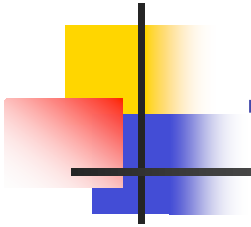
- Cartman sceglie un numero **e** < _(n) che sia primo con b, ovvero mcd(e,b) = 1
- Calcoliamo:

e -> mcd(10001,2106096) = 1 SI



e = 10001

- **e è la SECONDA CHIAVE PUBBLICA**

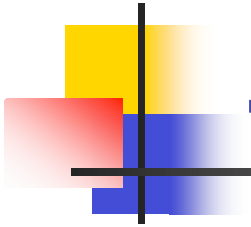


… continua …

- Utilizzando la versione estesa dell'algoritmo di Euclide (il teorema di Eulero sarebbe proibitivo), Cartman calcola il più piccolo numero **d** tale che:

$$e*d = 1 \bmod \_(n)$$

- Per essere più precisi d è l'inverso di e nell'aritmetica di ordine b
- **d è la CHIAVE SEGRETA**



… concludendo:

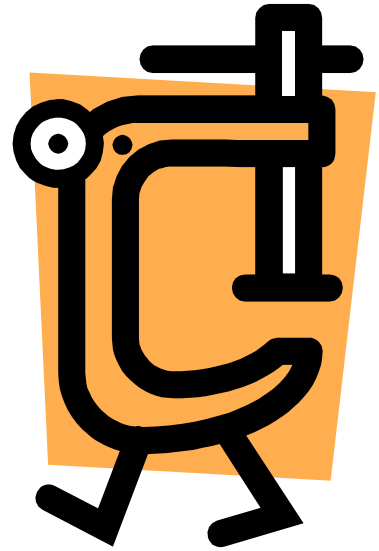
- I calcoli li vedremo successivamente, con numeri più "accessibili" a livello di calcolo, comunque, per ora, **d = 40433**
- Quindi:
  - Chiave pubblica (n,e) = (2109137, 10001)
  - Chiave privata (p,q,b,d) = (1069,1973, 2106096,40433)

… continua …

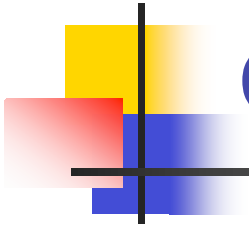
- Le **CHIAVI PUBBLICHE** che riceve Kyle sono:

Ricapitoliamo l'uso delle chiavi per cifratura e decifratura

- RSA utilizza numeri primi e funzioni matematiche quasi impossibili da invertire.
- Vediamo adesso di ricapitolare schematicamente l'algoritmo di generazione delle chiavi:



Algoritmo di generazione delle chiavi:



- Vengono scelti due numeri primi **p** e **q** molto grandi. (ricordiamo che per comodità scegliamo due numeri piccoli per effettuare facilmente i calcoli)

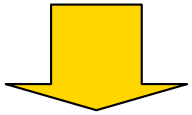
- **p = 5**
- **q = 11**

QUESTI DUE VALORI RESTERANNO **SEGRETI**

… continua …

- Viene calcolato il numero n, ottenuto moltiplicando p e q.
- Ricordiamo che:
  - **p = 5**
  - **q = 11**

n = p * q



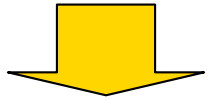
n = 5 * 11 = 55

n è UNA CHIAVE **PUBBLICA**

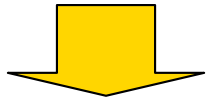
… continua …

- Viene calcolata la funzione di Eulero di n: **_(n)**
- Ricordiamo che:
  - **p = 5**
  - **q = 11**
  - **n = 55**

b=_(n)=(p-1)*(q-1)



b=_(55)=
(5-1)*(11-1)



b = 40

b è **SEGRETO**
(vengono distrutti
p e q)

… continua …

- Si sceglie un numero **e** < b (b = _(n)) e primo con esso, ovvero mcd(e,b) = 1
- Ricordiamo che:
  - **b = 40**
  - **n = 55**

~~e = 2 MCD(2,40)=2~~

e = 3 MCD(3,40)=1

OK!

e = 3

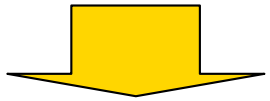
e è la seconda

CHIAVE PUBBLICA

… continua …

- Si calcola il più piccolo numero **d**, inverso di e nell'aritmetica di ordine b.
- Ricordiamo che:
  - **b= 40**
  - **n = 55**
  - **e = 3**

e*d = 1 mod _(n)



Devo trovare in Z_{40} $[3]^{-1}$

d è una

CHIAVE SEGRETA

Calcolo di d:

- Ricordiamo che:
  - **b = 40**
  - **e = 3**
- Vediamo i calcoli:
- Devo trovare in Z_{40} ,$[3]^{-1}$:
- Utilizzando la funzione di Eulero:

$$Z_{b,}\,[e]^{-1} = [\, e \_^{(b)} - 1]$$

Funzione di Eulero

$$\_(b) = \_(5)^* \_(4)$$

$$\_(40) = 4 * 2 = 8$$

$$\_(40) = 8$$

Calcolo di d:

- Utilizzando il teorema di Eulero posso calcolare **d**:
- Ricordiamo:
  - **$\lambda(b) = 8$**

$$Z_{b,}\,[e]^{-1} = [\, e^{\,\lambda(b)\,-\,1}]$$

$$Z_{40,}\,[3]^{-1} = [\, 3^{\,\lambda(40)\,-\,1}]$$

$$[\, 3^{\,8\,-\,1}] = 2187$$

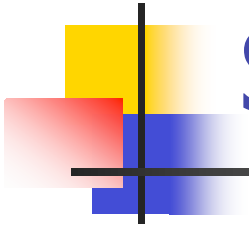
in Z_{40}

$$[27]_{40}$$

RISULTATO

Chiave pubblica:
n = 55
e = 3

Chiave segreta:
p = 5
q = 11
b = 40
d = 27



Struttura

1) Introduzione:
   a cura di Fabrizio Piacenza
2) Generazione chiavi & Test di primalità:
   a cura di Anna Rita Strazioso
3) Cifratura & Decifratura con esempi:
   a cura di Valentina Ventriglia
4) Dimostrazione:
   a cura di Fabrizio Piacenza

Prima della cifratura

- Kyle deve cifrare il suo messaggio per rendere l'informazione disponibile solo a Cartman

...continua ...

- La regola di cifratura, e decifratura, opera con numeri e non con lettere
- Il messaggio va tradotto
- Esitono molti modi per realizzare tale traduzione

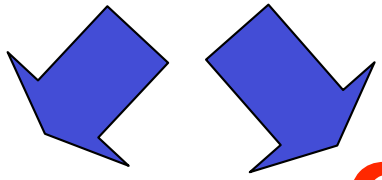


Tabella degli alfabeti

Codici ASCII

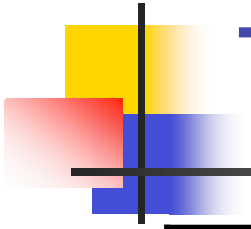
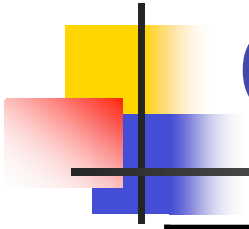


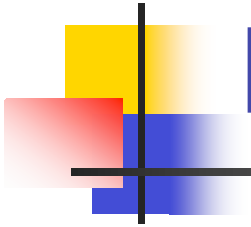
Tabella degli alfabeti

A=01	H=08	O=15	V=22
B=02	I=09	P=16	W=23
C=03	J=10	Q=17	X=24
D=04	K=11	R=18	Y=25
E=05	L=12	S=19	Z=26
F=06	M=13	T=20	_=27
G=07	N=14	U=21	!=28



Codice ASCII

A=01000001	H=01001000	O=01001111	V=01010110
B=01000010	I=01001001	P=01010000	W=01010111
C=01000011	J=01001010	Q=01010001	X=01011000
D=01000100	K=01001011	R=01010010	Y=01011001
E=01000101	L=01001100	S=01010011	Z=01011010
F=01000110	M=01001101	T=01010100	_=00100000
G=01000111	N=01001110	U=01010101	!00100001



ESEMPIO 1

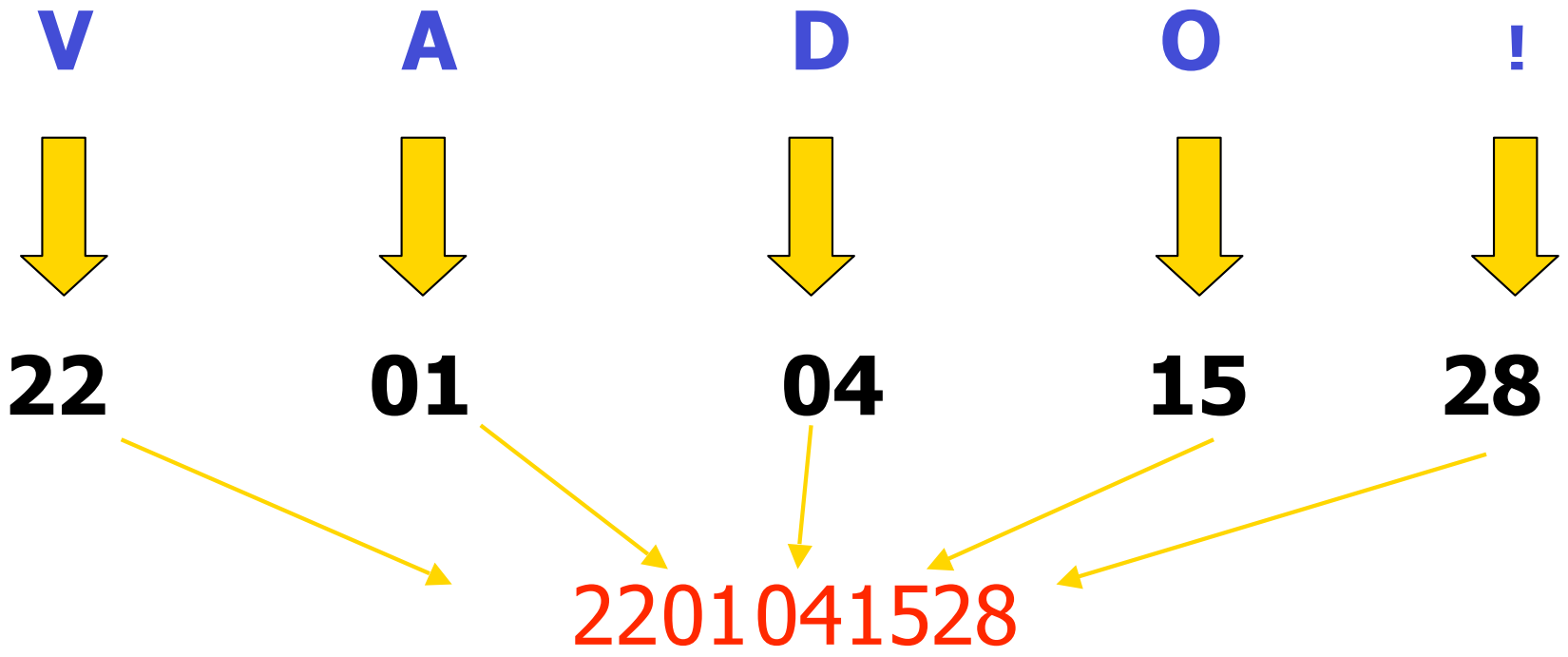
- TABELLA DEGLI ALFABETI
- Non esiste una sola tavola degli alfabeti
- Usiamo quella più banale

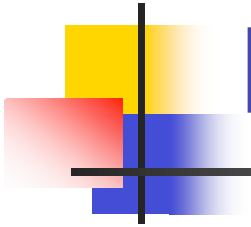
Tabella degli alfabeti

A=01	H=08	O=15	V=22
B=02	I=09	P=16	W=23
C=03	J=10	Q=17	X=24
D=04	K=11	R=18	Y=25
E=05	L=12	S=19	Z=26
F=06	M=13	T=20	_=27
G=07	N=14	U=21	!=28

Traduzione (tab. alfabeti)

- Traduzione tramite la tabella degli alfabeti



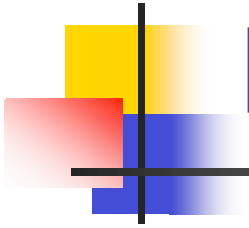


Formazione blocchi

- Kyle effettua il frazionamento in blocchi di k numeri della sequenza ottenuta
- Considerare sempre che il numero rappresentato da ogni blocco non deve essere maggiore della chiave n

$$m <= n$$

- Il testo cifrato non corrisponderebbe al testo in chiaro



Esempio blocchi

- 324850986517 n=350

Se formassi blocchi con k=3 numeri:

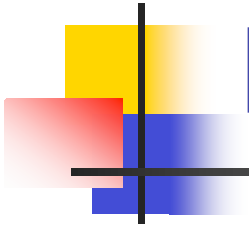
324 850 986 517

324<350 OK…

850>350 NO

per usare blocchi di tre numeri avrei dovuto avere n>986(blocco di valore max)

- uso blocchi di due numeri (k=2)



Blocchi

2201041528

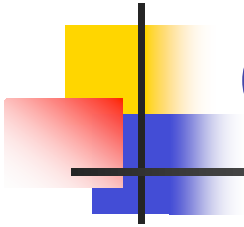
- k=3 ➔ 220>55 NO
- k=2 ➔22<55;

  01<55;

  04<55;

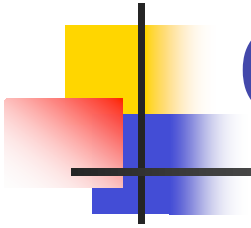
  15<55;

  28<55; OK!!!



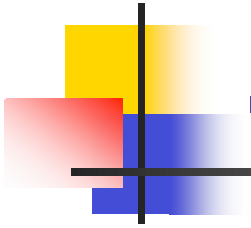
osservazioni

- Nella tavola usata per la traduzione, il valore massimo usato è 28<55. Se così non fosse stato avrei dovuto formare blocchi da un valore
- Nel caso in cui l'ultimo blocco non fosse lungo quanto k, si introduce nel testo una sequenza di spazi affinchè ogni blocco abbia k elementi (28)



Cifratura

- Finalmente Kyle può dar luogo alla cifratura vera e propria.
- Kyle legge le chiavi pubbliche di Cartman (n,e) e trasmette i blocchi m uno alla volta cifrandoli con la formula
- $c_i = m_i^e \bmod n$.



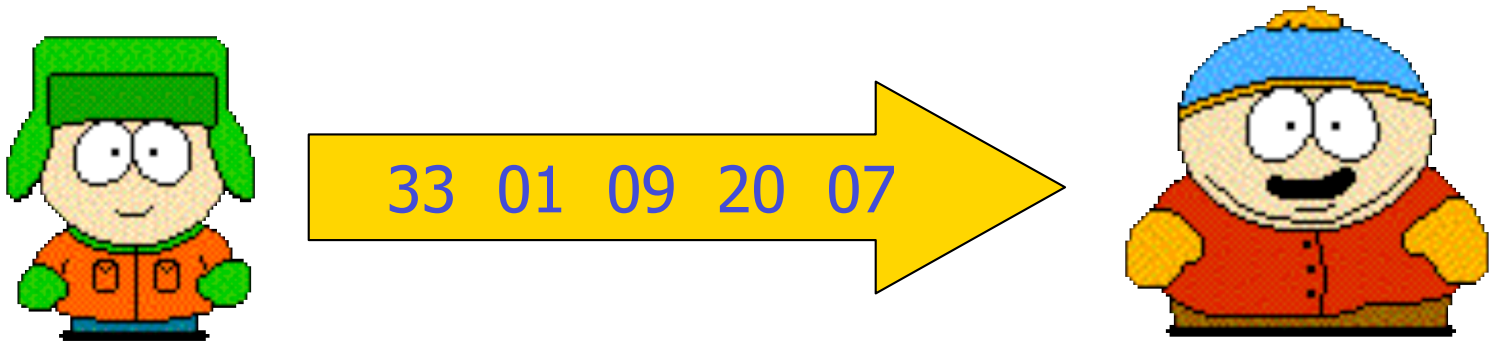
..continua (cifratura)

22 **01** **04** **15** **28**
m1 m2 m3 m4 m5

- C(1)=22^3 mod 55= 33
- C(2)=1^3 mod 55= 01
- C(3)=4^3 mod 55= 09
- C(4)=15^3 mod 55= 20
- C(5)=28^3 mod 55= 07

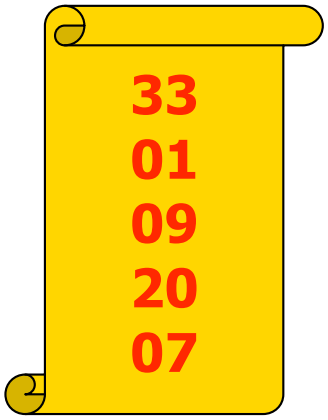
trasmissione

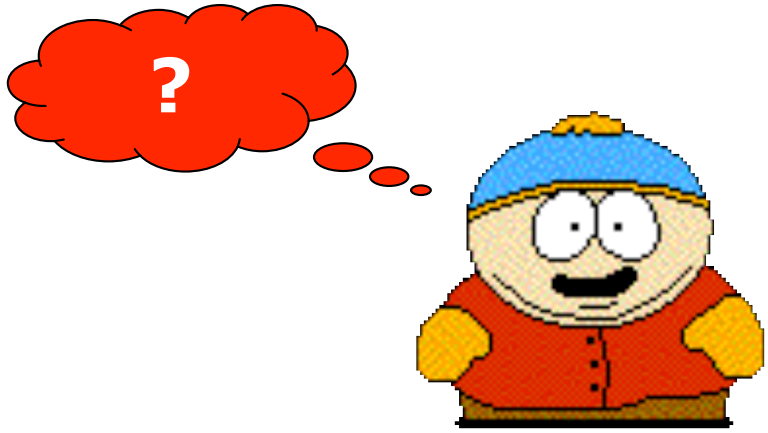
- Ora il messaggio di Kyle è pronto per essere spedito a Cartman



Decifratura….

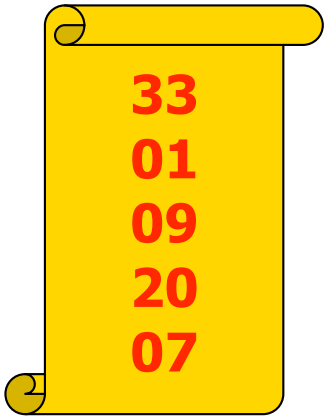
- Cartman ricevuto il messaggio deve decifrarlo. Nell'RSA il messaggio cifrato può essere decifrato solo dal leggittimo destinatario

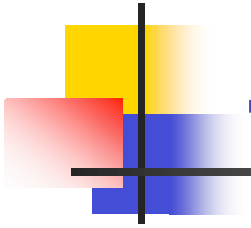




…continua (decifratura)…

- Cartman per decifrare il messaggio applica la sua chiave privata a tutti i numeri del testo cifrato c secondo la formula :$m_i = c_i^d \bmod n$





...continua...

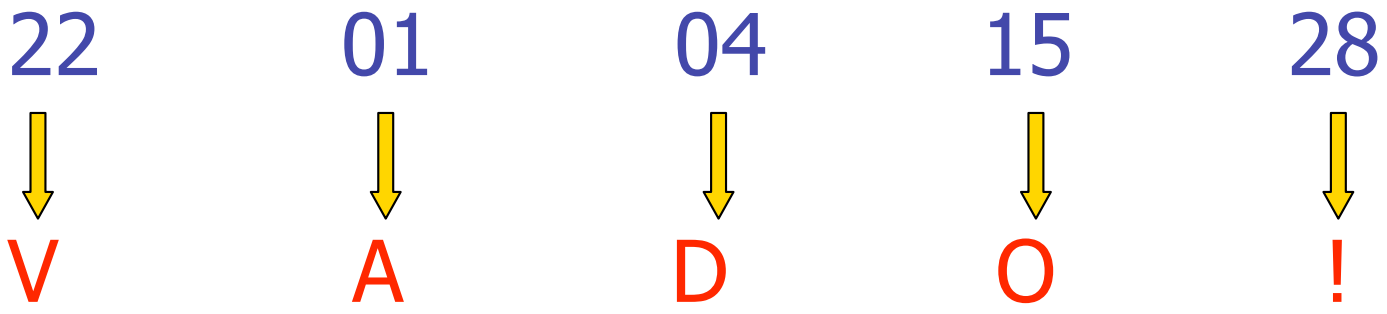
C=33 01 09 20 07

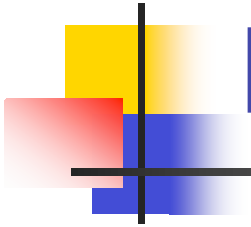
c1 c2 c3 c4 c5

- m(1) = 33^27 mod 55=22
- m (2)= 1^27 mod 55 =01
- m (3)= 9^27 mod 55 = 04
- m (4)= 20^27 mod 55 =15
- m (5)= 7^27 mod 55 = 28

…continua

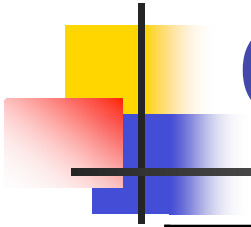
- Decifrato il messaggio Cartman ottiene la sequenza di numeri
- Confrontando i numeri con la tabella degli alfabeti otterrà il testo del messaggio inviatogli da Kyle





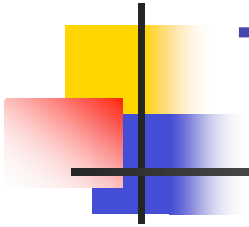
ESEMPIO 2

- TRADUZIONE CON IL CODICE ASCII
- Ad ogni lettera corrisponde una sequenza di 8 bit



Codice ASCII

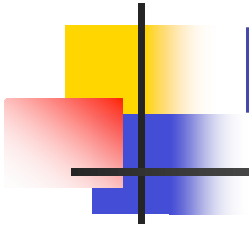
A=01000001	H=01001000	O=01001111	V=01010110
B=01000010	I=01001001	P=01010000	W=01010111
C=01000011	J=01001010	Q=01010001	X=01011000
D=01000100	K=01001011	R=01010010	Y=01011001
E=01000101	L=01001100	S=01010011	Z=01011010
F=01000110	M=01001101	T=01010100	_=00100000
G=01000111	N=01001110	U=01010101	!=00100001



Traduzione (ASCII)

- ASCII

V	A	D	O	!
01010110	01000001	01000100	01001111	00100001



Blocchi (ASCII)

- Per utilizzare la formula di cifratura e decifratura dobbiamo avere blocchi con valore m <=n
- Ogni blocco sarà costituito da k elementi
- In binario il numero 55 è rappresentato da 6 bit(110111). Per essere sicuri che m<=n facciamo blocchi da 5 numeri

..continua(blocchi)

V A D O !

01010110 01000001 01000100 01001111 00100000

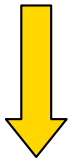
0101011001000001010001000100111100100000

Per riempire l'ultimo blocco, in caso ne avessimo bisogno,inseriamo gli zeri

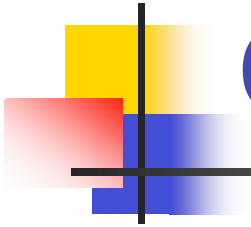
Prima della cifratura

- Calcoliamo il valore numerico corrispondente ad ogni blocco ottenuto

010101100100000101000100010011110100000



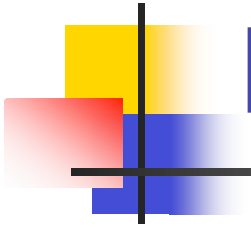
10 25 0 20 8 19 25 0



Cifratura

- C(1)=10^3 mod 55=10
- C(2)=25^3 mod 55=5
- C(3)=0^3 mod 55=0
- C(4)=20^3 mod 55=25
- C(5)=8^3 mod 55=17
- C(6)=19^3 mod 55=39
- C(7)=25^3 mod 55=5
- C(8)=0^3 mod 55=0

Trasmissione



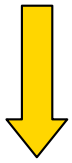
Decifratura

- m(1)=10^27 mod 55=10
- m(2)=5^27 mod 55=25
- m(3)=0^27 mod 55=0
- m(4)=25^27 mod 55=20
- m(5)=17^27 mod 55=8
- m(6)=39^27 mod 55=19
- m(7)=5^27 mod 55=25
- m(8)=0^27 mod 55=0

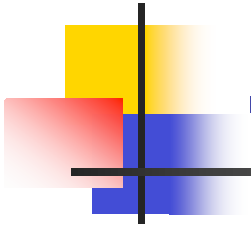
..traduzione..

- Per leggere il messaggi Cartman deve riottenere le lettere associate ai numeri ricevuti
- Traduciamo i numeri nel sistema binario

10 25 0 20 8 19 25 0



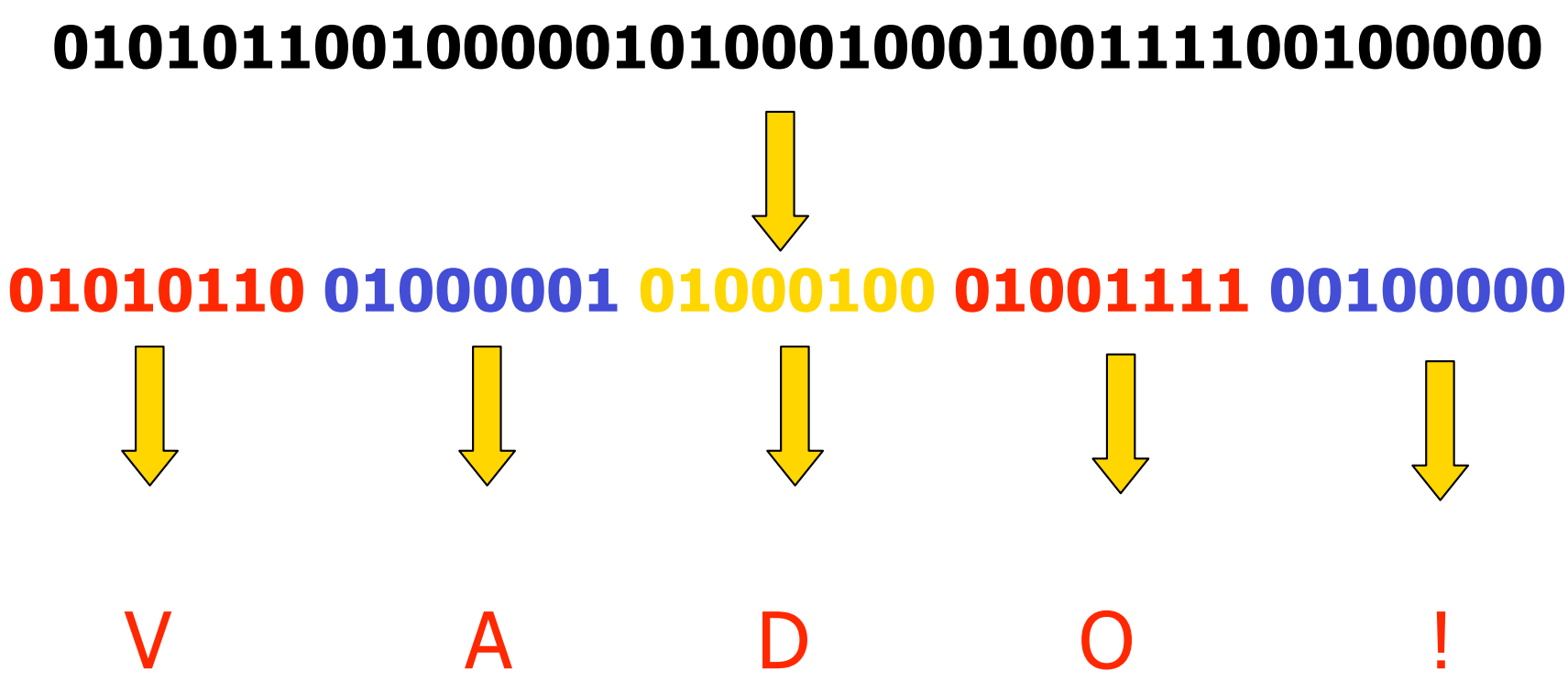
01010110010000010100010001001111001000000

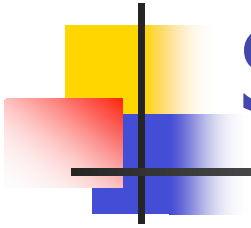


..traduzione..

- La sequenza così ottenuta deve essere divisa in blocchi di 8 numeri poiché il codice ascii traduce ogni numero con una sequenza di 8 bit

..traduzione


0101011001000001010001000100111100100000
01010110 01000001 01000100 01001111 00100000
V A D O !

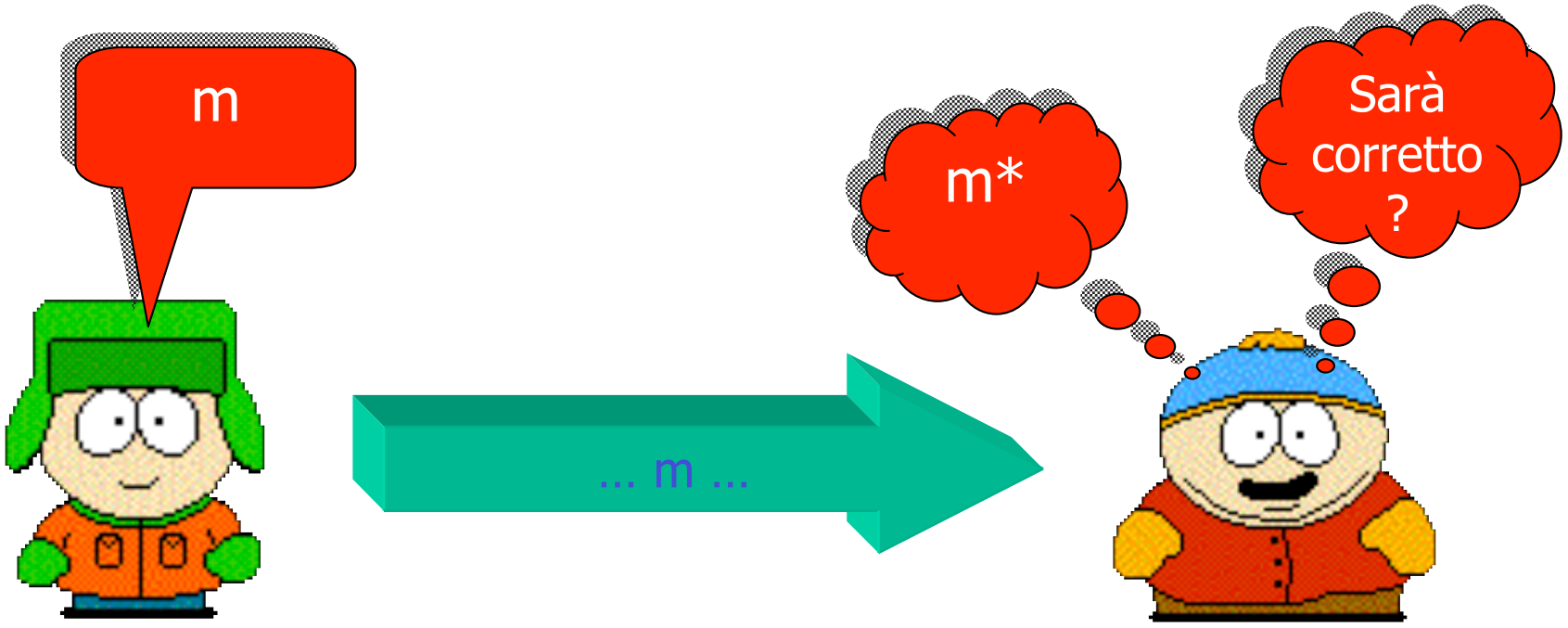


Struttura

1) Introduzione:
   a cura di Fabrizio Piacenza
2) Generazione chiavi & Test di primalità:
   a cura di Anna Rita Strazioso
3) Cifratura & Decifratura con esempi:
   a cura di Valentina Ventriglia
4) **Dimostrazione:**
   a cura di Fabrizio Piacenza

Dimostrazione

Il messaggio ottenuto da Cartman è veramente quello giusto ...???

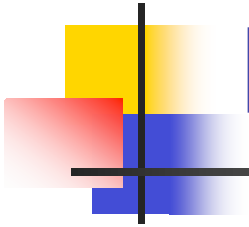


Dimostrazione

- Abbiamo visto che si usano 2 formule:
  - per la cifratura → $c = m^e \bmod n$
  - per la decifratura → $m^* = c^d \bmod n$

Dove ricordiamo che:

- n ⇒ 1° chiave pubblica
- e ⇒ 2° chiave pubblica
- m ⇒ blocco di partenza non cifrato
- c ⇒ blocco cifrato
- m* ⇒ blocco finale decifrato

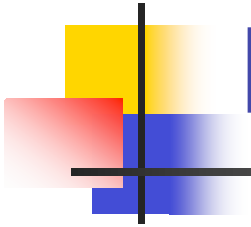


Dimostrazione

- Partendo dalle 2 formule:
  - c = m^e mod n
  - m* = c^d mod n

  - Troviamo per sostituzione che:

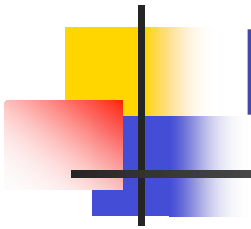
$$m^* = m^{(e*d)} \bmod n$$



Passo 1

1) Iniziamo ricordando che d è stato scelto tale che:
   - e*d = 1 mod _(n);
   - ciò significa che esiste (per definizione di congruenza) un intero positivo k tale che

$$e*d = 1 + k * \_(n)$$



Passo 2 & 3

2) Ricordiamo che:

$$\_(n)=(p-1)(q-1)$$

3) Dunque si ottiene:

$$e*d=1+k*\_(n)$$

$$e*d=1+k*(p-1)(q-1)$$

Passo 4

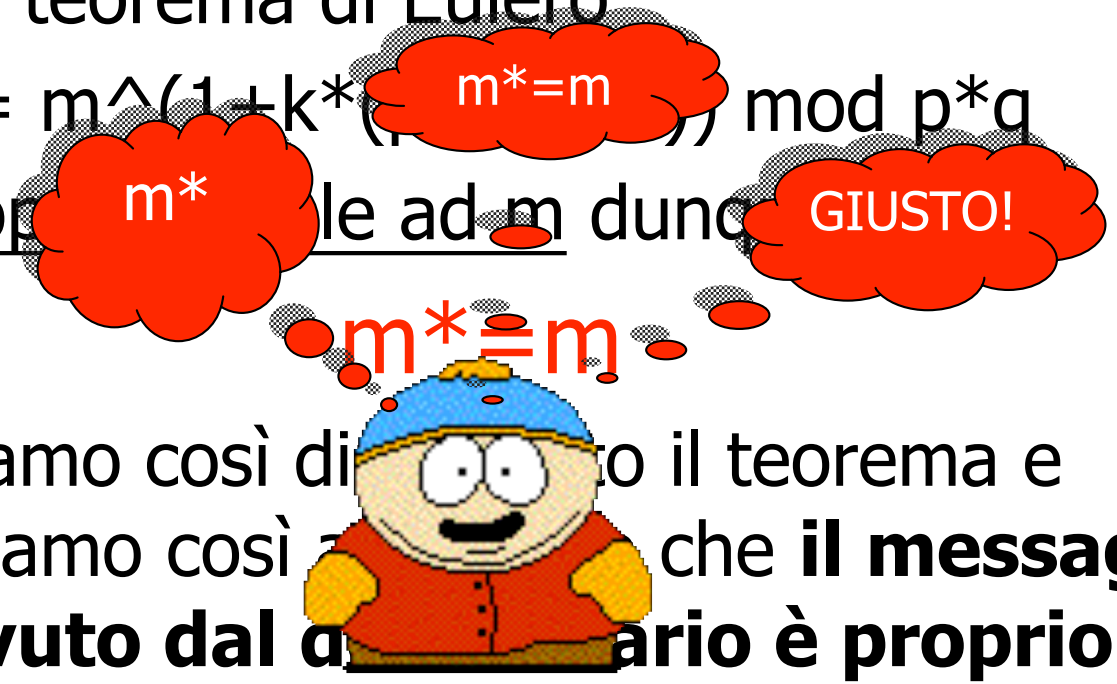
4) Il valore ottenuto al passo 3 possiamo ora sostituirlo:

- m* = m^(e*d) mod n
- e*d=1+k*(p-1)(q-1)
- p*q = n

  - m* = m^(1+k*(p-1)(q-1)) mod p*q

Passo finale

- Per il teorema di Eulero
  m* = m^(1+k*(p-1)*(q-1)) mod p*q
  è proprio uguale ad m dunque



- Abbiamo così dimostrato il teorema e possiamo così affermare che **il messaggio ricevuto dal destinatario è proprio quello mandato dal mittente**.

Bibliografia & Ringraziamenti

- Tutto il materiale proiettato è stato preso da Internet (i siti sono disponibili on-line su documento word)
- Le varie ClipArt sono della collezione di Microsoft Office
- Un grazie particolare va ai personaggi di South Park…