

Protocollo E-cash ed algoritmo RSA

Carlo Manasse

Giulio Baldantoni

Corso di laurea in Informatica

May 10, 2012

Introduzione

Carlo Manasse
Giulio Baldantoni

RSA è un algoritmo di crittografia asimmetrica.

Fu introdotto nel 1978 da

- Rivest Ronald
- Shamir Adi
- Adleman Leonard

Ancora oggi è uno degli algoritmi più utilizzati in numerosi campi d'applicazione.

Introduzione

Carlo Manasse
Giulio Baldantoni

Permette di garantire

- Riservatezza
- Autenticità
- Non ripudio

In altri termini

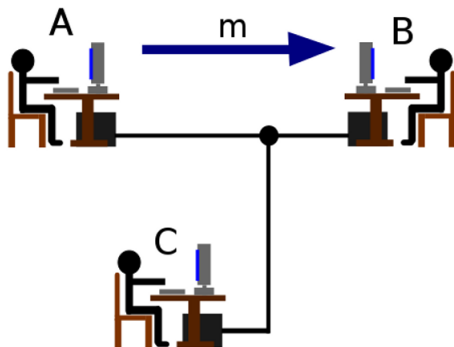
- Cifrare - decifrare un messaggio
- Firmare un messaggio

Una variante di RSA usata in E-cash permette

- Firma cieca

Riservatezza

Carlo Manasse
Giulio Baldantoni



C può leggere il messaggio m

Riservatezza

Lezione 11
Crittografia
Il Problema RSA

Carlo Manasse
Giulio Baldantoni

Il funzionamento di RSA si basa su 3 fasi

- Generazione delle chiavi
- Cifratura
- Decifratura

Generazione delle chiavi

Carlo Manasse
Giulio Baldantoni

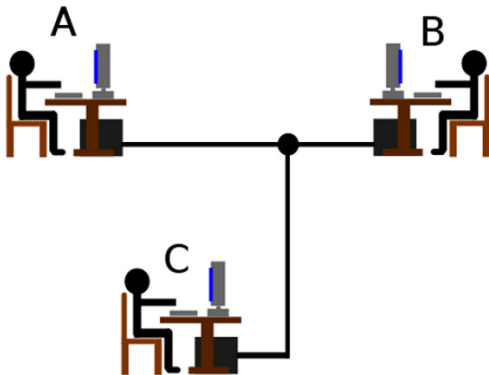
- 1 si scelgono due numeri primi p e q
- 2 si calcola $n = pq$
- 3 si calcola la funzione di Eulero $\varphi(n) = (p - 1)(q - 1)$
- 4 si sceglie un numero e tale che $1 < e < \varphi(n)$ coprimo con $\varphi(n)$
- 5 si calcola d come l'inverso moltiplicativo di e modulo $\varphi(n)$.
i.e $ed \equiv 1 \pmod{\varphi(n)}$

La coppia (e, n) è detta *chiave pubblica* mentre (d, n) è detta *chiave privata*

Cifratura

Per cifrare il messaggio m occorre calcolare il cyphertext con la chiave pubblica

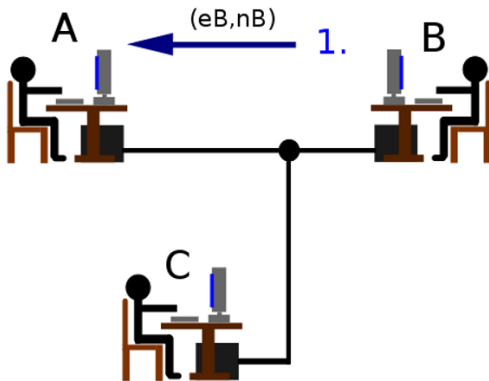
$$c \equiv m^e \pmod{n}.$$



Cifratura

Per cifrare il messaggio m occorre calcolare il cypher text con la chiave pubblica

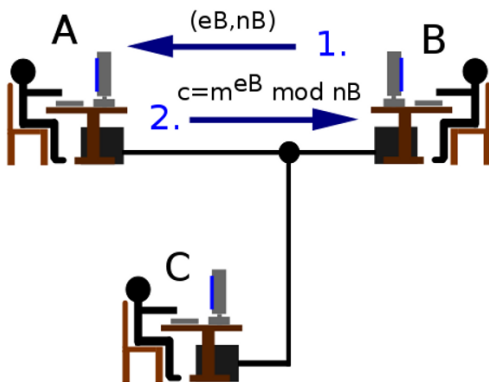
$$c \equiv m^e \pmod{n}.$$



Cifratura

Per cifrare il messaggio m occorre calcolare il cypher text con la chiave pubblica

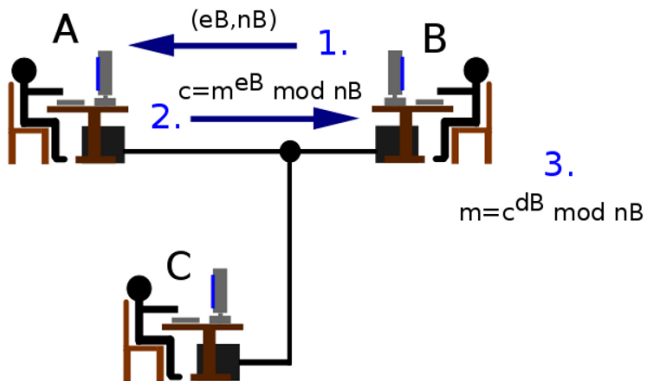
$$c \equiv m^e \pmod{n}.$$



Decifratura

Per decifrare il messaggio c si ricalcola il testo in chiaro con la chiave privata

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



Perché funziona

Si dimostra che $(m^e)^d \equiv m \pmod{pq}$.

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$



$$ed \equiv 1 \pmod{p-1} \quad ed \equiv 1 \pmod{q-1}$$

Per il piccolo teorema di Fermat se p e q sono primi valgono

$$m^{ed} \equiv m \pmod{p} \quad m^{ed} \equiv m \pmod{q}$$

Infine per il teorema cinese dei resti

$$m^{ed} \equiv m \pmod{pq}$$

cioè

$$c^d \equiv m \pmod{n}$$

Esempio numerico

Carlo Manasse
Giulio Baldantoni

- Generazione delle chiavi
 - ① $p = 5$ e $q = 11$ dunque $n = 55$
 - ② $\varphi(n) = (p - 1)(q - 1) = 40$
 - ③ $e = 7 \rightarrow e < 40, \text{MCD}(e, 40) = 1$
 - ④ $d = 23 \rightarrow 7 * 23 = 161 \equiv 1 \pmod{40}$

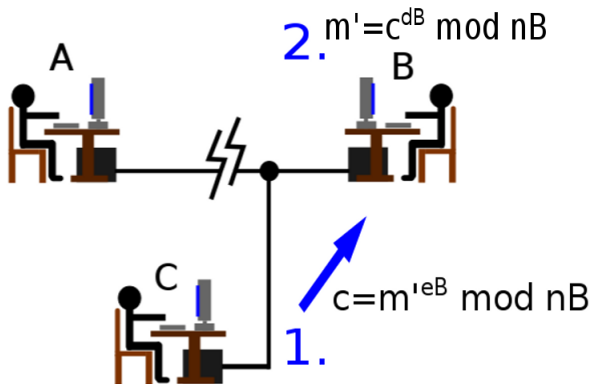
chiave pubblica $\rightarrow (7, 55)$

chiave privata $\rightarrow (23, 55)$

- Cifratura - decifratura
- $m = 18$
 - ① $m^e = 18^7 \equiv c \equiv 17 \pmod{55}$
 - ② $c^d = 17^{23} \equiv m \equiv 18 \pmod{55}$

Autenticità e non ripudio

Carlo Manasse
Giulio Baldantoni



C interrompe la connessione tra A e B. Come fa B a sapere chi ha spedito il messaggio m' ?

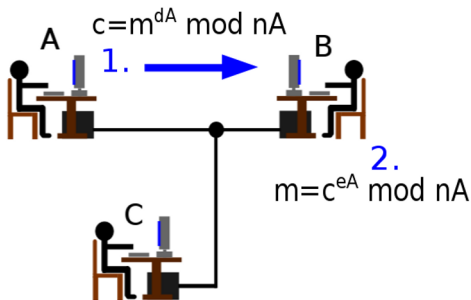
Autenticità e non ripudio

Firmare un messaggio m è simile al metodo precedente.
Occorre difatti cifrare con la chiave privata

$$c \equiv m^d \pmod{n}$$

e decifrare con la chiave pubblica

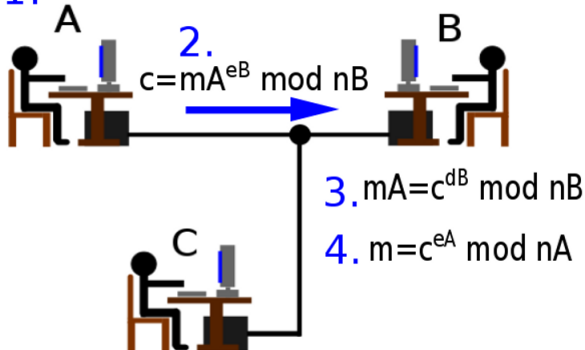
$$c^e \equiv (m^d)^e \equiv m \pmod{n}.$$



Riservatezza, autenticità e non ripudio

Combinando le due tecniche si possono raggiungere tutti gli obiettivi prefissati.

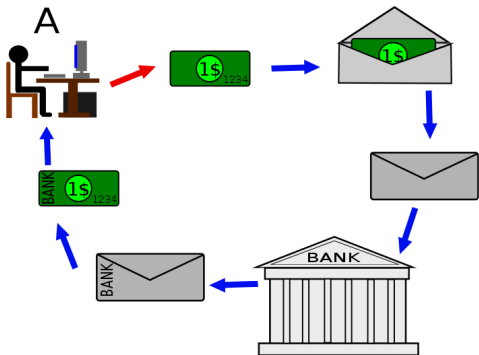
1. $m_A = m^{d_A} \bmod n_A$



Firma cieca

Carlo Manasse
Giulio Baldantoni

- Un'innovazione che E-cash ha portato nel mondo dei pagamenti elettronici
- Garantisce l'anonimato e la non tracciabilità delle transazioni
- Variante dell'algoritmo RSA



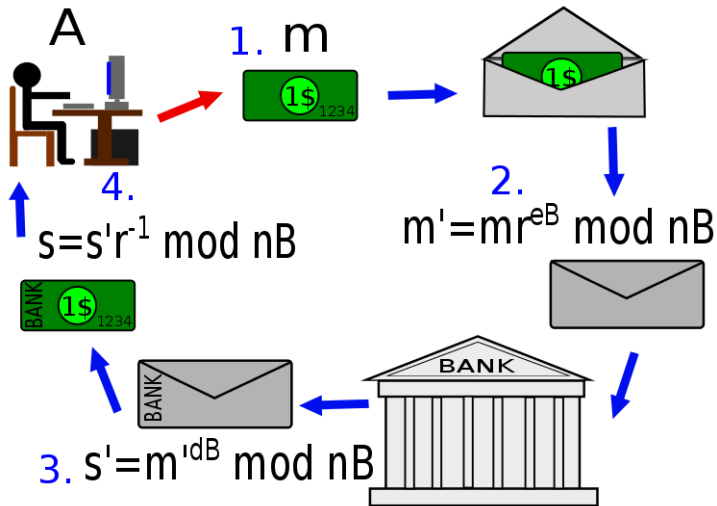
Firma cieca

Carlo Manasse
Giulio Baldantoni

- Imbustamento
 - ① A genera un numero casuale r compreso tra 1 e n che sia coprimo rispetto ad nB .
 - ② A aggiunge ad m il fattore di cecità tramite il passaggio $m' \equiv mr^{eB} \pmod{nB}$. Poiché r , e di conseguenza anche r^{eB} , è random, m' non porta alcuna informazione riguardo m .
- Certificazione
 - ① Nel momento in cui B riceve m' lo firma con la sua chiave privata ottenendo $s' \equiv m'^{dB} \pmod{nB}$. Come detto in questo passaggio B non può conoscere m . B infine manda s' ad A.
 - ② Ricevuto s' , A può rimuovere il fattore cecità tramite il passaggio $s \equiv s' r^{-1} \equiv m^{dB} \pmod{nB}$ per ottenere la moneta firmata dalla banca B.

Firma cieca

Carlo Manasse
Giulio Baldantoni



Fine

Università
Ca' Foscari
Venezia

Carlo Manasse
Giulio Baldantoni

Grazie per l'attenzione