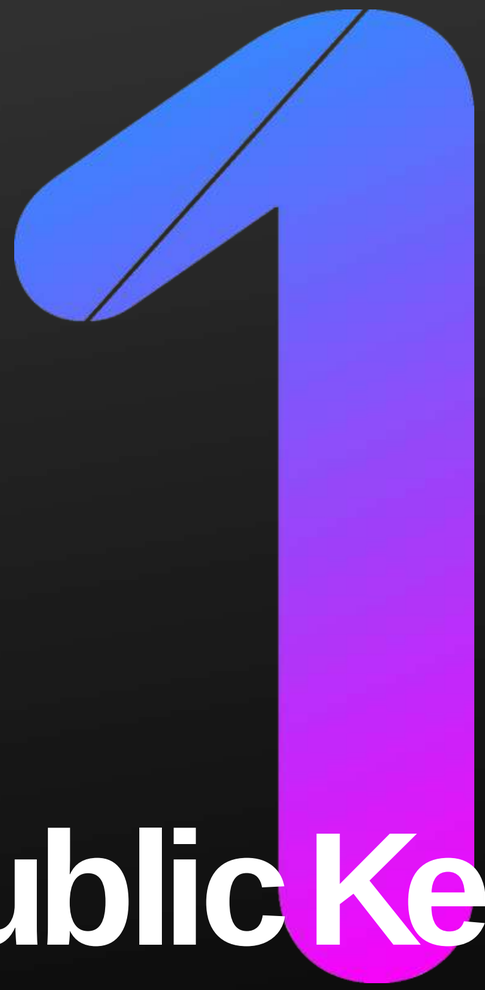
LA CRITTOGRAFIA ASIMMETRICA

Sicurezza informatica

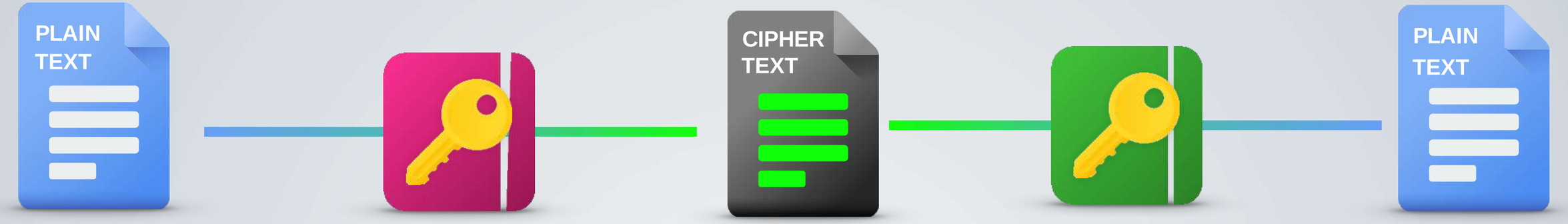
Elena Maria Dal Santo

elenamaria.dalsanto@its-ictpiemonte.it



Public Key Encryption


PREVIOUSLY ON
SONY



Encryption

Decryption

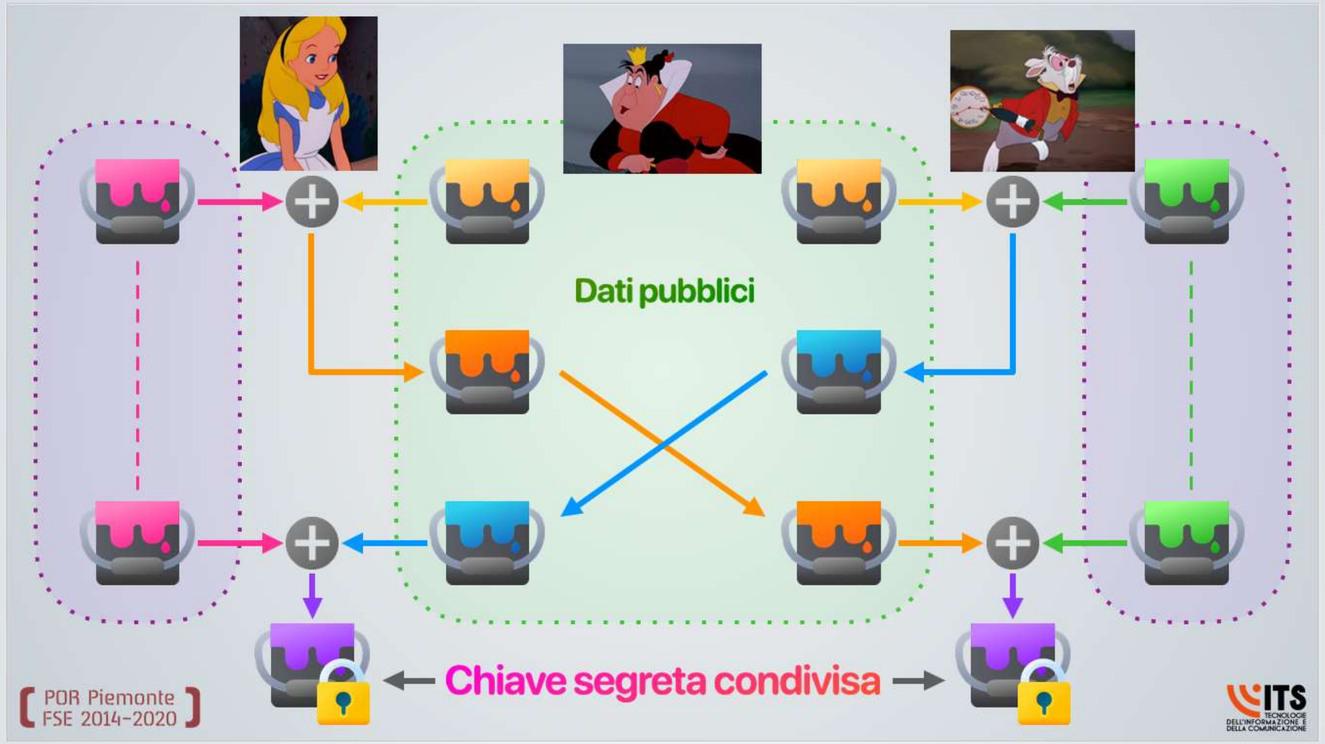
Nella crittografia simmetrica, la chiave era la stessa per cifrare e decifrare il messaggio

↓

Problema dello scambio della chiave → Diffie-Hellman

La crittografia asimmetrica

La crittografia asimmetrica (o crittografia a chiave pubblica) un tipo di crittografia dove ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi diverse, una pubblica e una privata.



Lo scambio delle chiavi di Diffie-Hellman è stato uno dei primi esempi di crittografia asimmetrica!

CHIAVI
PUBBLICHE

CHIAVI
PRIVATE

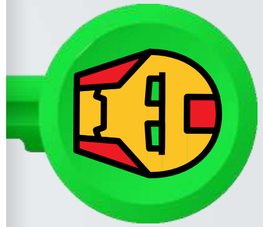
A inizio comunicazione, ognuno dei due ha:

- La sua chiave privata
- La chiave pubblica dell’altro

HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO

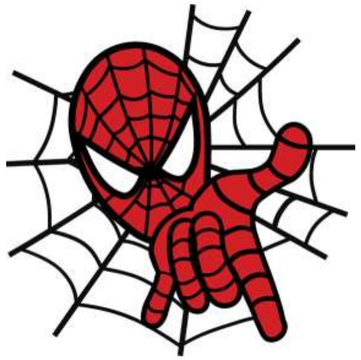
Peter usa la chiave pubblica di Mary Jane per cifrare il messaggio

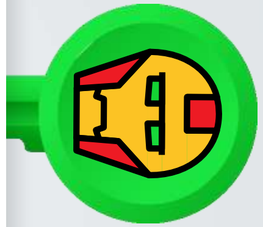
HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO



Mary Jane usa la sua chiave privata per decifrare il messaggio

I am
Spiderman.





Mary Jane usa la sua chiave privata per decifrare il messaggio

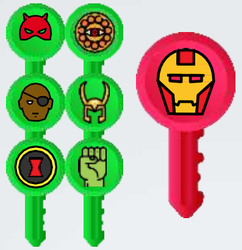
Creare un canale di comunicazione

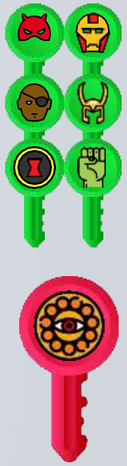
canale cifrato

Dopo essersi scambiati le chiavi pubbliche Mary Jane e Peter hanno instaurato un canale di comunicazione sicuro.

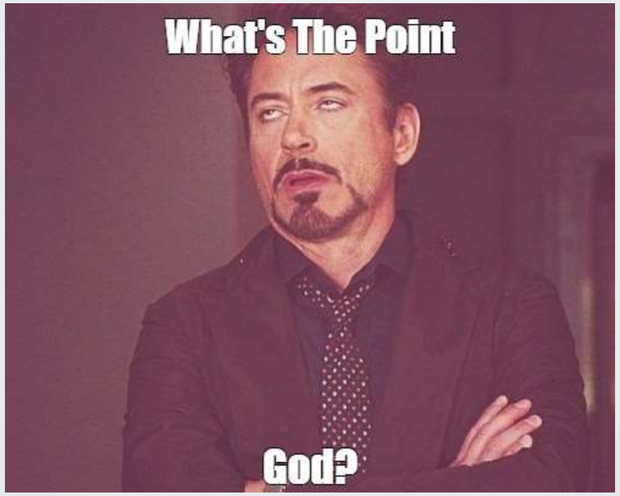
Creare canali cifrati multipli

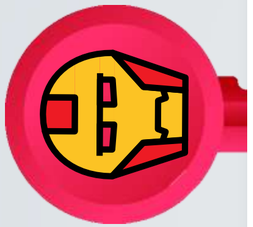
Creare canali cifrati multipli





Okay, ma… quali sono i vantaggi?





HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO

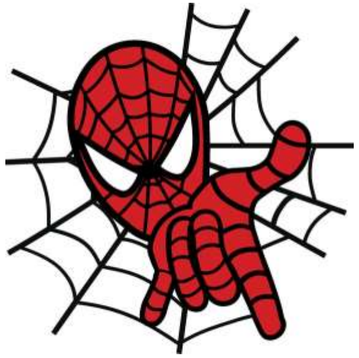
Peter usa la sua chiave privata per cifrare il messaggio

HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO

Mary Jane usa la chiave pubblica di Peter per decifrare il messaggio

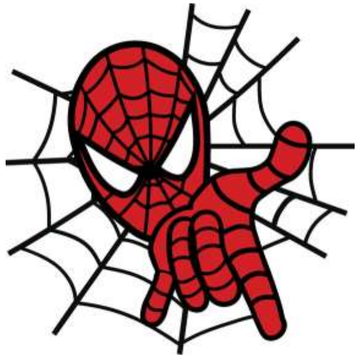
Inviare un messaggio autenticato!

I am Spiderman.



Mary Jane è sicura che il messaggio sia arrivato proprio da Peter!

I am
Spiderman.



Il messaggio è stato firmato.

La firma elettronica

19 gennaio 2000 → l'Italia si adegua alle richieste dell'Europa e crea una normativa per la firma digitale

↓

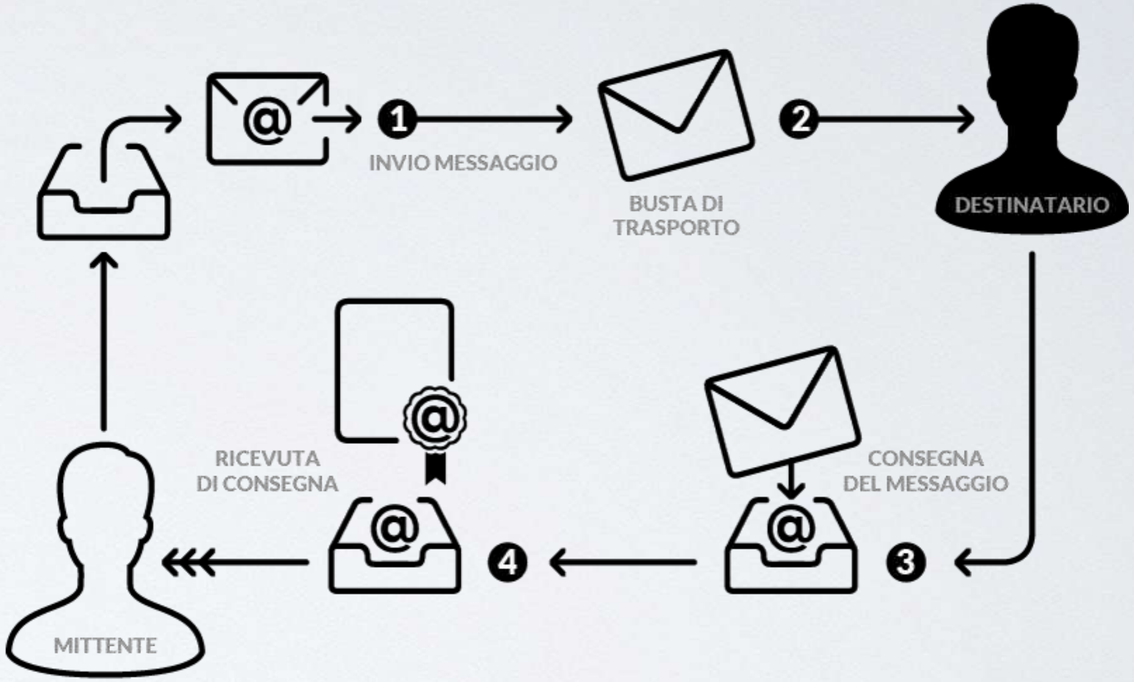
''Particolare tipo di firma qualificata, basato su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. ''

La PEC

1.Il mittente invia il messaggio al destinatario

2.Il gestore provvede a inviare al mittente una notifica di accettazione/non accettazione.

3.La ricevuta riporta data e ora di invio, oggetto, informazioni sul mittente e destinatario.

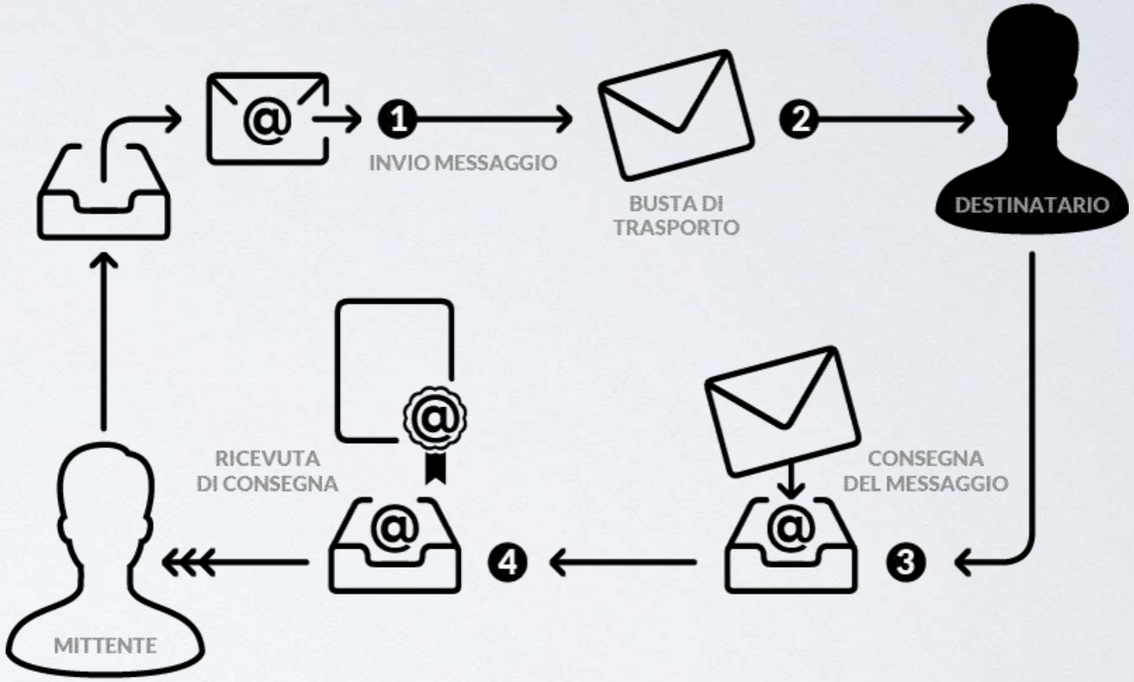


La PEC

4. Il messaggio viene imbustato in un nuovo messaggio (busta di trasporto).

5. Il documento viene firmato digitalmente dal gestore e inviato al destinatario.

6. Il gestore ricevente effettua un controllo sulla firma del gestore mittente e sulla validità.

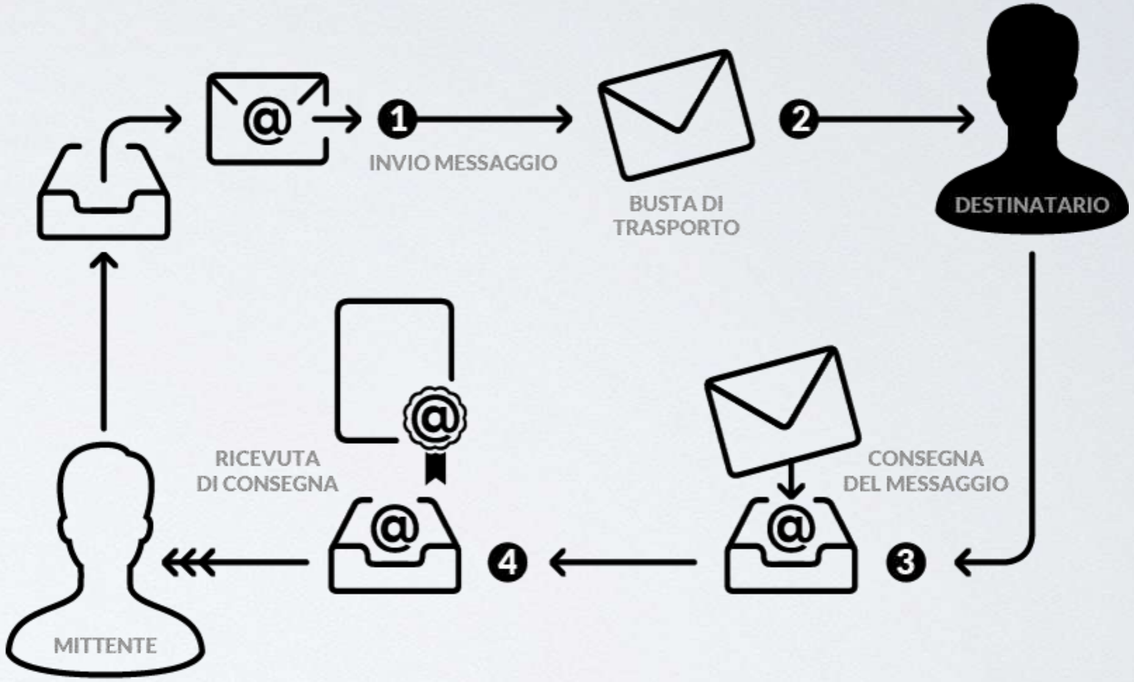


La PEC

7. In caso di verifica positiva, provvede a inviare una ricevuta di presa in carico.

8. Poi invia lo stesso alla mailbox del destinatario.

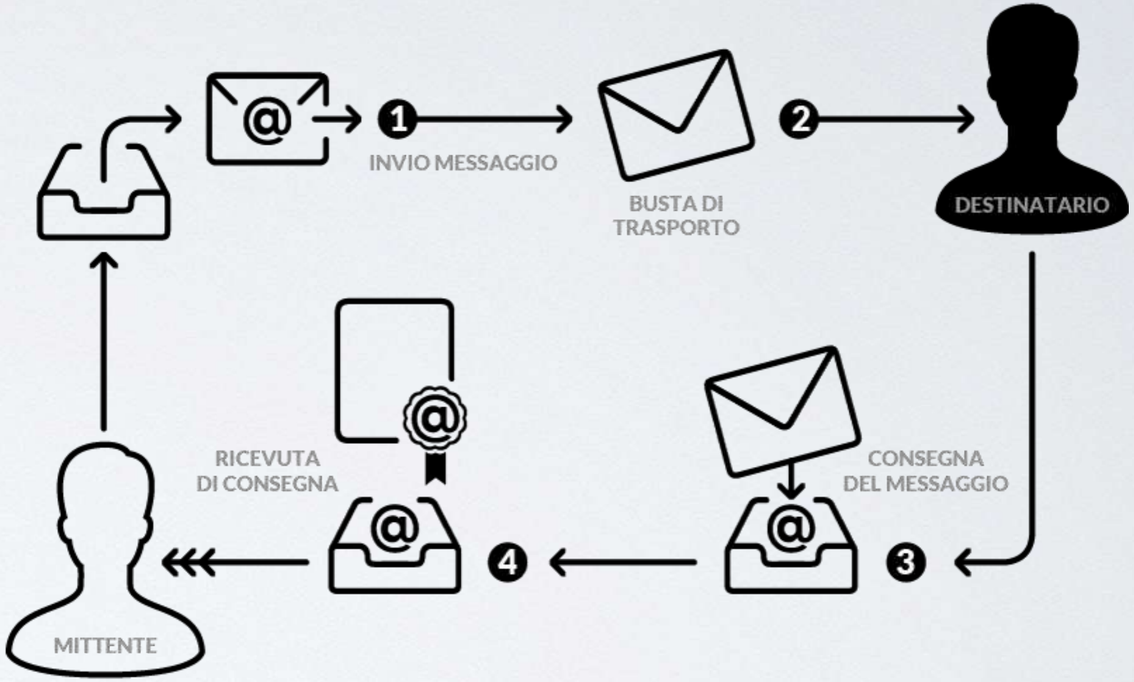
9. Il gestore ricevente rende disponibile il messaggio nella casella del destinatario.



La PEC

10. Il gestore ricevente invia al gestore mittente una ricevuta di avvenuta consegna.

11.Il mittente riceve nella sua mailbox la ricevuta di avvenuta consegna.



2

RSA

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE
DELL'INFORMAZIONE E
DELLA COMUNICAZIONE

Programming Techniques
S.L. Graham, R.L. Rivest* Editors

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science
and Department of Mathematics

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
(1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the

The era of "electronic mail" [1
us; we must ensure that two im
the current "paper mail" syster
messages are *private*, and (b) me
We demonstrate in this paper
capabilities into an electronic ma

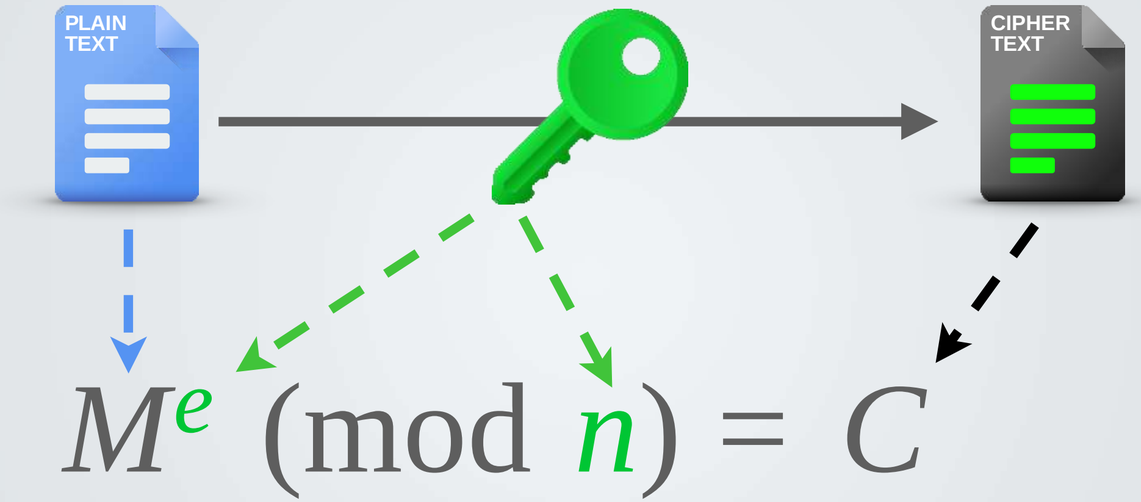
At the heart of our proposal
method. This method provides ar
"public-key cryptosystem", an
vented by Diffie and Hellman [1
vated our research, since they p
but not any practical implementa
Readers familiar with [1] may w
Section V for a description of ou

II. Public-Key Cryptosystems

In a "public-key cryptosysten

POR Piemonte FSE 2014-2020
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Encryption function



Cosa significano quei simboli?

$$M^e \pmod{n} = C$$

'' M alla e, modulo n è uguale a C ''

Significa che C è il resto della divisione di M^e per n

Vediamo un esempio pratico…

$$M^e \pmod{n} = C$$

Prendiamo
M = 44
e = 1
n = 6

44 = 42 + 2 = (6 x 7) + 2

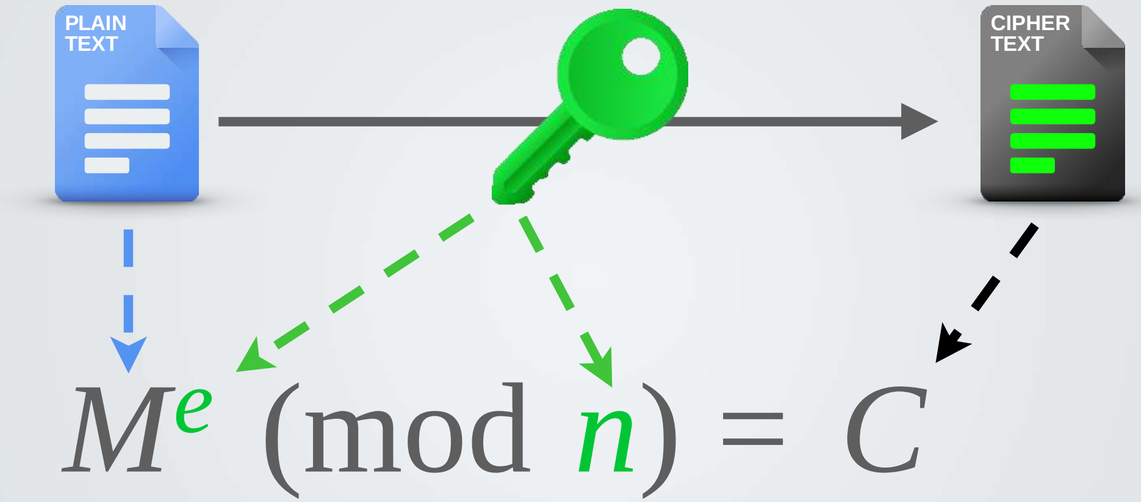
Vuol dire che 44 / 6 = 7
con un resto di 2

In conclusione…

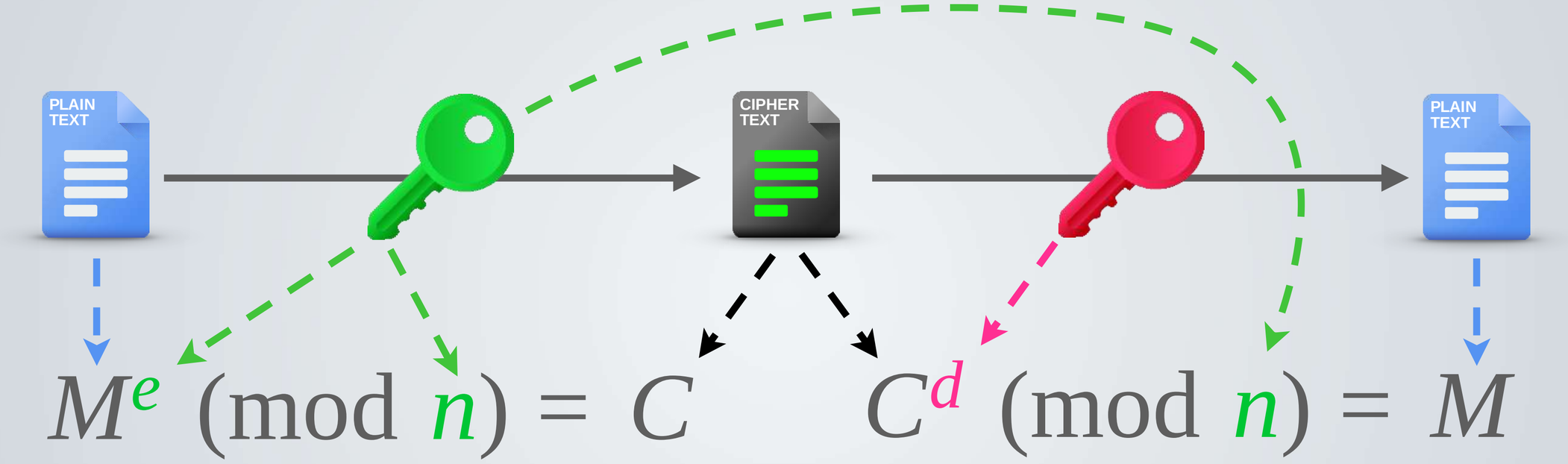
$$44^1 \pmod 6 = 2$$

Torniamo ora a RSA…

Encryption function



Principio di identità



Funzione di crittografia

Funzione di decrittografia

Esiste quindi un numero *d* che mi permette di tornare al messaggio originale

Dai, non ci credo che funziona

Proviamo utilizzando wolframalpha.com

- $M = 42$
- $e = 17$
- $n = 3233$
- $d = 2753$

$$M^e \pmod{n} = C$$

$$C^d \pmod{n} = M$$

Soluzione:

$42^{17} \pmod{3233} = 2557$ $\qquad$ $2557^{2753} \pmod{3233} = 42$

Abbiamo capito che con la funzione modulo possiamo cifrare e decifrare… ma come funziona RSA?

All’inizio, A possiede p e q, due numeri primi molto grandi

$$p \cdot q = n$$

Primo pezzo della chiave pubblica

Scegliere due numeri primi molto grandi

E già qui, è un casino: come troviamo numeri primi da 2048 bit?

Test di Miller-Rabin

```
write n as 2^r·d + 1 with d odd (by factoring out powers of 2 from n − 1)
WitnessLoop: repeat k times:
   pick a random integer a in the range [2, n − 2]
   x ← a^d mod n
   if x = 1 or x = n − 1 then
      continue WitnessLoop
   repeat r − 1 times:
      x ← x^2 mod n
      if x = n − 1 then
         continue WitnessLoop
   return "composite"
return "probably prime"
```

Test di Miller-Rabin

È un ciclo!!

non abbiamo una formula singola che ci dia la risposta, per ogni numero dobbiamo provare le varie divisioni e sperare di trovare un divisore abbastanza in fretta

Possiamo quindi dire che

Trovare due primi grandi non è semplice

Noi però avevamo detto che

$$p \cdot q = n$$

Se ho n, posso trovare *p* e *q* facilmente?

Quanto tempo ci vuole per calcolare?
Facciamo un esempio pratico

$$1889 \cdot 3547 = 6\,700\,283$$ 10s

$$p_1 \cdot p_2 = 6\,700\,283$$???

Quanto tempo serve per scomporre un numero in fattori primi?

Quindi quante divisioni devo fare?

$$p_1 \cdot p_2 = 6\,700\,283$$

$$x(1889) = 290$$

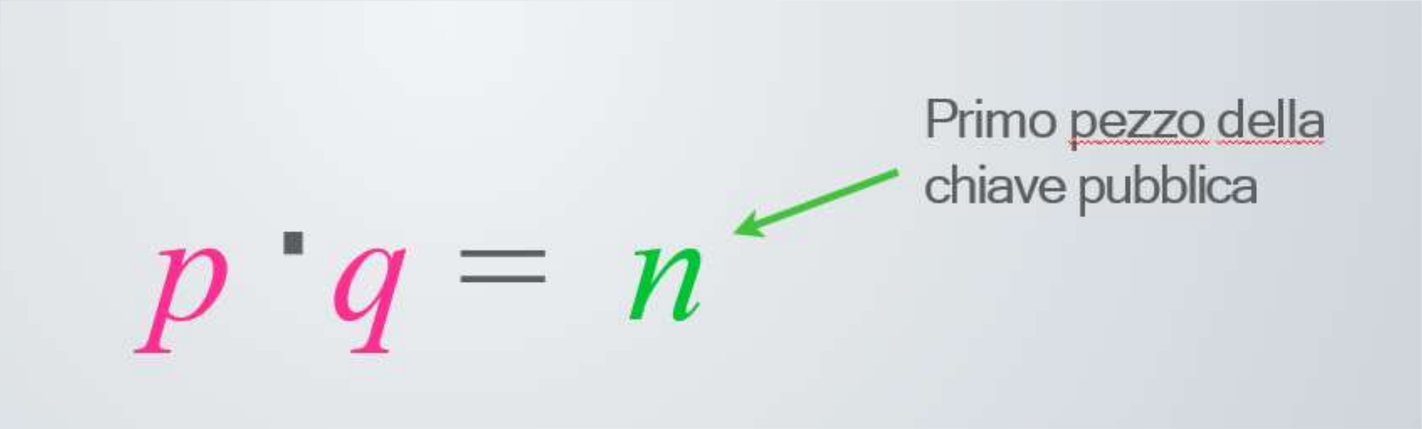
1 moltiplicazione: circa 10 secondi

290 divisioni: circa 48 minuti

$$p_1 \cdot p_2 =$$

22701801293785014193580405120204586741061235962766583907094021879215171483119139894870133091111044901683400949483846818299518041763507948922590774925466088171879259465921026597046700449819899096862039460017743094473811056991294128542891880855362707407670722593737772666973440977361243336397308051763091506836310795312607239520365290032105848839507981452307299417185715796297454995023505316040919859193718023307414880446217922800831766040938656344571034778553457121080530736394535923932651866030515041060966437313323672831539323500067937107541955437362433248361242525945868802353916766181532375855504886901432221349733

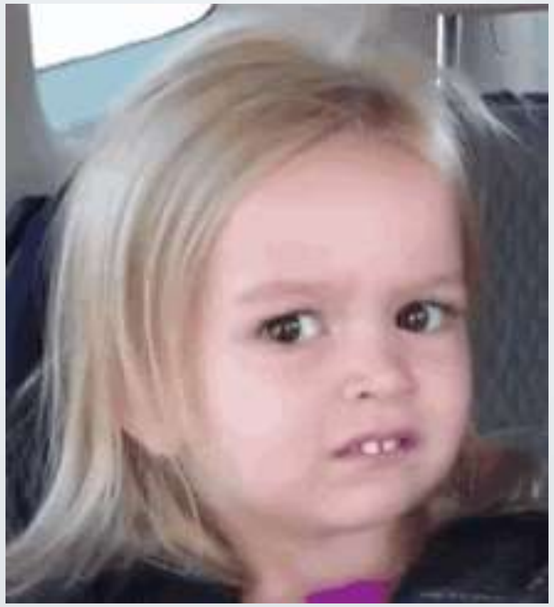
Di conseguenza *n* è sì pubblico, ma anche molto difficile da calcolare!



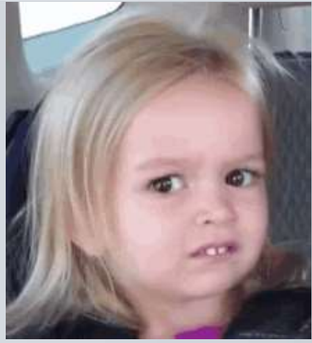
Vediamo ora il secondo pezzo della chiave pubblica

Abbiamo p e q primi e molto grandi.

A partire da questi due numeri calcoliamo la Funzione di Eulero



Calcolare la funzione $\varphi(n)$



Leonhard Euler

Basilea, 15 aprile 1707

San Pietroburgo, 18 settembre 1783

La funzione φ di Eulero (detta anche *funzione toziente*) è definita per ogni z come il numero degli interi compresi tra 1 e z coprimi con z.

Gli interi a e b si dicono coprimi se e solo se non hanno nessun divisore comune, eccetto 1 e -1 o, in modo equivalente, se il loro M.C.D. è 1.

Ad esempio, 2 e 5 sono coprimi, perché non hanno nessun divisore comune, mentre 14 e 7 non sono coprimi perché entrambi sono divisibili per 7.

In poche parole…

$$n = pq$$

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

E cosa ce ne facciamo?

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

Scegliamo un numero più piccolo di $\varphi(n)$ e coprimo con $\varphi(n)$

Questo numero lo chiamiamo e

Ed ecco la nostra chiave pubblica

Dati pubblici

n , e

E la nostra chiave privata

d

$d = e^{-1} (\mathrm{mod}\ \varphi(n))$

Oppure

$ed \equiv 1 (\mathrm{mod}\ \varphi(n))$

Da due numeri primi grandi *p* e *q* abbiamo ottenuto tutto ciò che ci serve

E la nostra chiave privata

d

Dati pubblici

n , e

Per inviare messaggi…

d

n , e

$C^d \pmod{n} = M$

$M^e \pmod{n} = C$

Per inviare messaggi…

d

n , e

$C^d \pmod{n} = M$

$M^e \pmod{n} = C$

- Solo Alice possiede *d* e quindi solo lei può decifrare!
- *de = 1 (mod* φ(*n*)) quindi i due esponenti ‘’si eliminano’’ lasciandoci solo con M

Riassumendo…

1. Scegliere due numeri primi molto grandi p e q;
2. Calcolare $n = p \cdot q$;
3. Calcolare $\varphi(n) = (p-1) \cdot (q-1)$;
4. Scegliere e coprimo e minore di $\varphi(n)$;
5. Risolvere $ed \pmod{\varphi(n)} = 1$ per calcolare d;
6. Cancellare p e q;
7. Tenere segreta la chiave privata d e distribuire la chiave pubblica (e, n).

Com’è possibile che sia sicuro??

In fondo, per individuare la chiave privata d è sufficiente per Eve risolvere l’equazione

$$ed \pmod{\varphi(n)} = 1$$

Come può agire Eve?

L'attaccante ha però due incognite: la chiave privata d e la funzione toziente $\varphi(n)$.

1. Cercare di trovare d a tentativi (ma abbiamo detto che stiamo lavorando con numeri **grandi**)
2. Contare i coprimi con e (**non** conosciamo una formula)
3. Fattorizzare (**non** conosciamo una formula).

Tutti i calcoli sono computazionalmente impossibili.

RSA factoring Challenge

Le chiavi RSA oggi comunemente usate sono di 2048 bit.

Il più grande *n* ad oggi fattorizzato è RSA-250 , un numero di 829 bit.

RSA-250

```
14032465024074496126442307283933563008614715144755017797754920881
41802344714013664334551909580467961099285187247091458768739626192155736304745477052080511905649310668769159001975940569345745223058932597669747168173806936489469987157849495937497937
```

=

```
64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367
```

x

```
33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711
```

The greatest cryptographers of all time

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Blind signature

Cos’è la blind signature?

Letteralmente, ‘’firma cieca’’

Ha l’obiettivo di far firmare il messaggio dal firmatario, senza rivelarne il contenuto.

Questo si ottiene cifrando il contenuto del messaggio prima di farlo firmare. Il messaggio firmato viene decodificato solo alla ricezione da parte del destinatario.

Cos’è la blind signature?

Il messaggio firmato viene decodificato solo alla ricezione da parte del destinatario. Una volta decifrato il messaggio, la blind signature può essere verificata come una normale firma digitale.

Le blind signatures si basano su un sistema di firma digitale a chiave pubblica. Molto utilizzato è RSA.

Perché è utile?

Le blind signature sono utilizzate da molti paesi che consentono il voto elettronico.

Facciamo un esempio pratico…

Perché è utile?

Un elettore va al seggio per votare. Gli viene consegnata una scheda, che compila con le sue preferenze di voto e che richiude secondo le istruzioni.

Un funzionario inserisce poi la scheda all’interno di una busta foderata di carta carbone.
All’esterno della busta ci sono solo le credenziali dell’elettore, in modo da non confonderla con altre buste.

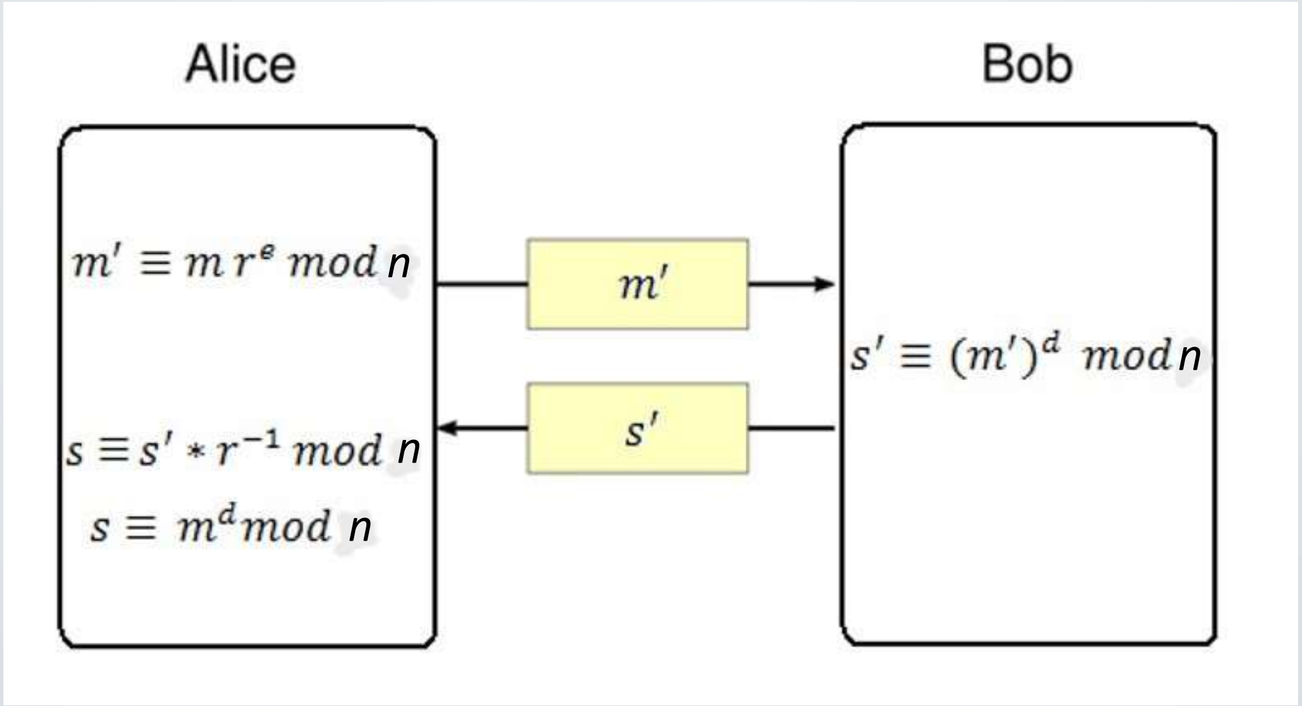
Perché è utile?

Il funzionario firma la busta, trasferendo così la sua firma alla scheda interna attraverso la carta carbone.

La busta viene restituita all’elettore, che la apre e trasferisce la scheda in una busta normale, non segnata, pronta per essere inviata per lo scrutinio.

Cosa c’entra RSA?

Ecco un’implementazione della blind signature che fa uso di RSA



Vediamolo con calma e nel dettaglio

Vuole inviare a B un messaggio *m*

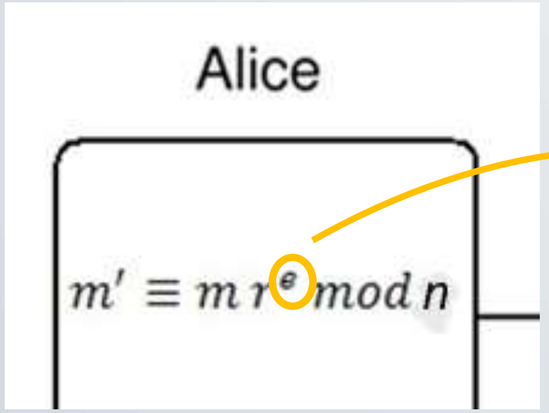
Chiave pubblica → (n,e)

Chiave privata → d

r si chiama *blinding factor*

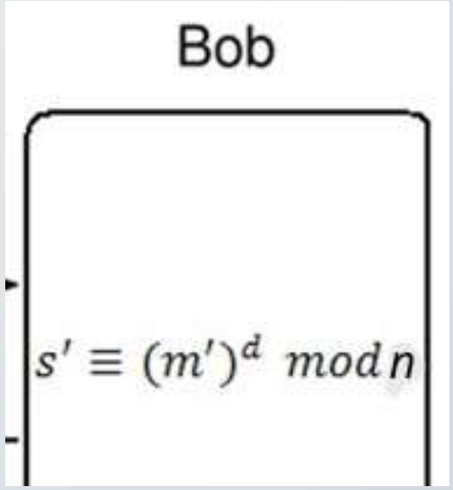
Sceglie un numero casuale *r* (coprimo con *n*) e calcola

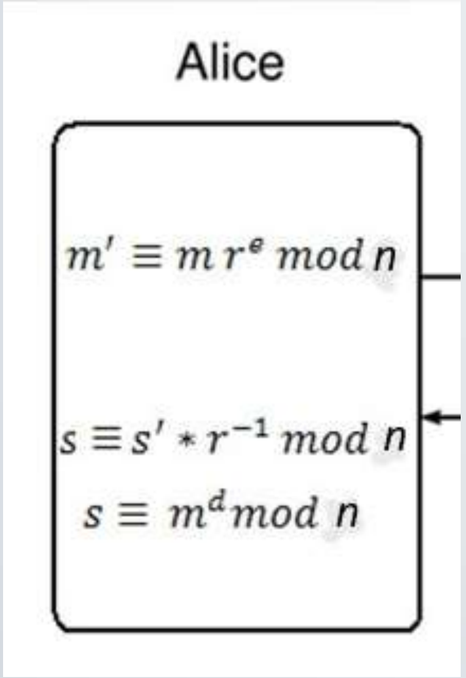
Chiave pubblica → (n,e)
Chiave privata → d



Utilizza la chiave pubblica di B per il calcolo!

Riceve m’ e chiude con la sua chiave privata





Riceve s’

$$s' = (m\, r^e)^d \bmod n$$

Per come è fatto RSA, sappiamo che

$$ed \bmod n = 1$$

Perciò

$$s' = m^d r \bmod n$$

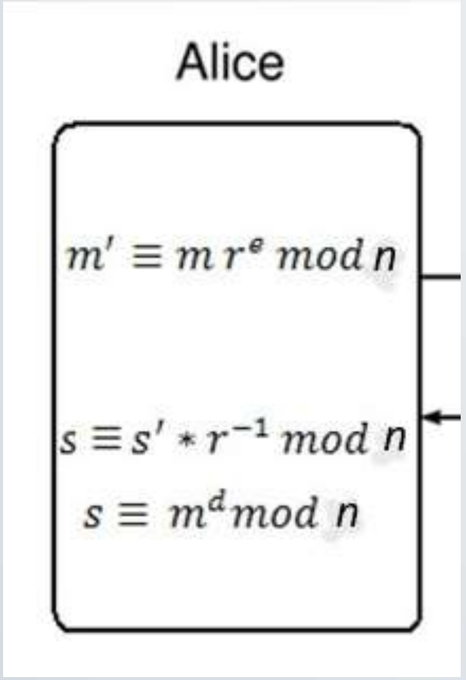
$$s' = m^d r \bmod n$$

A può allora togliere il suo *blinding factor*

$$s = m^d \, r \, \frac{1}{r} \bmod n$$

E ottiene quindi

$$s = m^d \bmod n$$



$$s = m^d \bmod n$$

È il messaggio di A chiuso con la chiave privata di B!

Il messaggio di A è quindi stato firmato senza che B vedesse il contenuto (non gli è mai arrivato *m* ‘’da solo’’)

Chiunque può verificare la firma di B utilizzando la sua chiave pubblica.

Link utili

- Cosa sono le blind signatures - https://blog.bitnovo.com/it/cosa-sono-le-blind-signatures/?cn-reloaded=1

- RSA step by step - https://www.youtube.com/watch?v=iMR1KIAzjYA