PIEMONTE
FONDI STRUTTURALI E DI INVESTIMENTO EUROPEI 2014/2020
fondo sociale europeo
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Crittografia RSA

Sicurezza informatica

v 2.0.1 ~ feb 2022

Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:
ISTITUTI TECNICI SUPERIORI
Ministero dell'Istruzione
UNIONE EUROPEA
REGIONE PIEMONTE
per una crescita intelligente, sostenibile ed inclusiva
www.regione.piemonte.it/europa2020
INIZIATIVA CO-FINANZIATA CON FSE

I favolosi anni ‘70

1969 — ArpaNet

1971 — FTP

1974 — TCP

1978 — IP v4

New Directions in Cryptography

Martin Hellman on cryptography

Diffie explains public-key encryption

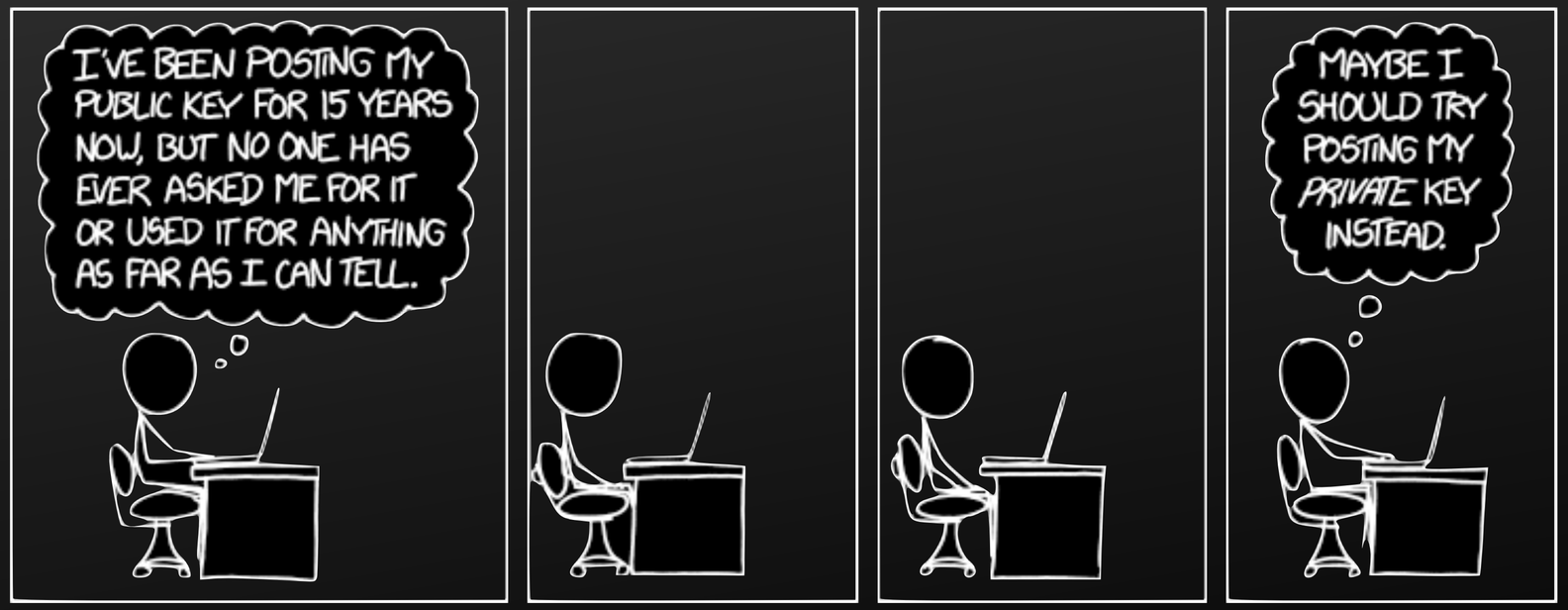
Rivest on the origins of RSA

“We propose that it is possible to develop systems in which two parties communicating solely over a public channel and using only publicly known techniques can create a secure connection. We examine two approaches to this problem, called **public key cryptosystems** and **public key distribution systems**, respectively. The first are more powerful, lending themselves to the solution of the authentication problems, while the second are much closer to realization. ”

New Directions in Cryptography, Whitfield Diffie e Martin Hellman, novembre 1976

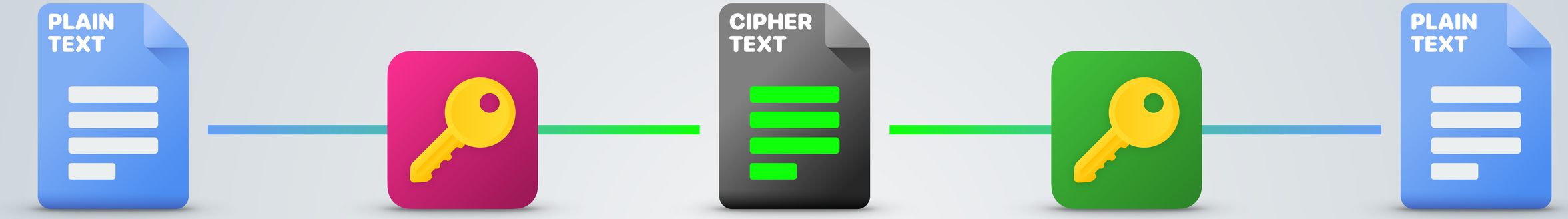
POR Piemonte
FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE



1 Public Key Encryption

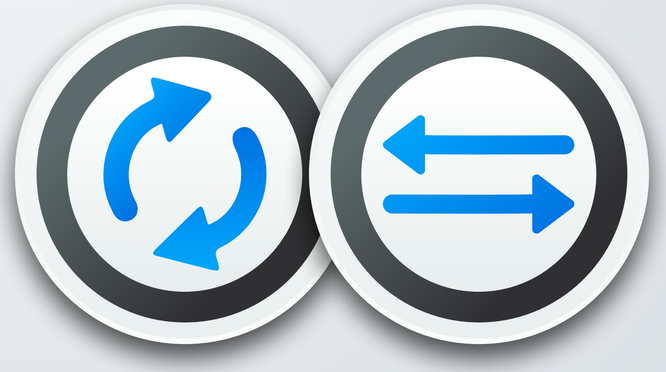
Cifrari simmetrici



Encryption

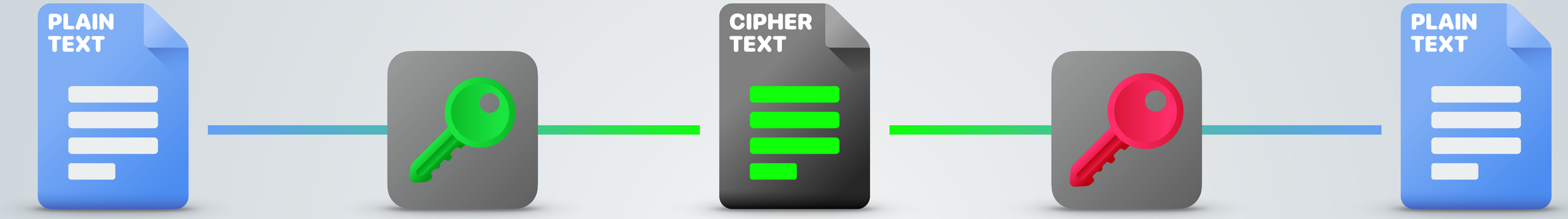
Decryption

Simmetria



Permutazioni e sostituzioni

Rompere la simmetria



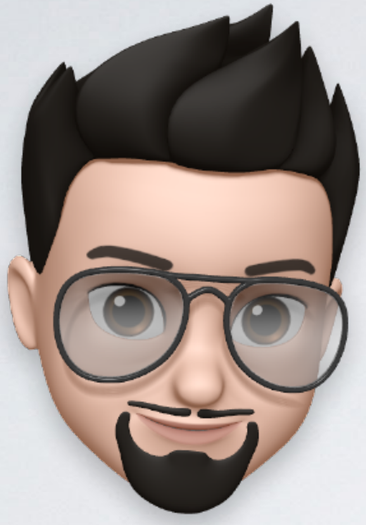
Chiave pubblica

Chiave privata

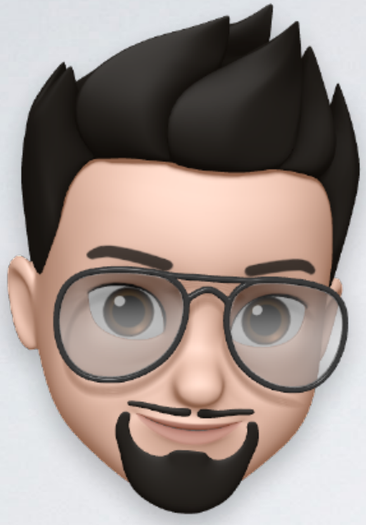
Asimmetria delle chiavi

Basato su funzioni matematiche

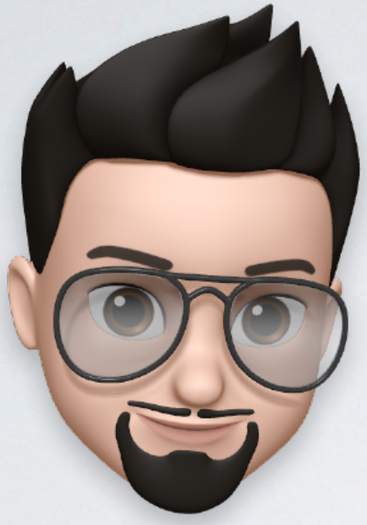
Creare un canale di comunicazione



Creare un canale di comunicazione



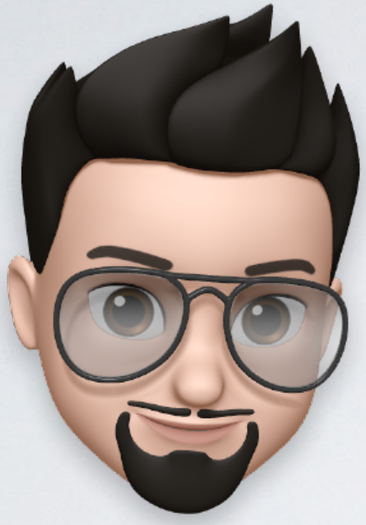
Creare un canale di comunicazione



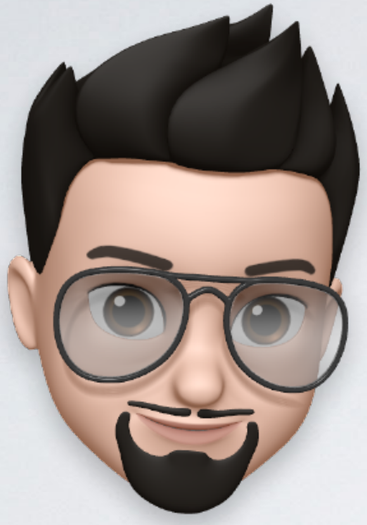
canale cifrato

Dopo essersi scambiati le chiavi pubbliche Alice e Bob hanno instaurato un canale di comunicazione sicuro.

Inviare un messaggio crittografato

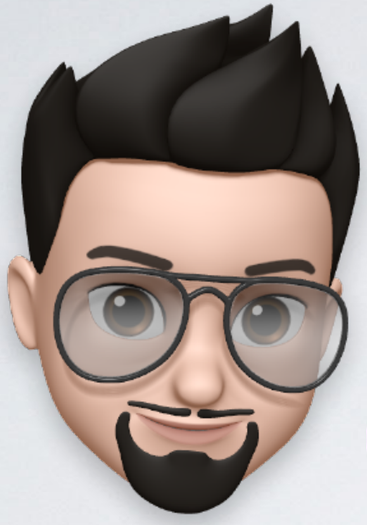


Inviare un messaggio crittografato



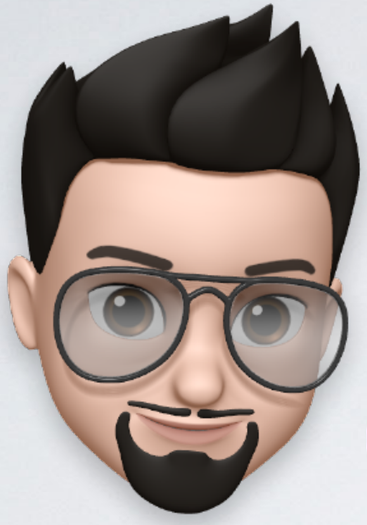
Steve only won because I let him, lol.

Inviare un messaggio crittografato



Steve only won because I let him, lol.

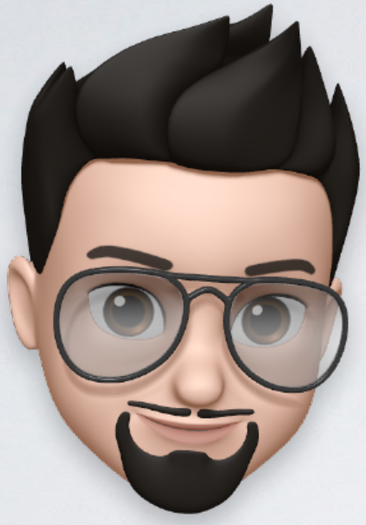
Inviare un messaggio crittografato



```
HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO
```

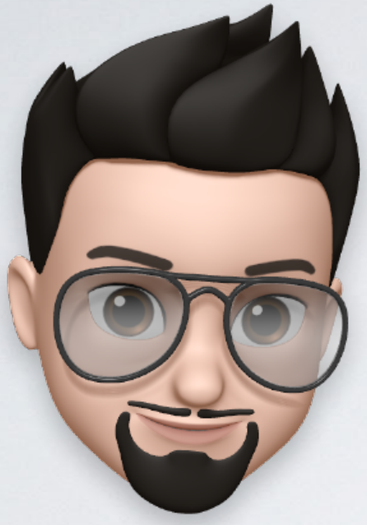
Bob usa la chiave pubblica di Alice
per crittografare il messaggio.

Inviare un messaggio crittografato

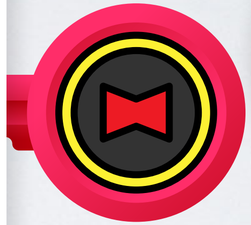


```
HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO
```

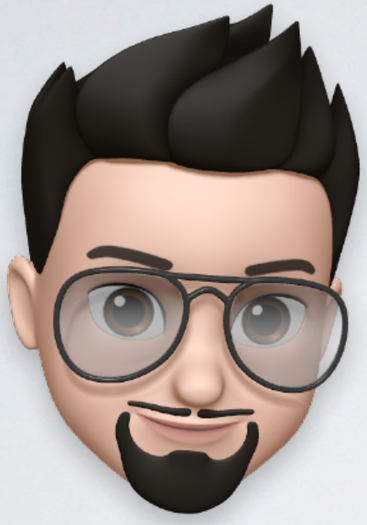
Inviare un messaggio crittografato



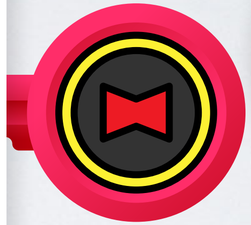
```
HQT3E0m5O
kmKbMPMad
fQqwDrRdr
HGmYshCb4
qOKy6w7RR
Fgtbr6Mh4
8U1QVEIcO
```



Inviare un messaggio crittografato

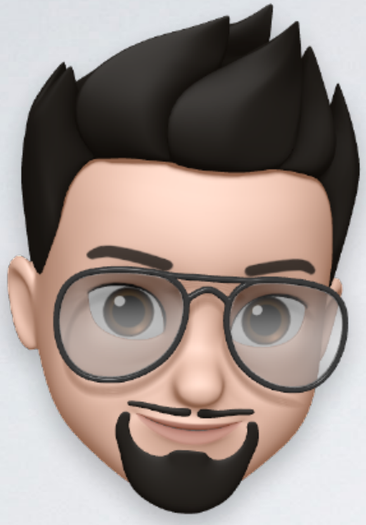


Steve only
won because
I let him, lol.



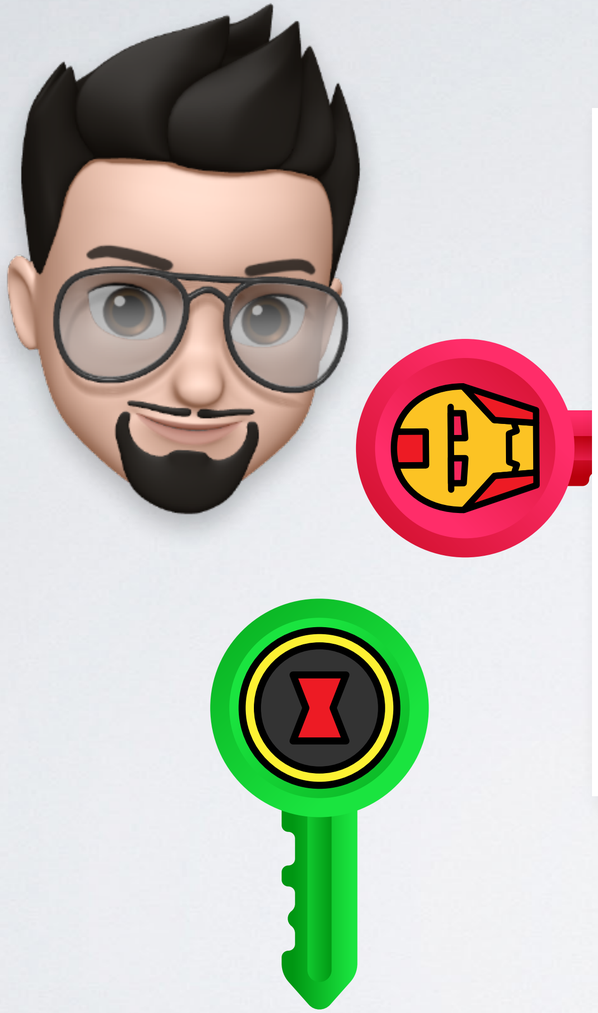
Alice usa la sua chiave privata per
decrittare il messaggio inviato da Bob.

Inviare un messaggio ...?

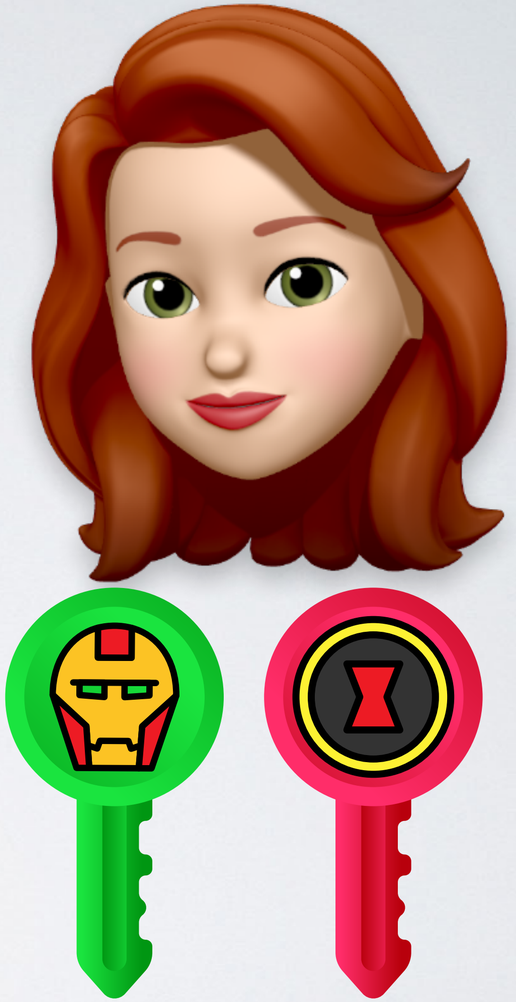


Steve only
won because
I let him, lol.

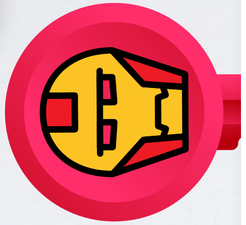
Inviare un messaggio ...?



Steve only won because I let him, lol.



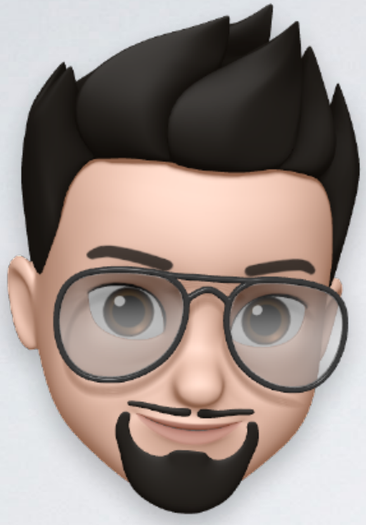
Inviare un messaggio ...?



```
1LbK3ofOf
0LFTkfxVM
BanTep6Pn
cUciDVOVG
UpWjRbl6O
GZKVCl021
vC7SdNxJm
```

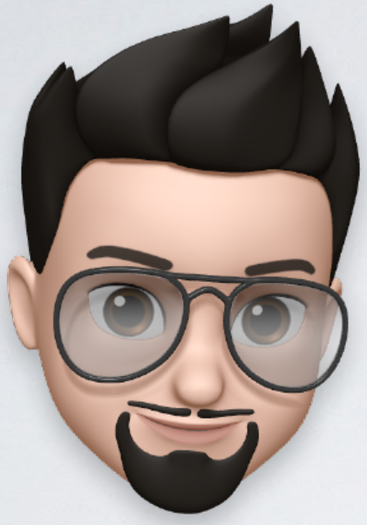
Bob usa la sua chiave privata per crittografare il messaggio.

Inviare un messaggio ...?

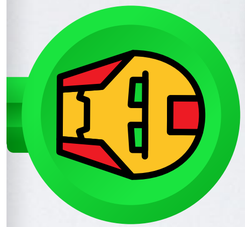


```
1LbK3ofOf
0LFTkfxVM
BanTep6Pn
cUciDVOVG
UpWjRbl6O
GZKVCl021
vC7SdNxJm
```

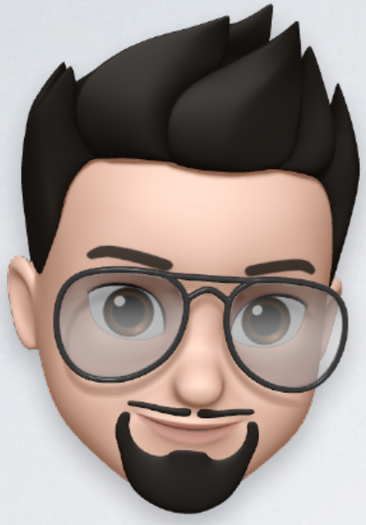
Inviare un messaggio ...?



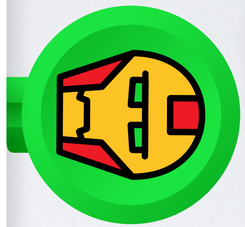
```
1LbK3ofOf
0LFTkfxVM
BanTep6Pn
cUciDVOVG
UpWjRbl6O
GZKVCl021
vC7SdNxJm
```



Inviare un messaggio ...?



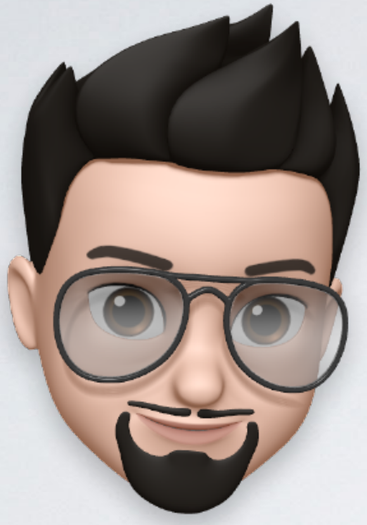
Steve only
won because
I let him, lol.



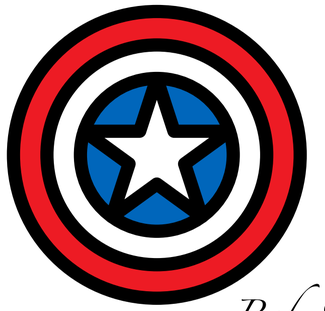
Alice usa la chiave pubblica di Bob per decrittare il messaggio ricevuto.

...perché?

Inviare un messaggio autenticato!



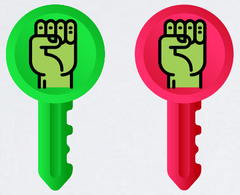
Steve only
won because
I let him, lol.

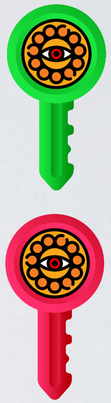


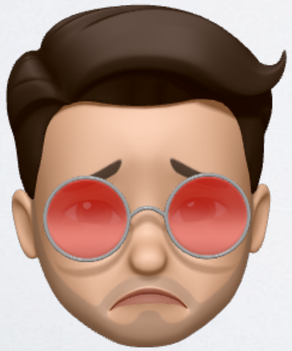
Bob Stark

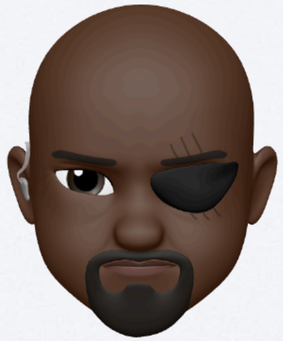
Alice è sicura che il messaggio provenga davvero da Bob. Il messaggio è stato firmato.

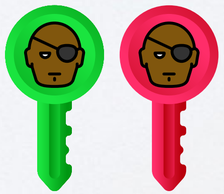
Creare canali cifrati multipli



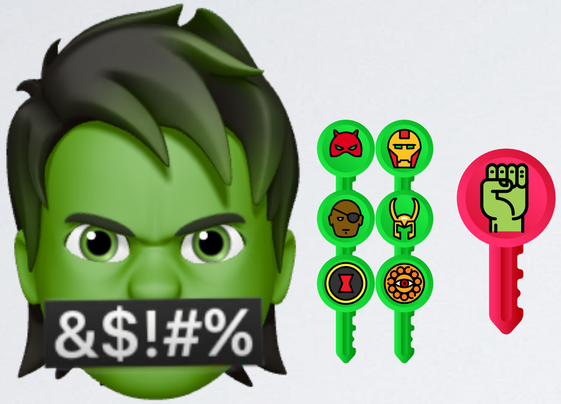


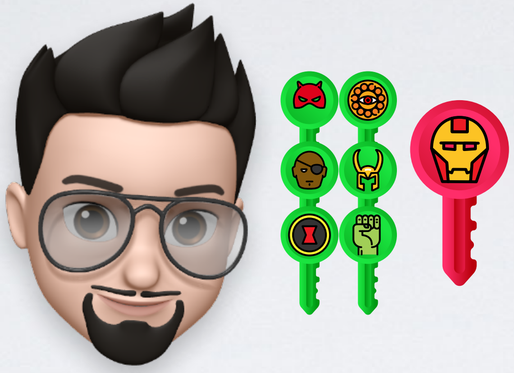


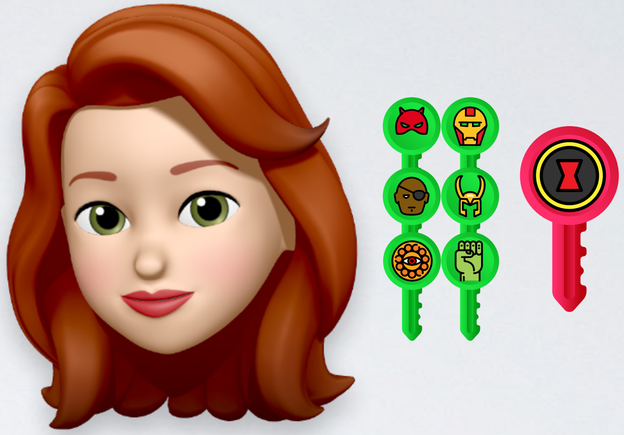


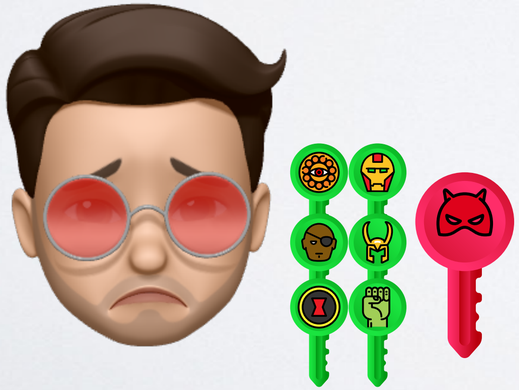


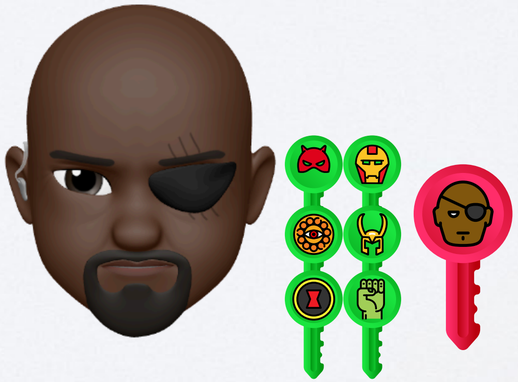
Creare canali cifrati multipli



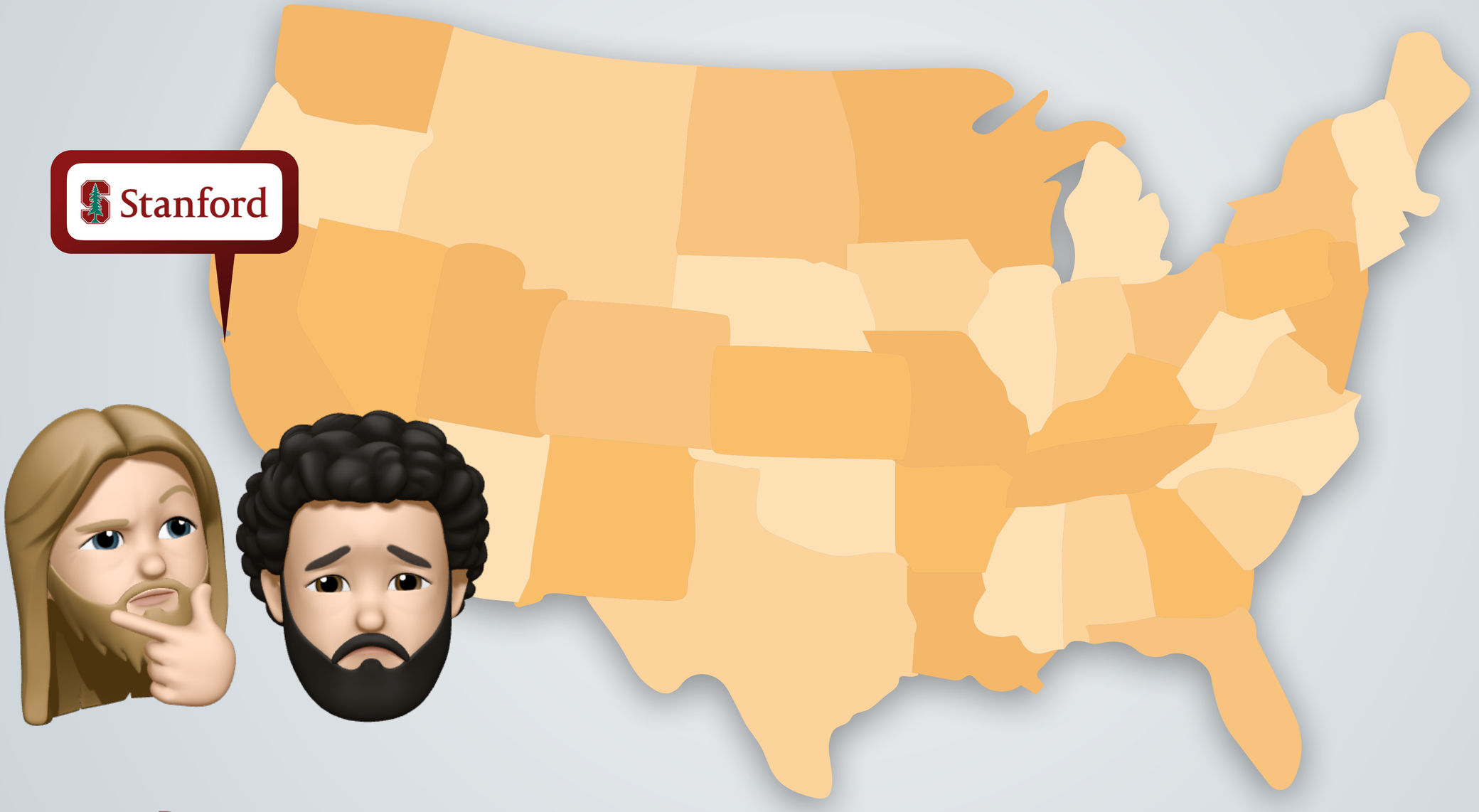






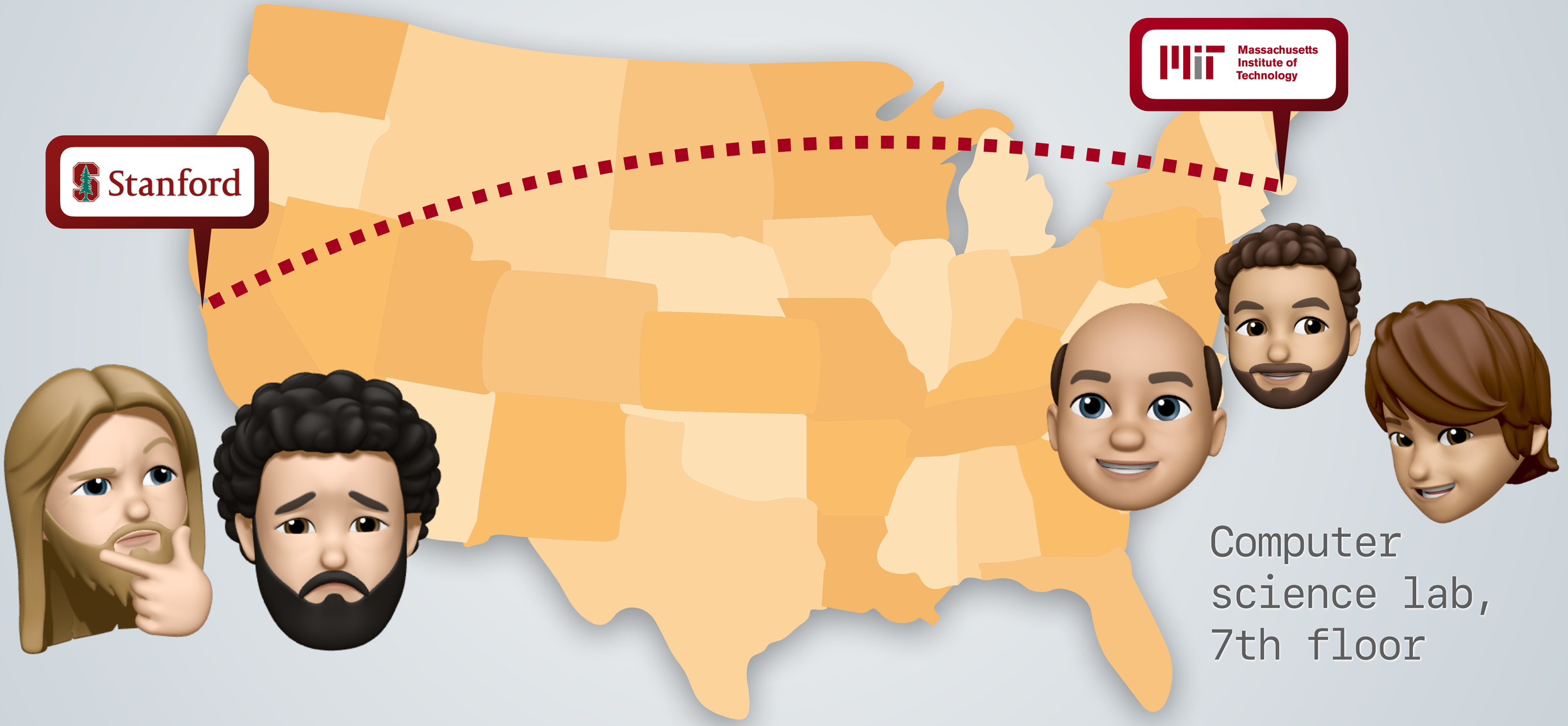


"God rewards fools"



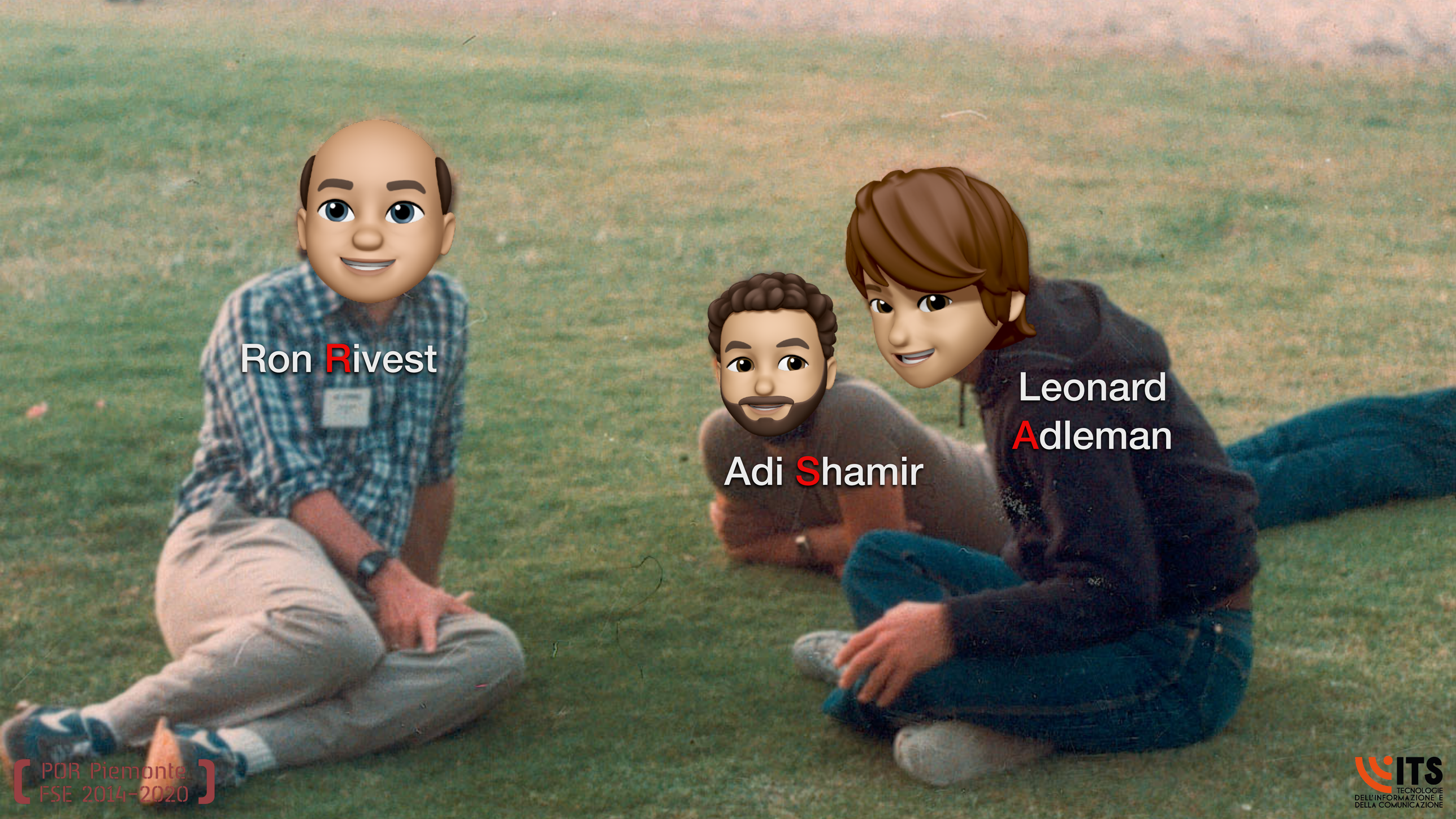
1976...

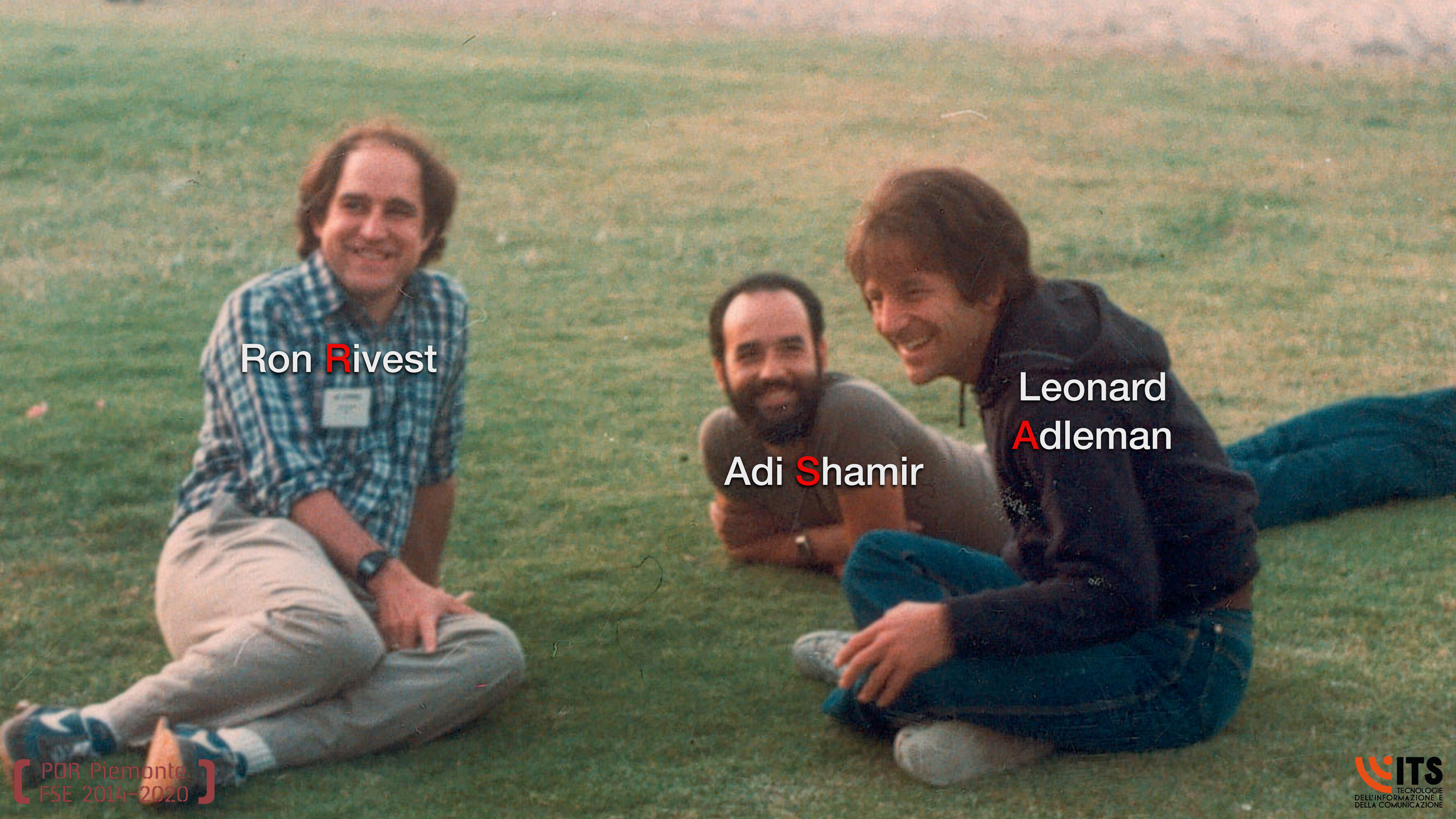
"God rewards fools"

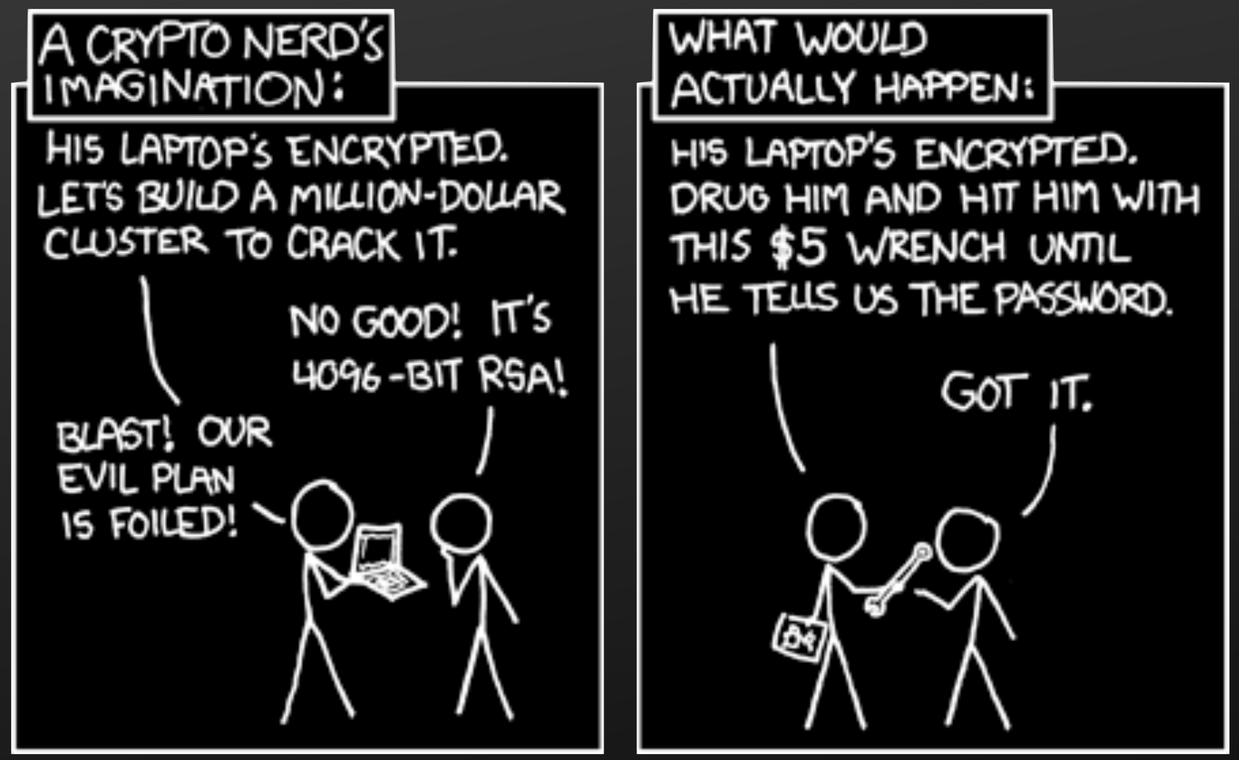


1976...

...1977







2

RSA Encryption

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

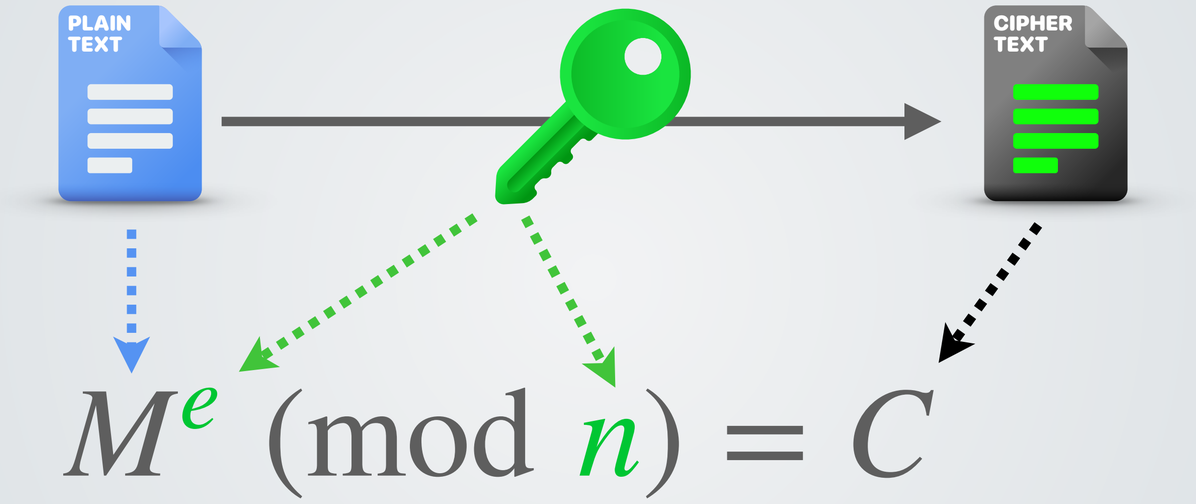
The era of "electronic mail" [
us; we must ensure that two im
the current "paper mail" syster
messages are *private*, and (b) me
We demonstrate in this paper
capabilities into an electronic ma

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

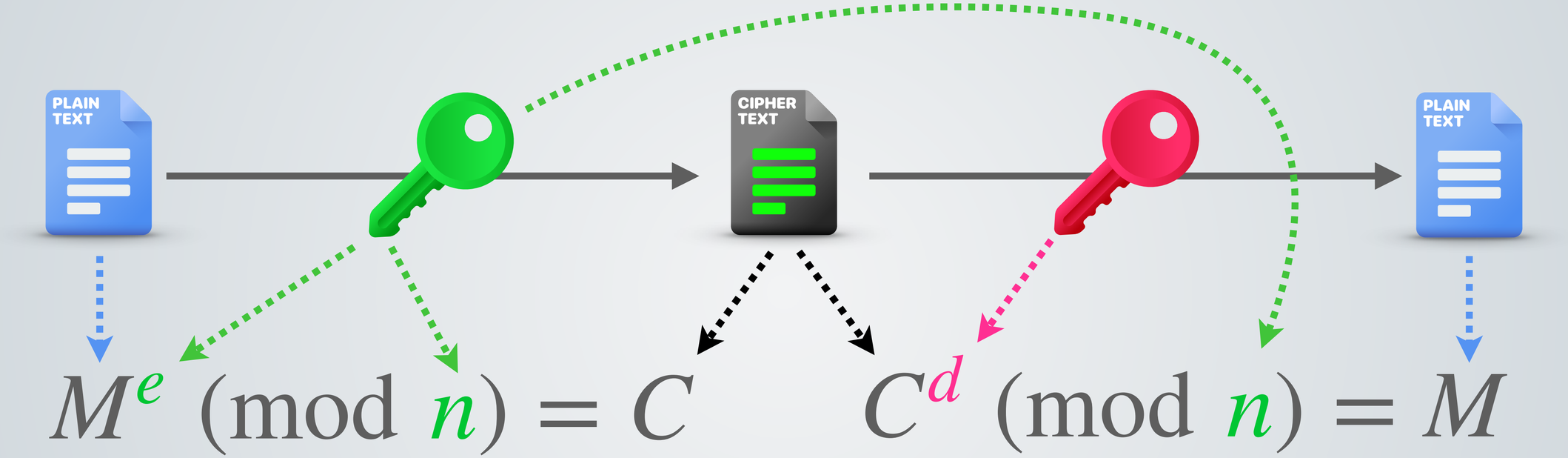
II. Public-Key Cryptosystems

In a "public-key cryptosysten

Encryption function



Principio di identità



Funzione di crittografia

Funzione di decrittografia

Dai, non ci credo che funziona

Bene, allora provate, miscredenti. Eseguite la cifratura e decifratura per verificare il *principio di identità*. Per i calcoli usate wolframalpha.com.

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

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

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

Dai, non ci credo che funziona

Bene, allora provate, miscredenti. Eseguite la cifratura e decifratura per verificare il *principio di identità*. Per i calcoli usate wolframalpha.com.

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

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

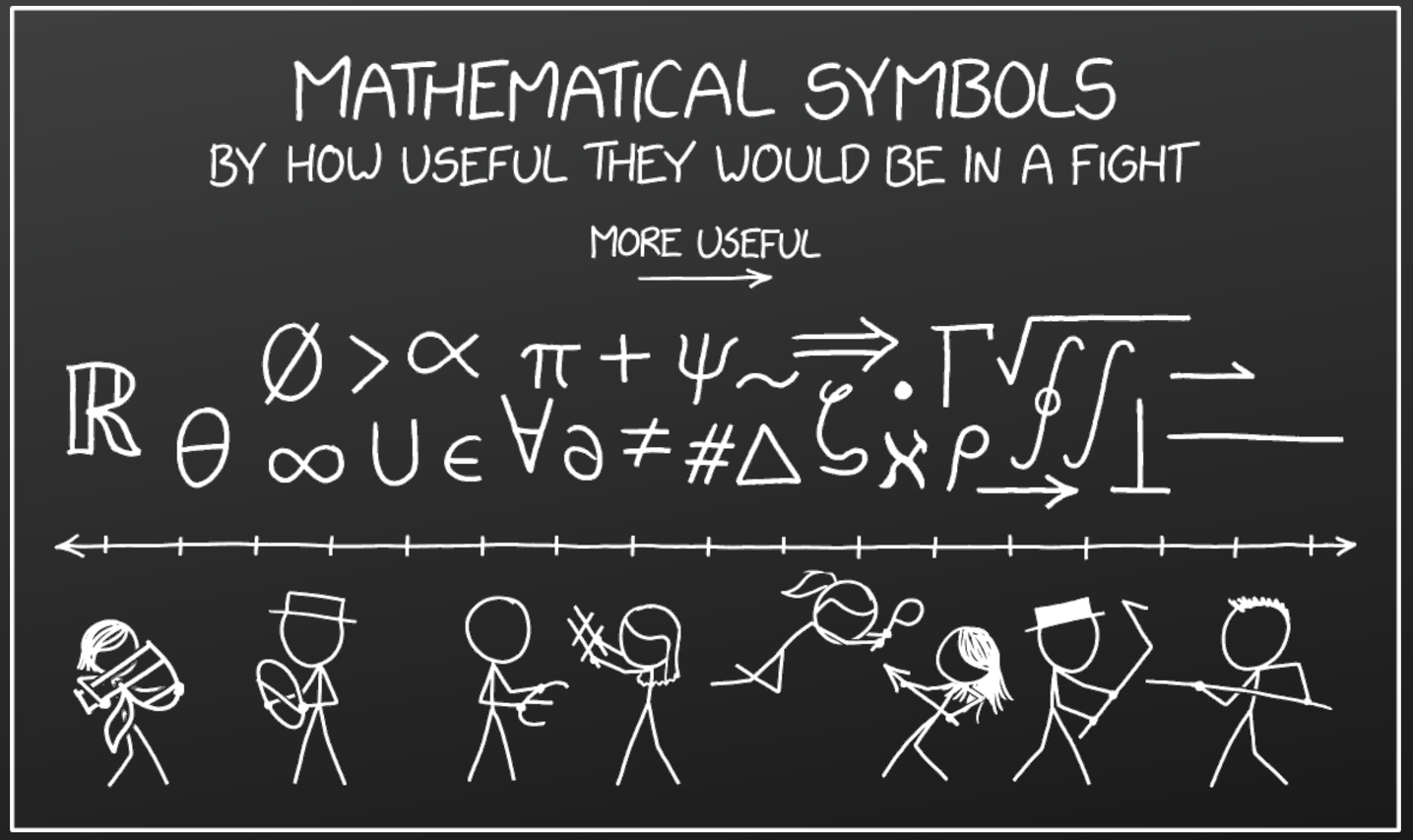
$$C^d \pmod{n} = M$$

Soluzione:

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

POR Piemonte
FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE



3

La matematica di RSA

A caccia di funzioni unidirezionali

Quanto tempo ci vuole
per calcolare ... ?

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

A caccia di funzioni unidirezionali

Quanto tempo ci vuole
per calcolare ... ?

$$1889 \cdot 3547 = 6\,700\,283 \quad \textbf{10s}$$

$$p_1 \cdot p_2 = 6\,700\,283 \quad \textbf{???}$$

Quanto tempo serve per scomporre un numero in fattori primi?

Scomposizione in fattori primi

per gli amici, “fattorizzazione”

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

Come si fattorizza un numero?

- Trovare il più piccolo numero primo p_1 la cui divisione è intera (ovvero dà resto 0).

Abbiamo una formula per calcolarlo?

- No, quindi dobbiamo procedere per divisioni successive.

E quindi quanto tempo ci vuole?

- La complessità computazionale è data dal numero di divisioni che devo fare.

E quante divisioni devo fare?

- Dipende da quanti numeri primi ci sono prima di p_1.

[POR Piemonte FSE 2014-2020]

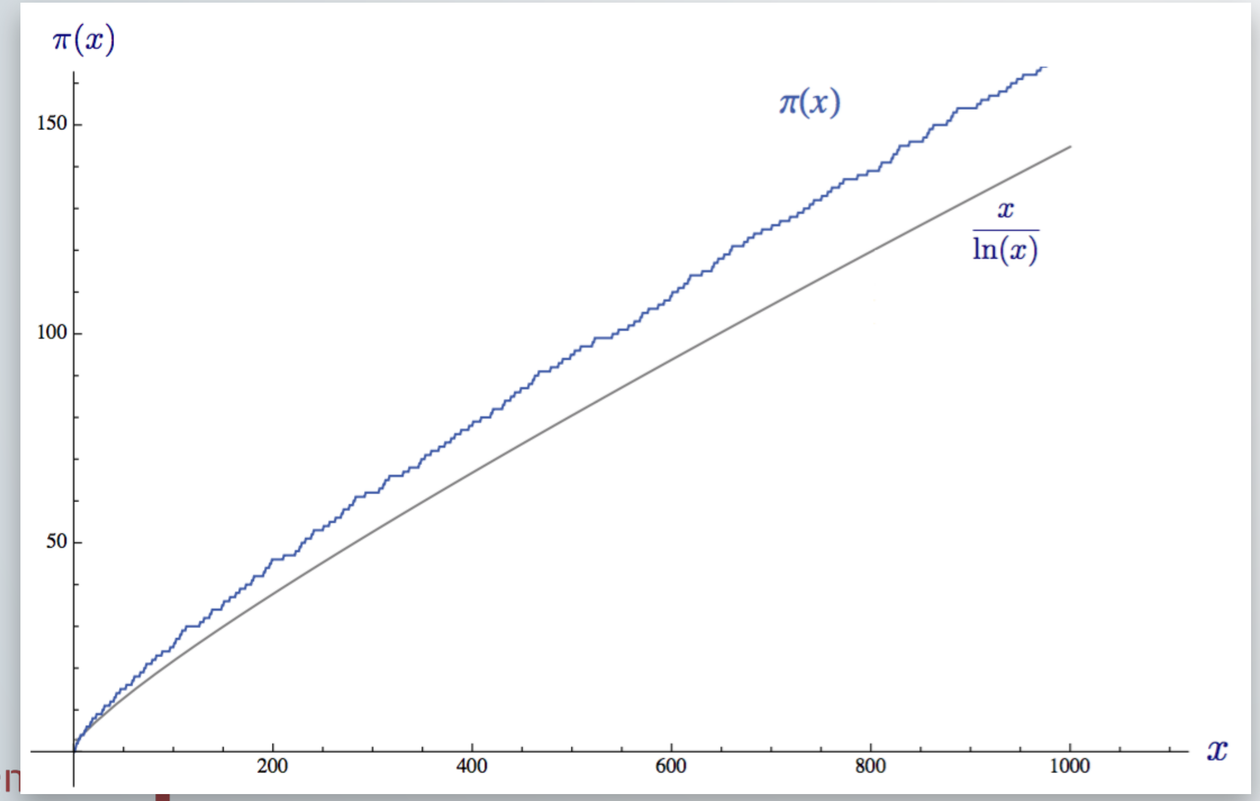
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Quanti numeri primi ci sono prima di x?

Funzione enumerativa $\pi(x)$

Occhio che π in questo caso non ha niente a che fare con il numero $3{,}14\ldots$

Conta quanti numeri primi ci sono prima di x.



La funzione $\pi(x)$ è ad oggi sconosciuta.

È approssimabile con la funzione $x/\ln(x)$.

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Quindi quante divisioni devo fare?

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

$$\pi(1889) = 290$$

$$\frac{1889}{\ln(1889)} \approx 250$$

1 moltiplicazione: circa 10 secondi

290 divisioni: circa 48 minuti

La moltiplicazione di due primi è una funzione unidirezionale.

$$p_1 \cdot p_2 =$$

22701801293785014193580405120204586741061235962766583907094021879215171483119139894870133091111044901683400949483846818299518041763507948922590774925466088171879259465921026597046700449819899096862039460017743094473811056991294128542891880855362707407670722593737772666973440977361243336397308051763091506836310795312607239520365290032105848839507981452307299417185715796297454995023505316040919859193718023307414880446217922800831766040938656344571034778553457121080530736394535923932651866030515041060966437313323672831539323500067937107541955437362433248361242525945868802353916766181532375855504886901432221349733

Tutto molto bello, ma...

come si calcolano le chiave pubblica e privata?

1. Scegliere due numeri primi molto grandi per ottenere n.
2. Calcolare la funzione $\varphi(n)$.
3. Scegliere di conseguenza l'esponente e.
4. Calcolare d.

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"
```

La precisione può essere aumentata a scapito del tempo di esecuzione.

Scegliere due numeri primi molto grandi

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

Test di Miller-Rabin

$$p \cdot q = n$$

Numeri primi molto grandi

Primo pezzo della chiave pubblica

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 $z \in \mathbb{Z}$ 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, 6 e 35 sono coprimi, perché non hanno nessun divisore comune, mentre 6 e 27 non sono coprimi perché entrambi sono divisibili per 3.

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 $z \in \mathbb{Z}$ come il numero degli interi compresi tra 1 e z coprimi con z.

Esempio

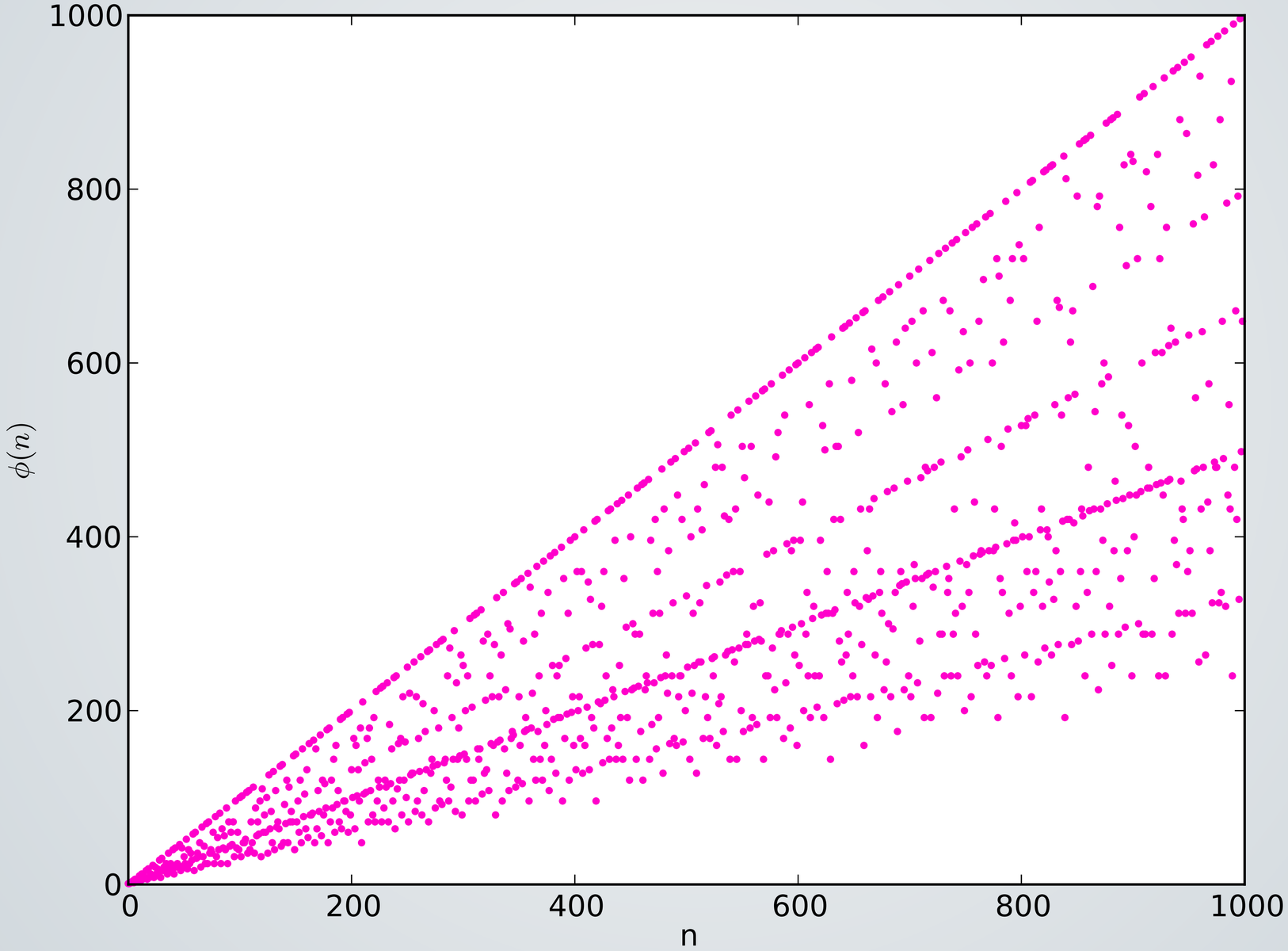
$\varphi(8) = 4$, poiché i numeri minori di 8 coprimi con 8 sono: $1, 3, 5$ e 7.

Quanto vale $\varphi(11)$?

Corollario

$\varphi(11) = 10$, poiché essendo 11 primo, tutti i numeri sono coprimi con esso.

Calcolare la funzione $\varphi(n)$



Cosa sono i punti sulla diagonale?

I numeri primi!

Proprietà della funzione φ

1. Primalità $\varphi(p) = (p - 1)$
2. Moltiplicatività $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

$$n := (p \cdot q) \rightarrow \varphi(n) = \varphi(p \cdot q)$$

$$= \varphi(p) \cdot \varphi(q) \quad \text{(per la moltiplicatività)}$$

$$= (p - 1)(q - 1) \quad \text{(per la primalità)}$$

POR Piemonte
FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Scegliere gli esponenti e e d

Scegliamo un numero e che sia:

- relativamente piccolo, maggiore di 2 e minore di $\varphi(n)$;
- coprimo con $\varphi(n)$.
- gli standard solitamente usano il numero 65537.

Questo numero viene usato per una questione di efficienza computazionale e risparmio energetico. La sua rappresentazione binaria infatti è `0b1000000000000001`, ovvero un numero sufficientemente grande ma con solo due 1 al suo interno.

Scegliere gli esponenti e e d

Scegliamo un numero e che sia:

- relativamente piccolo, maggiore di 2 e minore di $\varphi(n)$;
- coprimo con $\varphi(n)$.
- gli standard solitamente usano il numero 65537.

Calcoliamo la chiave privata d risolvendo l'equazione:

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

Il calcolo è facilmente risolvibile tramite l'*algoritmo esteso di Euclide*.

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).

Crittoanalisi

Per individuare la chiave privata d è sufficiente per Eve risolvere l'equazione

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

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

Eve ha due modi per calcolare $\varphi(n)$:

- contare i coprimi con n (**non** conosciamo una formula) oppure
- fattorizzare n (**non** conosciamo una formula).

Entrambi i calcoli sono computazionalmente impossibili.

RSA factoring Challenge

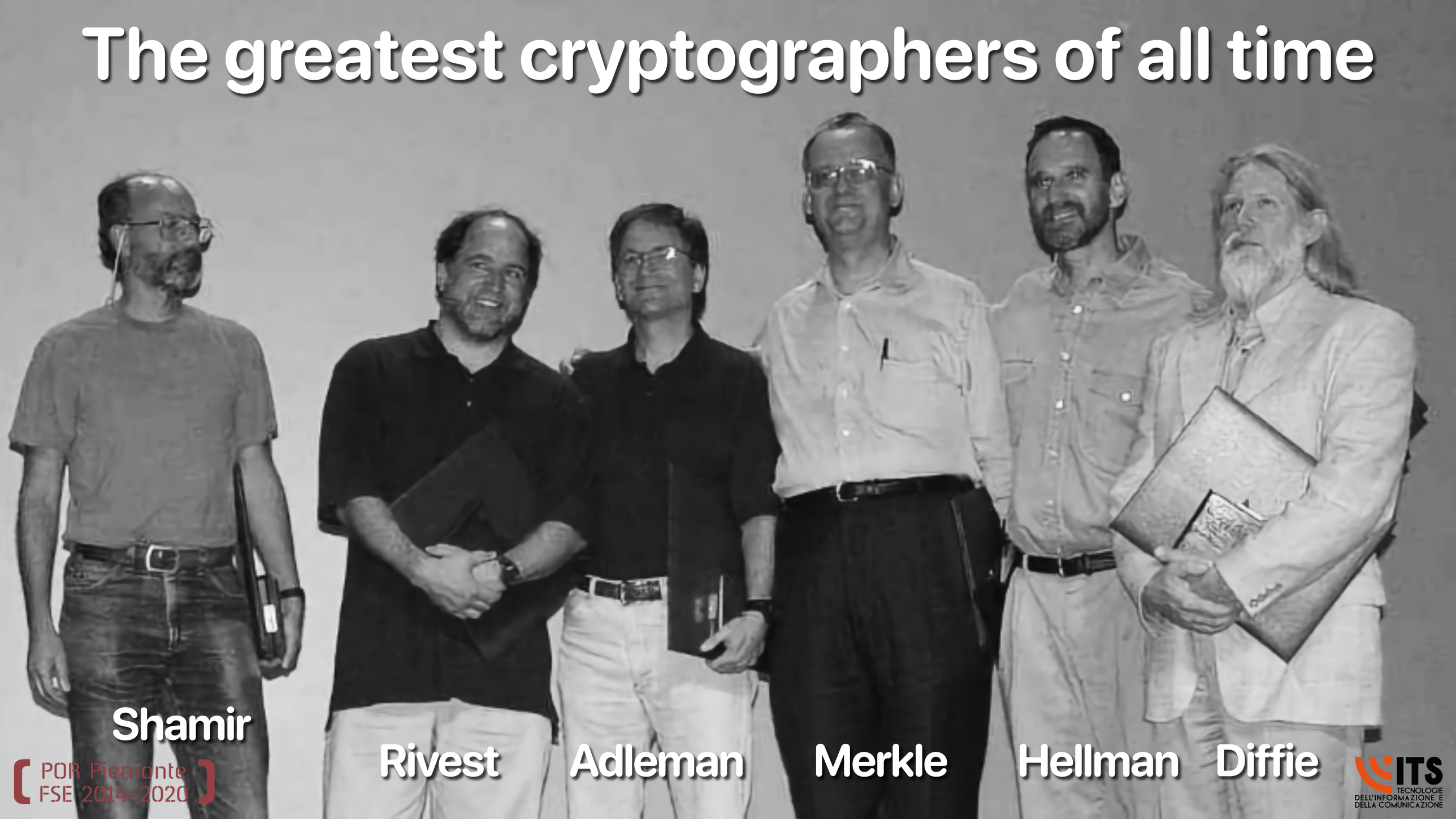
Le chiavi RSA oggi comunemente usate sono di 2048 bit.

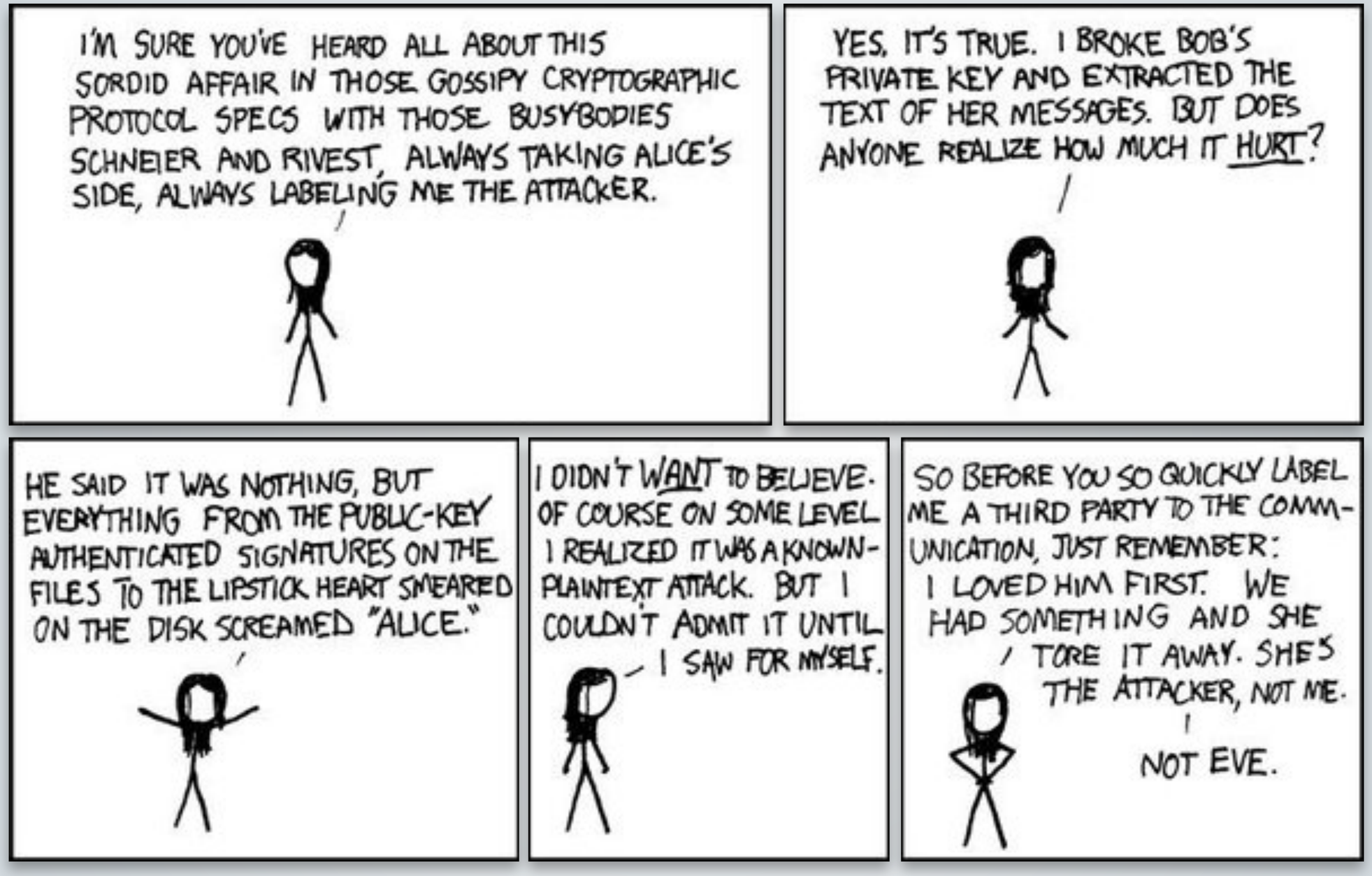
Il più grande n ad oggi (3 marzo 2021) fattorizzato è RSA–250, un numero di 829 bit.

RSA–250

```
14032465024074496126442307283933563008614715144755017797754920881
41802344714013664334551909580467961099285187247091458768739626192155736304745477052080511905649310668769159001975940569345745223058932597669747168173806936489469987157849497593749793
=
64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367
x
33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711
```

The greatest cryptographers of all time




I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.
YES. IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?
HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."
I DIDN'T WANT TO BELIEVE. OF COURSE ON SOME LEVEL I REALIZED IT WAS A KNOWN-PLAINTEXT ATTACK. BUT I COULDN'T ADMIT IT UNTIL I SAW FOR MYSELF.
SO BEFORE YOU SO QUICKLY LABEL ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER: I LOVED HIM FIRST. WE HAD SOMETHING AND SHE TORE IT AWAY. SHE'S THE ATTACKER, NOT ME.
NOT EVE.