Alumni Mathematica

Crittografia

da Whatsapp a Wikileakes, tra spie e segreti di stato

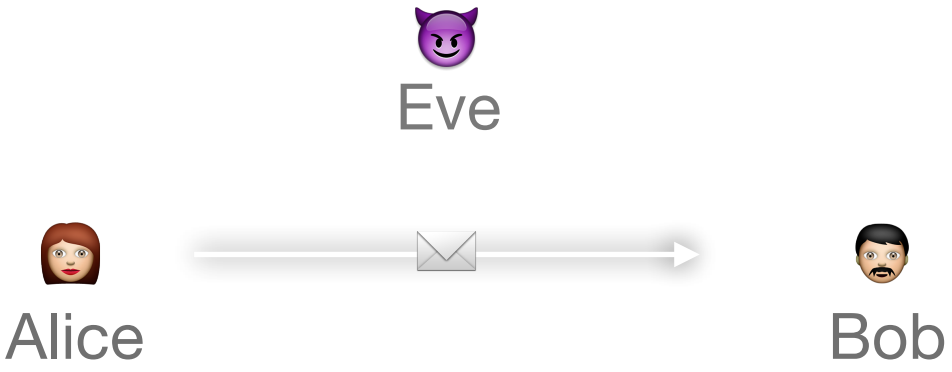
Donatella Iacono Sabina Milella

BGeek
BARIGEEKFEST2015
27/2806 PALAFLORIO

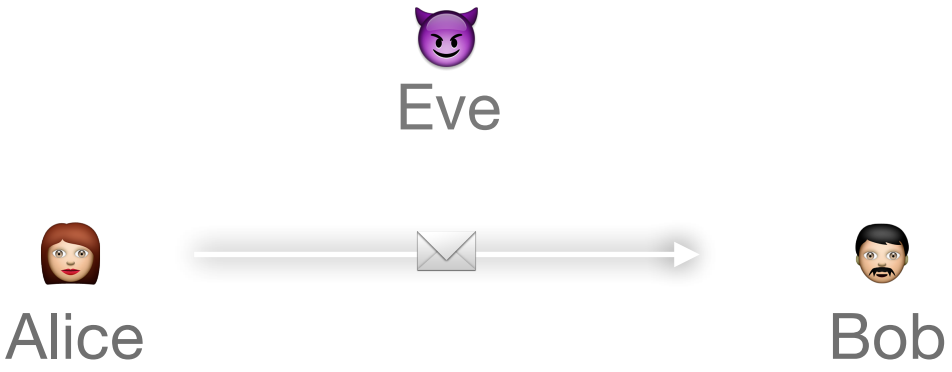
Bari | 27.06.2015

Crittografia…ne abbiamo piene le tasche!

C’era una volta…



C’era una volta…



Scopo

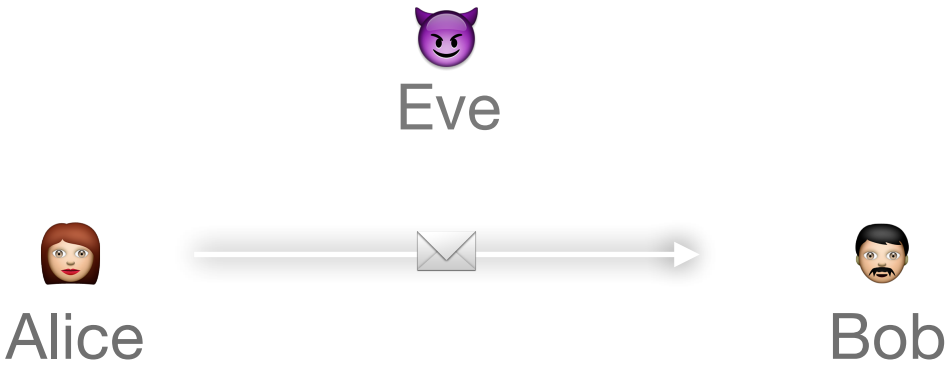
Spedire un messaggio in modo che solo Bob possa leggerlo e comprenderlo

Come?

modificare il messaggio = cifrare il messaggio

C’era una volta...

kryptos = nascosto + graphia = scrittura → crittografia



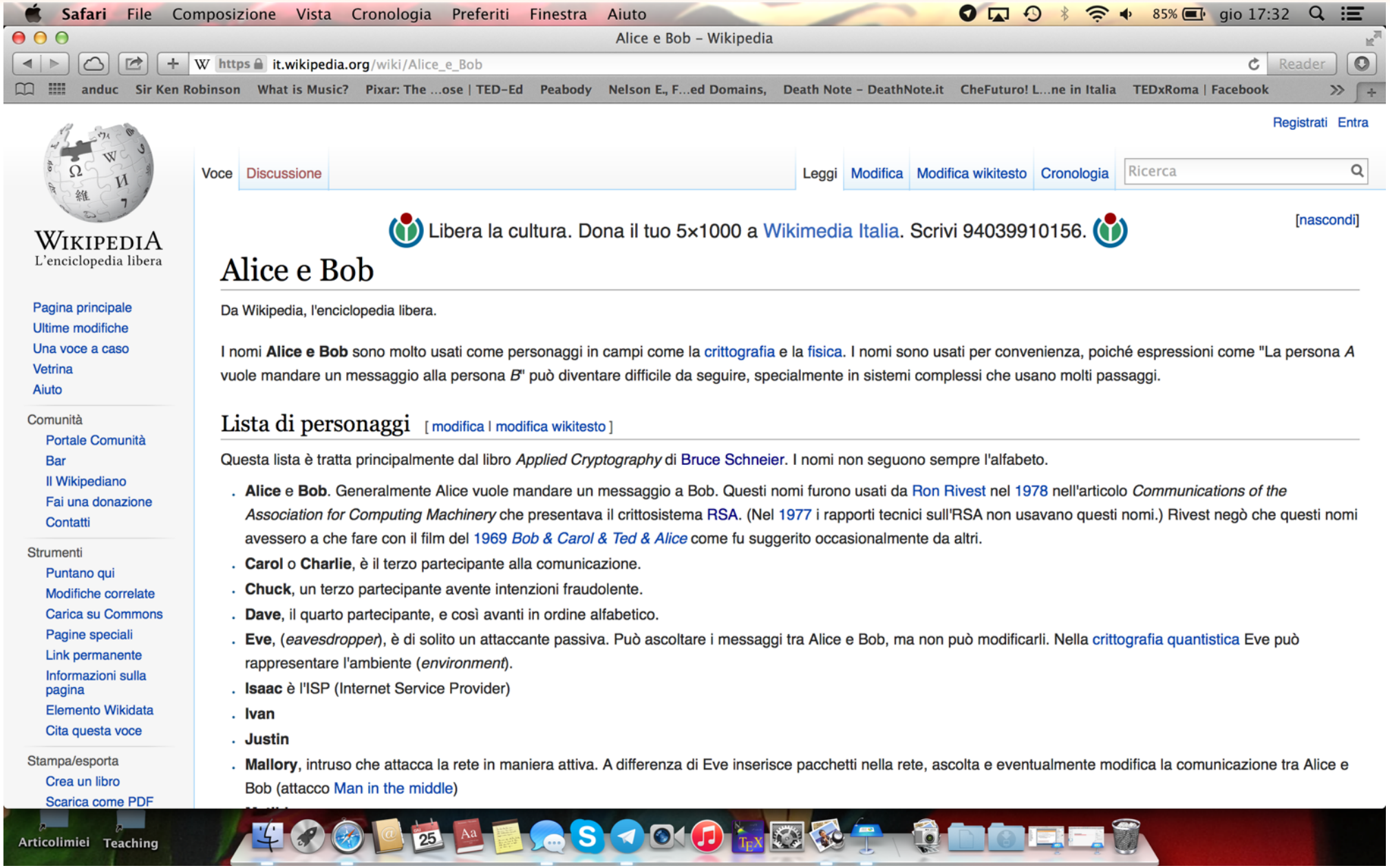
Scopo

Spedire un messaggio in modo che solo Bob possa leggerlo e comprenderlo

Come?

modificare il messaggio = cifrare il messaggio

Non solo Eve!


Safari File Composizione Vista Cronologia Preferiti Finestra Aiuto
85% gio 17:32
Alice e Bob – Wikipedia
https it.wikipedia.org/wiki/Alice_e_Bob
Reader
anduc Sir Ken Robinson What is Music? Pixar: The ...ose | TED-Ed Peabody Nelson E., F...ed Domains, Death Note – DeathNote.it CheFuturo! L...ne in Italia TEDxRoma | Facebook
Registrati Entra
Voce Discussione Leggi Modifica Modifica wikitesto Cronologia Ricerca
WIKIPEDIA
L'enciclopedia libera
Libera la cultura. Dona il tuo 5×1000 a Wikimedia Italia. Scrivi 94039910156.
[nascondi]
Alice e Bob
Da Wikipedia, l'enciclopedia libera.
I nomi Alice e Bob sono molto usati come personaggi in campi come la crittografia e la fisica. I nomi sono usati per convenienza, poiché espressioni come "La persona A vuole mandare un messaggio alla persona B" può diventare difficile da seguire, specialmente in sistemi complessi che usano molti passaggi.
Lista di personaggi [modifica | modifica wikitesto]
Questa lista è tratta principalmente dal libro Applied Cryptography di Bruce Schneier. I nomi non seguono sempre l'alfabeto.
Alice e Bob. Generalmente Alice vuole mandare un messaggio a Bob. Questi nomi furono usati da Ron Rivest nel 1978 nell'articolo Communications of the Association for Computing Machinery che presentava il crittosistema RSA. (Nel 1977 i rapporti tecnici sull'RSA non usavano questi nomi.) Rivest negò che questi nomi avessero a che fare con il film del 1969 Bob & Carol & Ted & Alice come fu suggerito occasionalmente da altri.
Carol o Charlie, è il terzo partecipante alla comunicazione.
Chuck, un terzo partecipante avente intenzioni fraudolente.
Dave, il quarto partecipante, e così avanti in ordine alfabetico.
Eve, (eavesdropper), è di solito un attaccante passiva. Può ascoltare i messaggi tra Alice e Bob, ma non può modificarli. Nella crittografia quantistica Eve può rappresentare l'ambiente (environment).
Isaac è l'ISP (Internet Service Provider)
Ivan
Justin
Mallory, intruso che attacca la rete in maniera attiva. A differenza di Eve inserisce pacchetti nella rete, ascolta e eventualmente modifica la comunicazione tra Alice e Bob (attacco Man in the middle)
Pagina principale
Ultime modifiche
Una voce a caso
Vetrina
Aiuto
Comunità
Portale Comunità
Bar
Il Wikipediano
Fai una donazione
Contatti
Strumenti
Puntano qui
Modifiche correlate
Carica su Commons
Pagine speciali
Link permanente
Informazioni sulla pagina
Elemento Wikidata
Cita questa voce
Stampa/esporta
Crea un libro
Scarica come PDF
Articolimiei
Teaching

Perché?

- Sicurezza (bancomat, carte di credito,…)
- Autenticazione (firme digitali)
- Privacy (email, chat)
- Pay per view (segnale televisivo criptato)

E’ un nostro diritto

art 15: La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
La loro limitazione può avvenire soltanto per atto motivato dell’autorità giudiziaria con le garanzie stabilite dalla legge.

Parole e numeri

Ad ogni lettera si può associare un numero:

- A=0, B=1, C=2…
- A=11, B=12, … (matrici)
- A=065, B=066, … (codice ASCII= American Standard Code for Information Interchange)
- basi diverse dalla base 10

……

parola = sequenza di numeri

da manipolare!

I Flinstones GeeK...

- Greci e la Scitala

skytale = bastone (400 a.c.)

- Cifrario di Cesare

(chiaro) A B C D E F G H I K L M N O P Q R S T V X

(cifrato) D E F G H I K L M N O P Q R S T V X A B C

BGeek = EKhhn 🔑 +3

Svantaggi

- non è un sistema sicuro: analisi delle frequenze (20 possibilità nell'alfabeto italiano)
- stessa chiave utilizzata per cifrare e decifrare il testo
- come comunicare la chiave?

Sistema Vernam (1917)

- password lunga almeno quanto il messaggio
- password usata una sola volta : OTP = one time pad
- come scambiare la chiave?

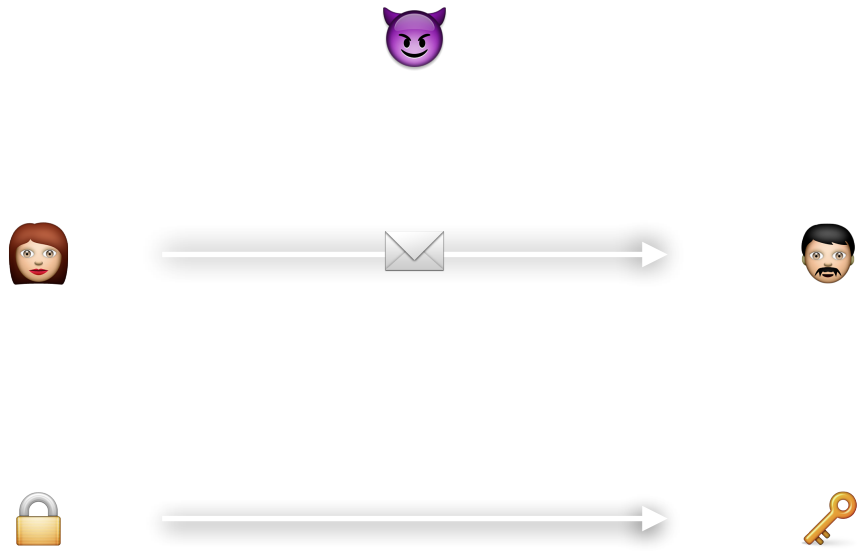
Claude Shannon (1949) ha dimostrato matematicamente che tale sistema è invulnerabile e che tutti i sistemi invulnerabili sono di tipo Vernam.

Su questo sistema si basava la comunicazione sulla linea rossa tra Mosca e Washington durante la guerra fredda.

Chiave privata

Erano tutti esempi di Crittografia Simmetrica:

unica chiave usata per cifrare e decifrare



Chiave privata

Sistemi crittografici simmetrici più recenti sono

- DES = Data Encryption Standard (inizi anni 70), utilizzato su internet e dalla NSA
- AES = Advanced Encryption Standard (2000)
- IDEA = International Data Encryption Algorithm

stesso algoritmo di cifratura e decifratura

f serie di operazioni (matematiche) che si possono anche ripetere in maniera inversa.

Chiave privata nei sistemi moderni

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi : chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

Chiave privata nei sistemi moderni

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi : chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

Arrivano i matematici!!!

Chiave privata nei sistemi moderni

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi : chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

Arrivano i matematici!!!

- fattorizzazione in numeri primi: 2201=31x71
- aritmetica modulare : 2+2=1

Chiave pubblica/privata - sistema RSA

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema **RSA**

Chiave pubblica/privata - sistema RSA

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema RSA

👨 rende visibile la sua chiave pubblica 🔓

👩 invia ✉🔒

👨 apre ✉🔓 utilizzando 🔑 chiave privata

Chiave pubblica/privata - sistema RSA

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema RSA

La conoscenza della chiave pubblica e dell'algoritmo di cifratura, anch'esso pubblico, non bastano per risalire alla chiave privata in tempi brevi.

Chiave pubblica/privata - sistema RSA

😱 da decifrare….

Alice sceglie due numeri primi molto grandi p_A e q_A
ed un terzo numero e_A (chiave pubblica)

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A = 1 \pmod{(p_A-1)(q_A-1)}$ 😱 😱

Bob fa la stessa cosa

Alice trasforma il suo messaggio per Bob in un numero M e lo cripta

$$M^{e_A} = C \pmod{p_B q_B}$$

C è il messaggio cifrato!

Chiave pubblica/privata - sistema RSA

😱 da decifrare….

Bob riceve C e lo decifra con la sua chiave privata d_B

$$C^{d_B} = M^{e_B d_B} = M \pmod{p_B q_B}$$

😱 😱

Livello di sicurezza?

E’ pubblico il numero n ottenuto dal prodotto di p e q e NON i due numeri primi p e q

La fattorizzazione di un numero molto grande richiede tempi di calcolo molto lunghi.

Chiave pubblica/privata - sistema RSA

- La chiave pubblica di un utente può essere diffusa in diversi modi: in coda ad un messaggio, su server accessibili a tutti…

- Firma digitale: Alice cifra un messaggio con la propria chiave privata e lo invia. Bob, ricevuto il messaggio, lo decifra con la chiave pubblica di Alice.

  → sicurezza sull'identità di Alice.

Dalla NSA (National Security Agency) intimarono a Rivest, Shamir ed Adleman di non pubblicare le loro ricerche, loro lo ignorarono e pubblicarono il tutto su un libro del MIT press.

Chiave pubblica/privata - PGP

- Zimmermann (1991): PGP = Pretty God Privacy

primo software crittografico pubblico

- tutti possono creare la propria coppia di chiavi (🔒,🔑), pubblica e privata, e rendere nota la chiave pubblica.
- tutti possono criptare ed autenticare i propri file di testo

  → sicurezza email, instant messaging,…

- “PGP empowers people to take their privacy into their own hands.There has been a growing social need for it. That's why I wrote it.”

Wikileaks

Wikileaks

wikileaks .org, founded in 2006

“to bring important news and information
to the public”

Guantanamo, Swiss Bank Cayman, Iraq, Afghanistan

Insurance.aes.256 = Assicurazione di Wikileaks

Messaggistica e crittografia end to end

end to end = da nodo a nodo

- sistema a chiave pubblica/privata
- un software installato sui dispositivi (smartphone, pc,…) di Alice e Bob genera le chiavi
- la chiave privata resta sui singoli dispositivi ed è usata per decifrare
- la chiave pubblica sarà condivisa ed è utilizzata per criptare

il servizio di messaggistica si occupa solo della “spedizione” e non sa leggere i messaggi

Messaggistica e crittografia end to end

end to end = da nodo a nodo

Telegram

iMessage

FaceTime

Whatsapp

encryption e decryption **locali**

Telegram

https://telegram.org/blog/cryptocontest

IMCR;fK4aLPx3xAGnfiiZ;UsHk2Ij534HaMrWvx2moPg==;
MxQS6HHezo0p4lRX39yQ/CMiPfAkn2y33tVX7BfOi8HuNB7c/zFkvs6Gy7eNnNCw

IMCR;fK4aLPx3xAGnfiiZ;UsHk2Ij534HaMrWvx2moPg==;
MxQS6HHezo0p4lRX39yQ/CMiPfAkn2y33tVX7BfOi8HuNB7c/zFkvs6Gy7eNnNCw

(by immediate crypt)

Grazie e Buon BGeek!