Come Spedire un Diamante in Segreto

Messaggi Privati con Io SmartPhone

Giuseppe Persiano

Università di Salerno

25 Febbraio 2019

Privacy delle comunicazioni

Booking e Repubblica

- prenoto l'albergo per Torino usando Booking
- da quel momento in poi Repubblica mi mostra pubblicità di eventi in Piemonte

Privacy delle comunicazioni

Booking e Repubblica

- prenoto l'albergo per Torino usando Booking
- da quel momento in poi Repubblica mi mostra pubblicità di eventi in Piemonte

Privacy delle comunicazioni

Facebook e Chrome

- visito un sito di orologi
- Facebook inizia a presentarmi pubblicità di orologi

Privacy delle comunicazioni

Facebook e Chrome

- visito un sito di orologi
- Facebook inizia a presentarmi pubblicità di orologi

Gmail

- scambio email per accordarmi ad una visita di lavoro a NYU
- pubblicità per alberghi a New York

Privacy delle comunicazioni

Facebook e Chrome

- visito un sito di orologi
- Facebook inizia a presentarmi pubblicità di orologi

Gmail

- scambio email per accordarmi ad una visita di lavoro a NYU
- pubblicità per alberghi a New York

Whatsapp???

Whatsapp usa end-to-end encryption

Anna vuole inviare un messaggio a Bernardo

- Il messaggio è cifrato dallo smart phone di Anna
- Attraversa Internet fino a Bernardo in forma cifrato
- Lo smart phone di Bernardo lo decifra

Whatsapp usa end-to-end encryption

Anna vuole inviare un messaggio a Bernardo

- Il messaggio è cifrato dallo smart phone di Anna
- Attraversa Internet fino a Bernardo in forma cifrato
- Lo smart phone di Bernardo lo decifra

Come è possibile?

Schemi di Cifratura

Una coppia di algoritmi (E, D)

$$E(K, M) = C \qquad D(K, C) = M$$

$$K \in \{0,1\}^k \quad M \in \{0,1\}^m \quad C \in \{0,1\}^c$$

chiave *messaggio* *crittogramma*

Schemi di Cifratura

Una coppia di algoritmi (E, D)

$$E(K, M) = C \qquad D(K, C) = M$$

$$K \in \{0,1\}^k \quad M \in \{0,1\}^m \quad C \in \{0,1\}^c$$

chiave *messaggio* *crittogramma*

1. A(nna) sceglie $K \in \{0,1\}^k$
2. Cifra il file usando la chiave K
3. Conserva il file e la chiave in luoghi separati

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)
- Ratificato dal *National Institute of Standards and Technology*, USA

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)
- Ratificato dal *National Institute of Standards and Technology*, USA
- Chiave di 128, 192, 256 bit

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)
- Ratificato dal *National Institute of Standards and Technology*, USA
- Chiave di 128, 192, 256 bit
- Cifra blocchi di dati di 128 bit

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)
- Ratificato dal *National Institute of Standards and Technology*, USA
- Chiave di 128, 192, 256 bit
- Cifra blocchi di dati di 128 bit
- Considerato sicuro dalla comunità scientifica

Advanced Encryption Standard

- Algoritmo pubblico e utilizzabile gratuitamente
- Scelto dopo una competizione scientifica durata dal 1997-2000
  - Annuncio del Gennaio 1997
  - Richiesta ufficiale del Settembre 1997 per proposte di algoritmi di cifratura
  - 15 proposte iniziali da gruppi di ricercatori da tutto il mondo
  - 5 finalisti annunciati, Agosto 1999
  - Rijndael scelto ad Ottobre 2000 come Advanced Encryption Standard (AES)
- Ratificato dal *National Institute of Standards and Technology*, USA
- Chiave di 128, 192, 256 bit
- Cifra blocchi di dati di 128 bit
- Considerato sicuro dalla comunità scientifica
- Implementazioni disponibili: openssl.org

Inviare messaggi privati

Anna vuole mandare un messaggio privato a Bernardo

Inviare messaggi privati

Anna vuole mandare un messaggio privato a Bernardo

- Anna cifra
- Bernardo decifra

Inviare messaggi privati

Anna vuole mandare un messaggio privato a Bernardo

- Anna cifra
- Bernardo decifra

Ma con quale chiave?

La chiave usata per decifrare deve essere la stessa usata per cifrare.

Inviare messaggi privati

Anna vuole mandare un messaggio privato a Bernardo

- Anna cifra
- Bernardo decifra

Ma con quale chiave?

La chiave usata per decifrare deve essere la stessa usata per cifrare.

Anna e Bernardo si incontrano e si scambiano una chiavetta USB con la chiave

Ideale per applicazioni militari

Inviare messaggi privati nell'era di WhatsApp

ma anche Messenger, Telegram, Signal, Hangout,...

Inviare messaggi privati nell'era di WhatsApp

ma anche Messenger, Telegram, Signal, Hangout,...

Key Agreement

- Come fanno due persone che non si sono mai incontrate a scambiarsi una chiave?

Inviare messaggi privati nell'era di WhatsApp

ma anche Messenger, Telegram, Signal, Hangout,...

Key Agreement

- Come fanno due persone che non si sono mai incontrate a scambiarsi una chiave?
- In modo privato, senza che nessuno la legga.

Inviare messaggi privati nell'era di WhatsApp

ma anche Messenger, Telegram, Signal, Hangout,...

Key Agreement

- Come fanno due persone che non si sono mai incontrate a scambiarsi una chiave?
- In modo privato, senza che nessuno la legga.
- Un cane che si morde la coda:
  - se Anna e Bernardo possono scambiarsi una chiave in modo privato, perché non si scambiano direttamente il messaggio che voglio inviarsi?

Inviare messaggi privati nell'era di WhatsApp

ma anche Messenger, Telegram, Signal, Hangout,...

Key Agreement

- Come fanno due persone che non si sono mai incontrate a scambiarsi una chiave?
- In modo privato, senza che nessuno la legga.
- Un cane che si morde la coda:
  - se Anna e Bernardo possono scambiarsi una chiave in modo privato, perché non si scambiano direttamente il messaggio che voglio inviarsi?
- Ma è **possibile**?

Un problema simile

Come spedire un diamante

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?
  - Può metterlo in una cassaforte e chiuderla con un lucchetto.

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?
  - Può metterlo in una cassaforte e chiuderla con un lucchetto.
  - Ed inviare la cassaforte e la chiave una con DHL e l'altra con FedExp.

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?
  - Può metterlo in una cassaforte e chiuderla con un lucchetto.
  - Ed inviare la cassaforte e la chiave una con DHL e l'altra con FedExp.
  - Funziona se i due corrieri non si mettono d'accordo...

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?
  - Può metterlo in una cassaforte e chiuderla con un lucchetto.
  - Ed inviare la cassaforte e la chiave una con DHL e l'altra con FedExp.
  - Funziona se i due corrieri non si mettono d'accordo...
  - O se nessuno intercetta i pacchi...

Un problema simile

Come spedire un diamante

- Bernardo è in viaggio e compra un diamante per Anna.
- Come può spedirglielo in maniera sicura?
  - Può metterlo in una cassaforte e chiuderla con un lucchetto.
  - Ed inviare la cassaforte e la chiave una con DHL e l'altra con FedExp.
  - Funziona se i due corrieri non si mettono d'accordo...
  - O se nessuno intercetta i pacchi...
- Possibile una soluzione che garantisce che nessuno può rubare il diamante?

Un problema simile

Una soluzione

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e mette un lucchetto nell'occhiello libero. Tiene per sé la chiave del lucchetto.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e mette un lucchetto nell'occhiello libero. Tiene per sé la chiave del lucchetto.
- Anna invia la cassaforte a Bernardo.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e mette un lucchetto nell'occhiello libero. Tiene per sé la chiave del lucchetto.
- Anna invia la cassaforte a Bernardo.
- Bernardo rimuove il suo lucchetto.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e mette un lucchetto nell'occhiello libero. Tiene per sé la chiave del lucchetto.
- Anna invia la cassaforte a Bernardo.
- Bernardo rimuove il suo lucchetto.
- Bernardo invia la cassaforte ad Anna.

Un problema simile

Una soluzione

- Bernardo compra una cassaforte con **due** occhielli per lucchetto.
- Bernardo mette il diamante nella cassaforte e un lucchetto in uno dei due occhielli. Tiene per sé la chiave del lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e mette un lucchetto nell'occhiello libero. Tiene per sé la chiave del lucchetto.
- Anna invia la cassaforte a Bernardo.
- Bernardo rimuove il suo lucchetto.
- Bernardo invia la cassaforte ad Anna.
- Anna riceve la cassaforte e usa la sua chiave per aprirla.

Cosa succede???

La potenza della commutatività

- una cassaforta chiusa non può essere aperta senza la chiave
- i lucchetti commutano:
  - la cassaforte si apre anche se i lucchetti non sono rimossi nello stesso ordine

Cosa succede???

La potenza della commutatività

- una cassaforta chiusa non può essere aperta senza la chiave
- i lucchetti commutano:
  - la cassaforte si apre anche se i lucchetti non sono rimossi nello stesso ordine

La moltiplicazione è commutativa!

$$x \cdot y = y \cdot x$$

Cosa succede???

La potenza della commutatività

- una cassaforta chiusa non può essere aperta senza la chiave
- i lucchetti commutano:
  - la cassaforte si apre anche se i lucchetti non sono rimossi nello stesso ordine

La moltiplicazione è commutativa!

$$x \cdot y = y \cdot x$$

Cercasi cassaforte digitale che interagisca con moltiplicazione.

Esponenziazione

$$(2^x)^y = 2^{x \cdot y} = (2^y)^x$$

Esponenziazione

$$(2^x)^y = 2^{x \cdot y} = (2^y)^x$$

È una cassaforte sicura?

Esponenziazione

$$(2^x)^y = 2^{x \cdot y} = (2^y)^x$$

È una cassaforte sicura?

Non sugli interi...

Diffie-Hellman

Sia p un primo.

Diffie-Hellman

Sia p un primo.

$\mathbb{Z}_p^\star$ è il gruppo degli interi $[1, \ldots, p-1]$ con moltiplicazione modulo p.

Diffie-Hellman

Sia p un primo.

$\mathbb{Z}_p^\star$ è il gruppo degli interi $[1, \ldots, p-1]$ con moltiplicazione modulo p.

$\mathbb{Z}_p^\star$ è un gruppo ciclico

Diffie-Hellman

Sia p un primo.

$\mathbb{Z}_p^\star$ è il gruppo degli interi $[1, \ldots, p-1]$ con moltiplicazione modulo p.

$\mathbb{Z}_p^\star$ è un gruppo ciclico $\Rightarrow$ Esiste un generatore g t.c.:

$$\mathbb{Z}_p^\star = \{g^0, g^1, \ldots, g^{p-2}\}.$$

Diffie-Hellman

Sia p un primo.

$\mathbb{Z}_p^\star$ è il gruppo degli interi $[1, \ldots, p-1]$ con moltiplicazione modulo p.

$\mathbb{Z}_p^\star$ è un gruppo ciclico $\Rightarrow$ Esiste un generatore g t.c.:

$$\mathbb{Z}_p^\star = \{g^0, g^1, \ldots, g^{p-2}\}.$$

Ogni $a \in \mathbb{Z}_p^\star$ ha il *logaritmo discreto in base g*.

$$x \text{ t.c. } a = g^x.$$

Esempio con $p = 47$

Esempio in Sage

```
K=GF(47)
g=K(5)
a=K.random_element()
A=g^a

b=K.random_element()
B=g^b

print "Chiave calcolata da
Anna",B^a
print "Chiave calcolata da
Bernardo",A^b
```

Esecuzione

```
Diffie Hellman con p =
47 e g = 5

a = 31 A = 39

b = 12 B = 18

Chiave calcolata da Anna
14

Chiave calcolata da
Bernardo 14
```

Scegliamo un primo più grande

Il documento *Algorithms, Key Size and Protocols Report (2018)*, raccomanda p di almeno 1024 bit. Per applicazioni con alto livello di sicurezza almeno 3072 bit.

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74
020BBEA6 3B139B22 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437
4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05
98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB
9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B
E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718
3995497C EA956AE5 15D22618 98FA0510 15728E5A 8AAAC42D AD33170D 04507A33
A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D B3970F85 A6E1E4C7
ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864
D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2
08E24FA0 74E5AB31 43DB5BFC E0FD108E 4B82D120 A93AD2CA FFFFFFFF FFFFFFFF
```

https://www.ietf.org/rfc/rfc3526.txt

Difficoltà del Logaritmo Discreto

Il tempo per calcolare il logaritmo discreto dipende dalla lunghezza del modulo p.

- logaritmo discreto a 1024 bit richiede la potenza di calcolo di uno stato
- logaritmo discreto a 3072 bit resta difficile da calcolare per i prossimi 30 anni

Whatsapp usa end-to-end encryption

Anna vuole inviare un messaggio a Bernardo

- Il messaggio è cifrato dallo smart phone di Anna
- Anna e Bernardo eseguono DH
  - Condividono lo stesso intero P
- Calcolano un hash di 256 bit di P ed ottengono una chiave K per AES a 256 bit
- Anna cifra il messaggio
- Attraversa Internet fino a Bernardo in forma cifrato
- Lo smart phone di Bernardo lo decifra
- Usando AES a 256 e chiave K

Whatsapp usa end-to-end encryption

Anna vuole inviare un messaggio a Bernardo

- Il messaggio è cifrato dallo smart phone di Anna
- Anna e Bernardo eseguono DH
  - Condividono lo stesso intero P
- Calcolano un hash di 256 bit di P ed ottengono una chiave K per AES a 256 bit
- Anna cifra il messaggio
- Attraversa Internet fino a Bernardo in forma cifrato
- Lo smart phone di Bernardo lo decifra
- Usando AES a 256 e chiave K

Versione semplificata!

Morale della favola

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.
- Esistono metodi *scientificamente* provati per proteggerli.

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.
- Esistono metodi *scientificamente* provati per proteggerli.
- Esistono applicazioni che usano metodi *scientificamente* provati per proteggerli.

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.
- Esistono metodi *scientificamente* provati per proteggerli.
- Esistono applicazioni che usano metodi *scientificamente* provati per proteggerli.
- Alcune sono open-source
  - OpenSSL, Signal,...

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.
- Esistono metodi *scientificamente* provati per proteggerli.
- Esistono applicazioni che usano metodi *scientificamente* provati per proteggerli.
- Alcune sono open-source
  - OpenSSL, Signal,...
- Basati su matematica avanzata con cui possiamo sperimentare usando Sage.

Morale della favola

- La riservatezza delle comunicazioni personali è importante ed è sotto attacco.
- Esistono metodi *scientificamente* provati per proteggerli.
- Esistono applicazioni che usano metodi *scientificamente* provati per proteggerli.
- Alcune sono open-source
  - OpenSSL, Signal,...
- Basati su matematica avanzata con cui possiamo sperimentare usando Sage.
  - Sage è open source e gratuito.