Crittografia

Contenuti

- Crittografia
- Firma Digitale
- Steganografia

Crittologia

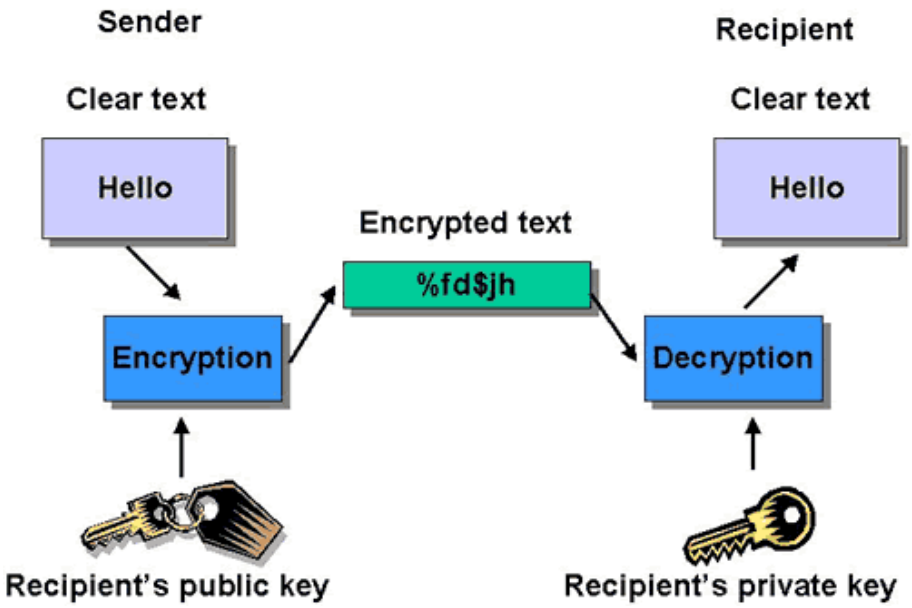
Si suddivide in…

- **Crittografia**: studio di tecniche per codificare i messaggi in maniera che solo il destinatario sia in grado di decifrarli
- **Crittoanalisi** : si occupa della «rottura» dei codici per decodificare i messaggi

Crittografia

- **Crittazione**: operazione di «cifratura» del messaggio
- **Decrittazione**: operazioni di «decifrazione» del messaggio

Entrambe le operazioni si effettuano attraverso appositi algoritmi e richiedono come input delle **stringhe di bit** dette **«chiavi»**



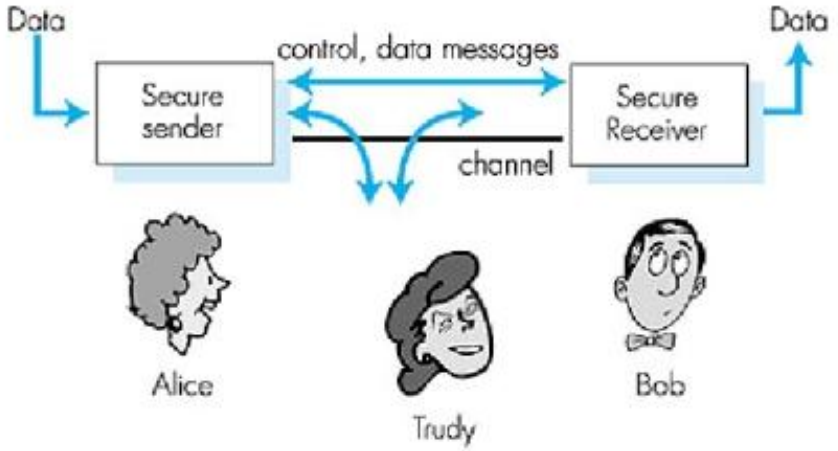
Crittografia

Utilizzata per garantire…

- Riservatezza
- Integrità
- Autenticazione

Crittografia

Friends and enemies: Alice, Bob, Trudy



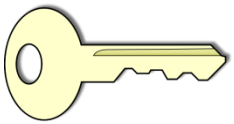
- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy, the "intruder" may intercept, delete, add messages

Crittografia: storia

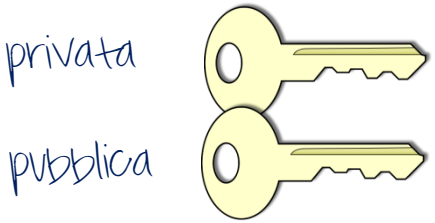
5 Video

Crittografia

- **Simmetrica**: chiave decrittazione = chiave crittazione
- **Asimmetrica**: chiavi diverse, non è essere possibile risalire ad una conoscendo l'altra.



Simmetrica



Asimmetrica

Crittografia Asimmetrica

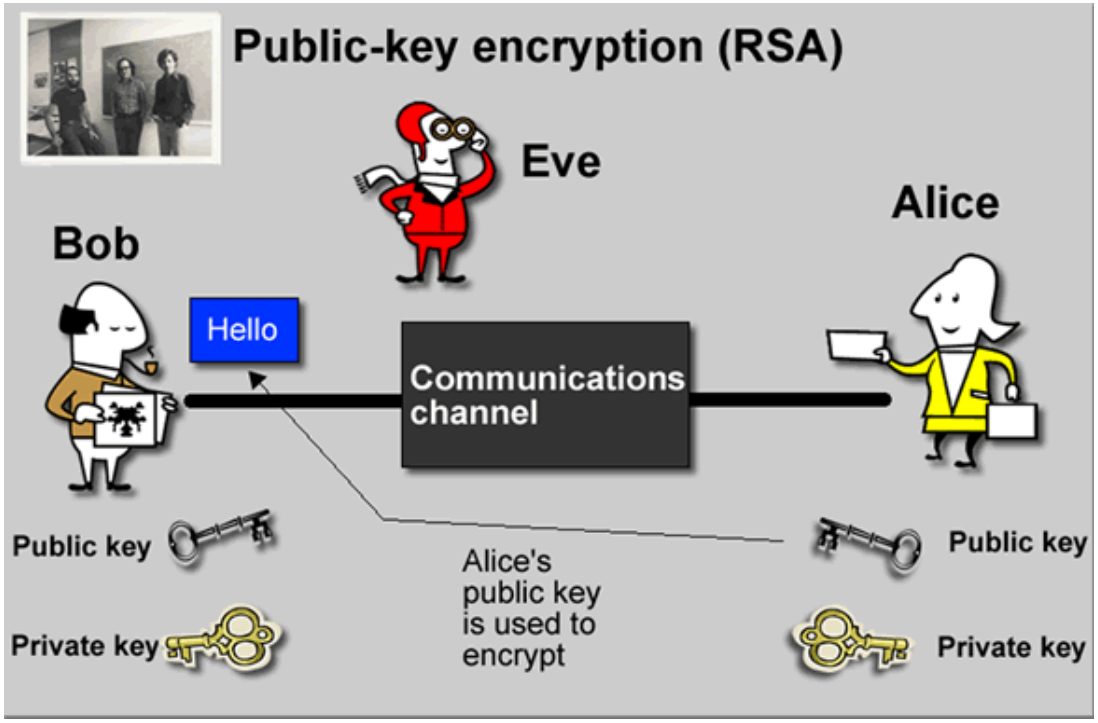
Ogni utente possiede una **coppia univoca** di chiavi complementari:

- una è **pubblica**, nel senso che può essere conosciuta da tutti, ed è usata per cifrare il messaggio.
- una è **privata** ed è tenuta al sicuro dal suo proprietario di modo che solo lui possa utilizzarla.
- Le due chiavi sono create in maniera tale che un messaggio cifrato da una delle due può essere decifrato solo e soltanto dall'altra.

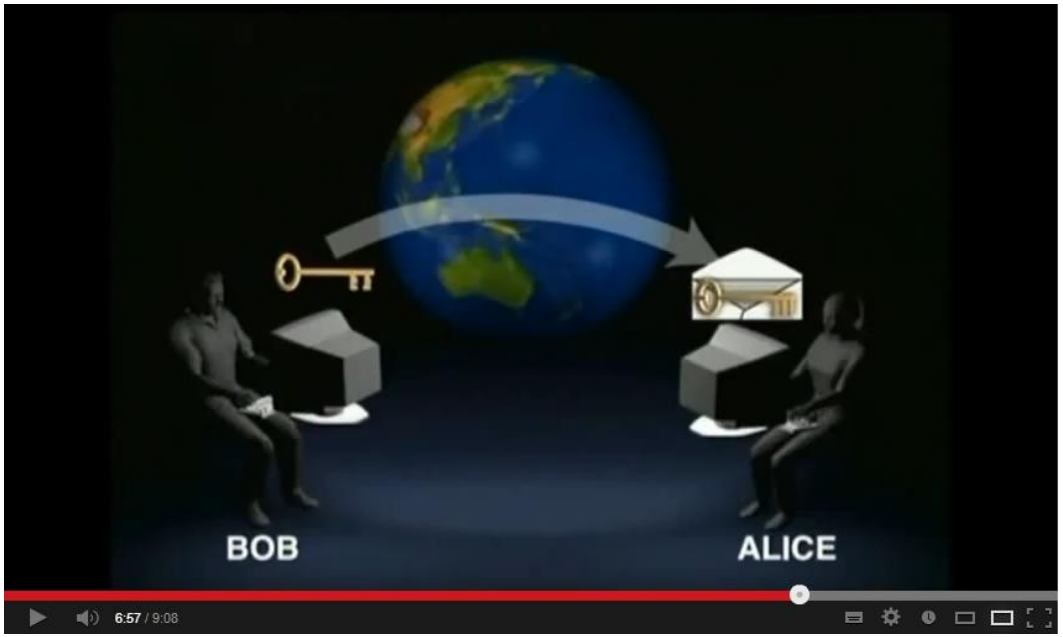
- Questo algoritmo è noto anche come crittografia **a chiave pubblica**

Crittografia a chiave pubblica

Si critta il messaggio con la chiave pubblica del destinatario, soltanto lui potrà decifrarlo con la propria chiave privata.



Crittografia a chiave pubblica



Crittografia

Simmetrica :

- Meno sicura (problema della comunicazione della chiave) ma più veloce
- Utilizzata per cifrare grandi quantità di dati
- DES, AES

Asimmetrica :

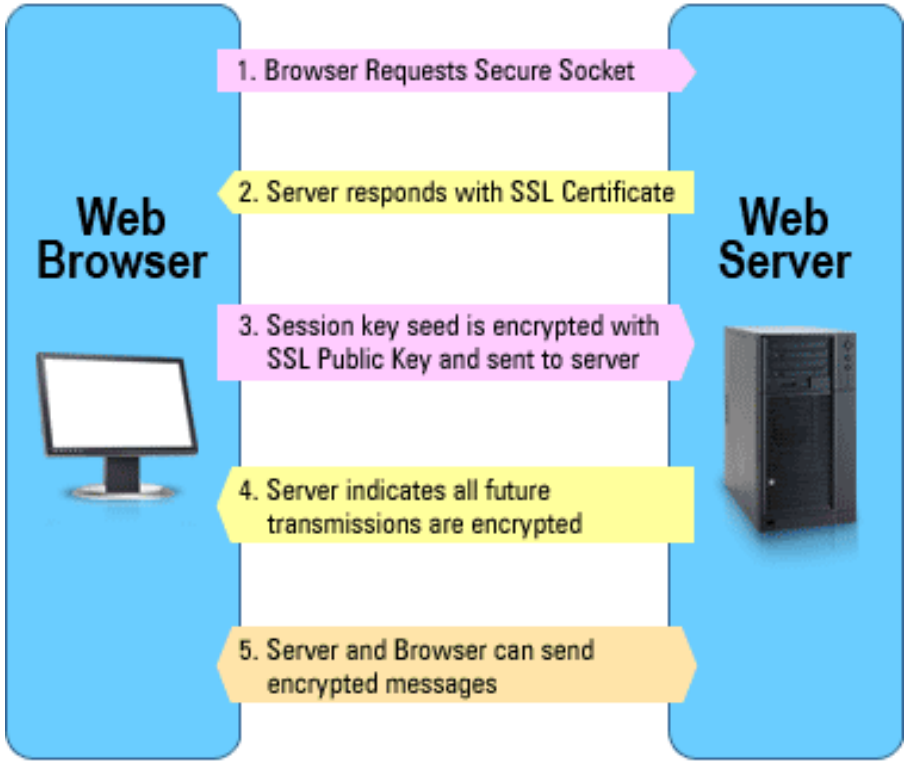
- Più sicura ma più lenta
- RSA (fattorizzazione di numeri primi grandi)
- Diffie-Hellman,…

Ibrida:

- la chiave «simmetrica» viene scambiata con un algoritmo a chiave «pubblica»
- il contenuto viene crittografato con la chiave «simmetrica»
- approccio utilizzato per criptare le comunicazioni sul web

Protocollo SSL

Il protocollo SSL (Secure Socket Layer) utilizza proprio questo schema ibrido…



Certificati digitali

Servono a garantire l'identità del server (autenticazione) e a criptare la comunicazione (riservatezza)

Per approndire…

Firma Digitale

- È l'equivalente informatico di una tradizionale firma apposta su carta
- applicazione del metodo di crittografia a chiave pubblica
- Garantisce autenticazione mittente e integrità del messaggio

Firma Digitale: come funziona?

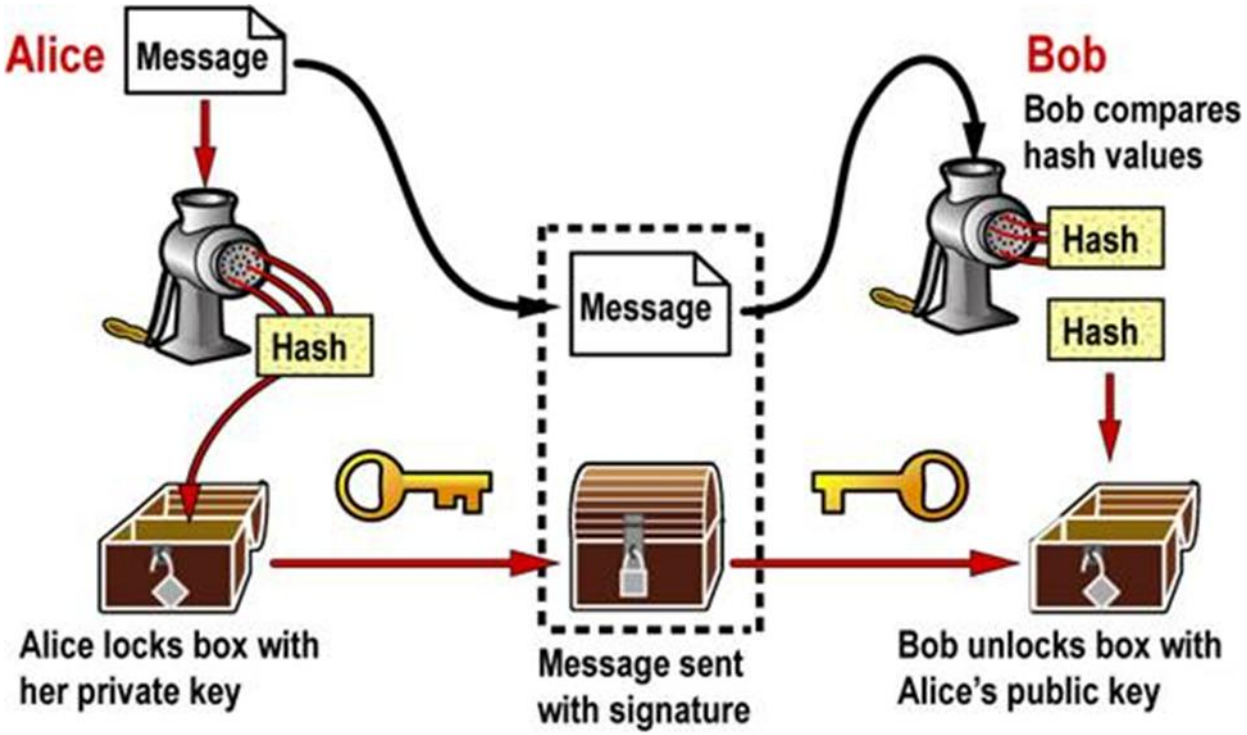
Mittente

- Calcolo valore hash (digest)
- Crittazione del digest con la chiave privata del mittente
- Al file(messaggio) viene aggiunta un'intestazione che specifica l'algoritmo applicato per il calcolo del valore hash (es. MD5) e il digest
- Digest e messaggio (che può essere a sua volta criptato o meno) vengono inviati al destinatario che…

Destinatario

- Decritta il digest (ed eventualmente il contenuto del messaggio) utilizzando la chiave pubblica del mittente, ricalcola l'hash e lo confronta con quello ricevuto
- Se il confronto è positivo ciò significa che nessuno ha alterato il messaggio durante la trasmissione, la crittografia a chiave pubblica garantisce l'identità del mittente

Firma Digitale



Steganografia

- Il messaggio da trasmettere (opportunamente crittografato) viene occultato all'interno di un altro messaggio dall'aspetto innocuo es. immagine, file audio, pagina web…
- In questo modo si nasconde l'esistenza stessa della comunicazione oltre al contenuto

Per approndire…