

Informatica per le discipline umanistiche

Lezione 15 – Crittografia Asimmetrica

`cristiano.longo@unict.it`

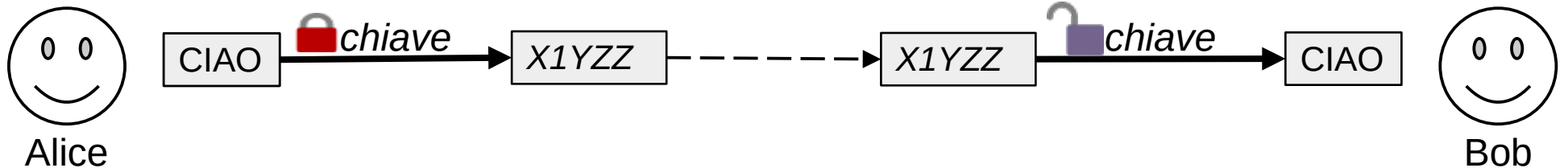


Crittografia simmetrica

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**, tra le parti che devono scambiarsi messaggi confidenziali.

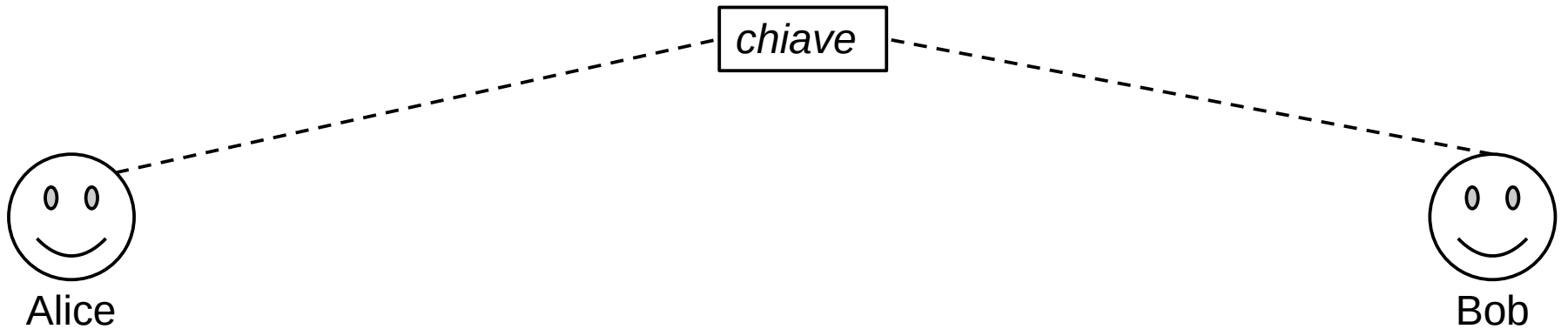
L'operazione di **cifratura** genera un *crittotesto* (incomprensibile a chi non conosce la chiave) a partire da un testo originario (detto *in chiaro*) e la chiave.

La **decifrazione** applica la chiave al crittotesto per restituire il messaggio in chiaro.



Scambiarsi le chiavi

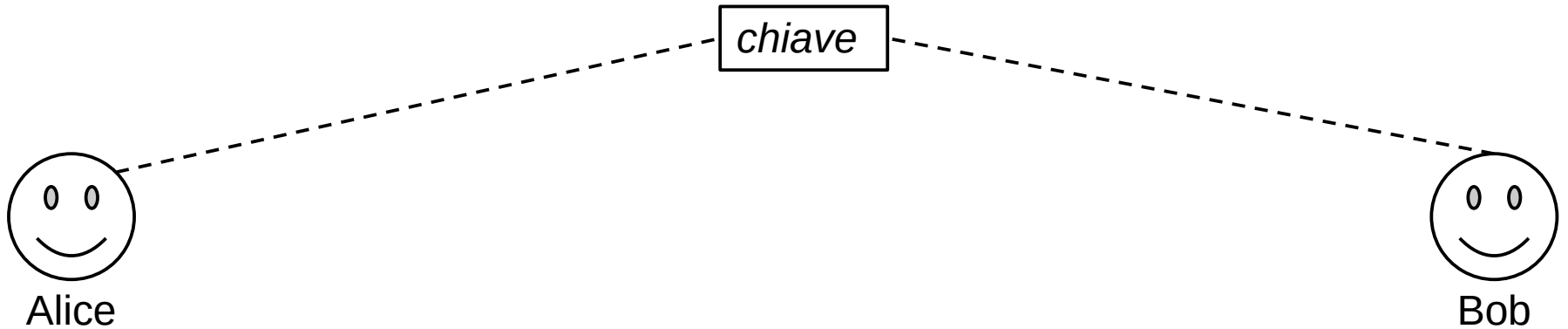
Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.



Scambiarsi le chiavi

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.

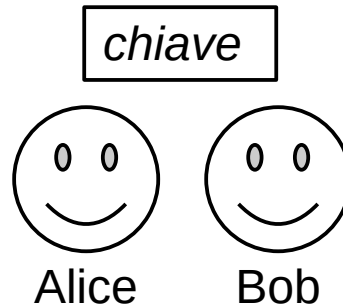
È necessario che la condivisione avvenga in maniera sicura



Crittografia asimmetrica

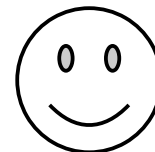
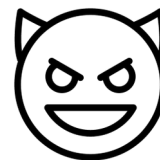
Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.

È necessario che la condivisione avvenga in maniera sicura, solitamente di persona.

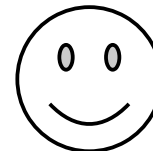


Crittografia asimmetrica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti



Alice



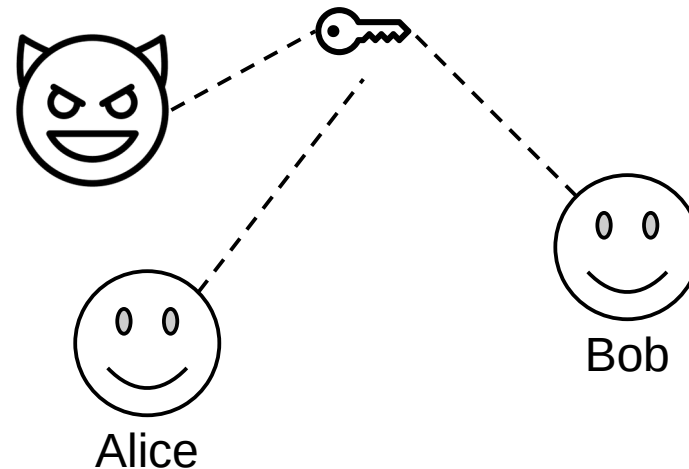
Bob

Crittografia asimmetrica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti



chiave **pubblica** da distribuire a tutti, e



Copyright © (c) 2019-2023 The Bootstrap authors

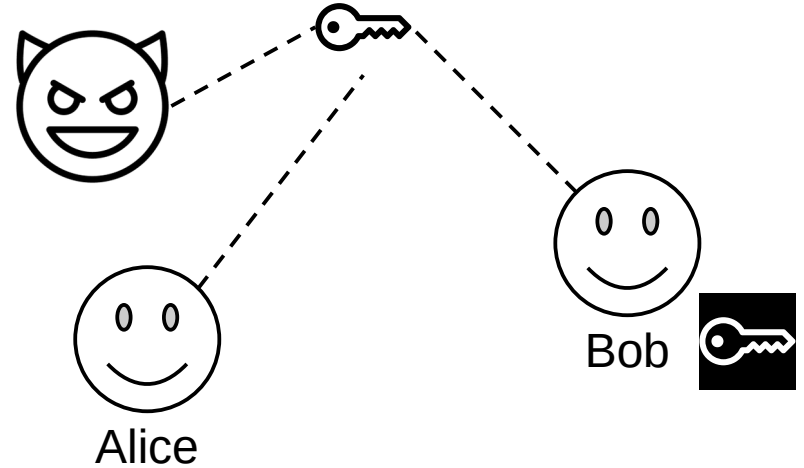
Crittografia asimmetrica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti



chiave **pubblica** da distribuire a tutti, e

chiave **privata**, che il possessore deve mantenere segreta.



Copyright © (c) 2019-2023 The Bootstrap authors

Crittografia asimmetrica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti



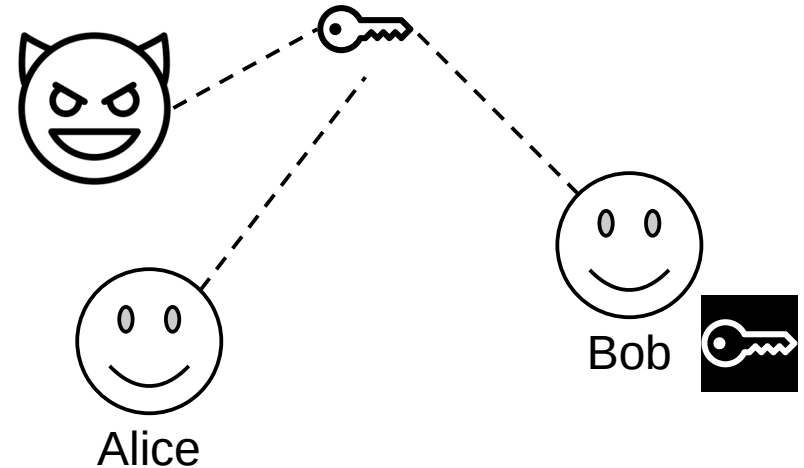
chiave **pubblica** da distribuire a tutti, e



chiave **privata**, che il possessore deve mantenere segreta.

Un messaggio cifrato con la chiave pubblica deve essere decifrato con la chiave privata.

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.



Copyright © (c) 2019-2023 The Bootstrap authors

Chiave pubblica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti

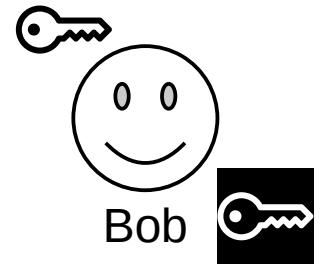
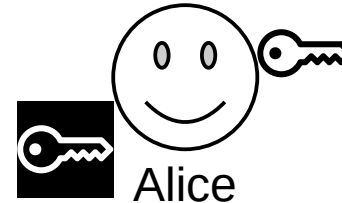
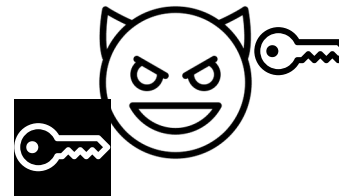


chiave **pubblica** da distribuire a tutti, e



chiave **privata**, che il possessore deve mantenere segreta.

Ad ogni utente è associata una coppia di chiavi.



Copyright © (c) 2019-2023 The Bootstrap authors

Chiave pubblica

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti



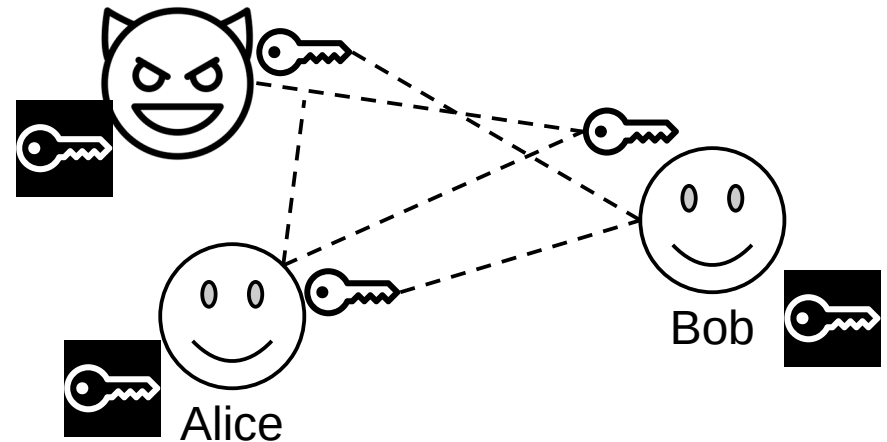
chiave **pubblica** da distribuire a tutti, e



chiave **privata**, che il possessore deve mantenere segreta.

Ad ogni utente è associata una coppia di chiavi.

Le chiavi pubbliche sono note a tutti, quelle private solo al possessore.

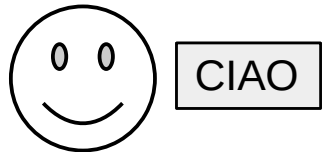


Copyright © (c) 2019-2023 The Bootstrap authors

Crittografia asimmetrica - confidenzialità

Un messaggio cifrato con la chiave pubblica può essere decifrato solo con la chiave privata.

1) Alice vuole mandare un messaggio confidenziale a Bob.



Alice

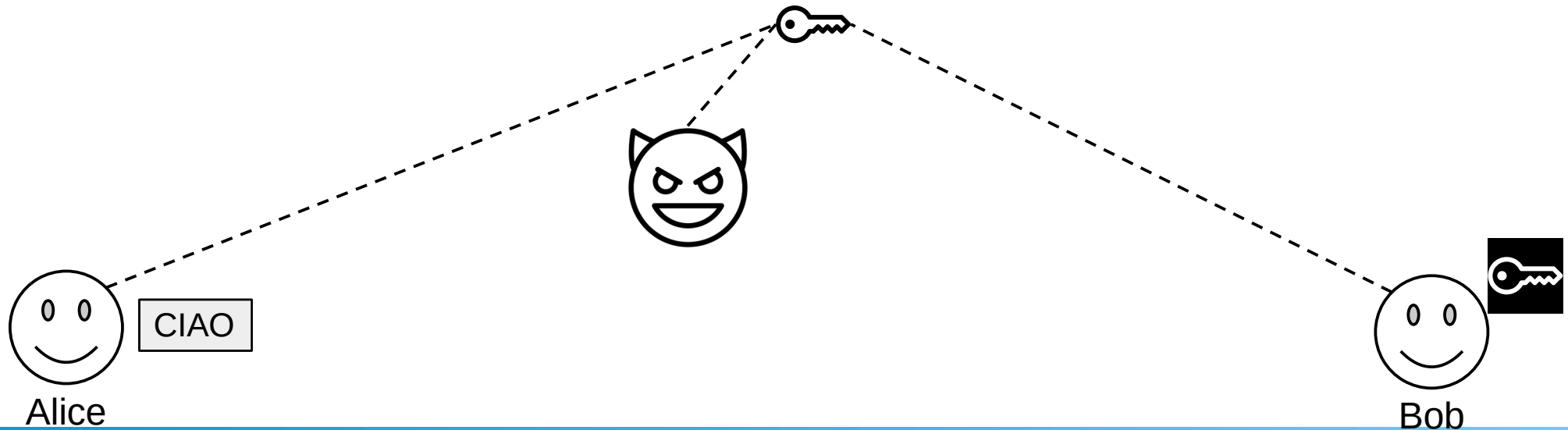


Bob

Crittografia asimmetrica - confidenzialità

Un messaggio cifrato con la chiave pubblica può essere decifrato solo con la chiave privata.

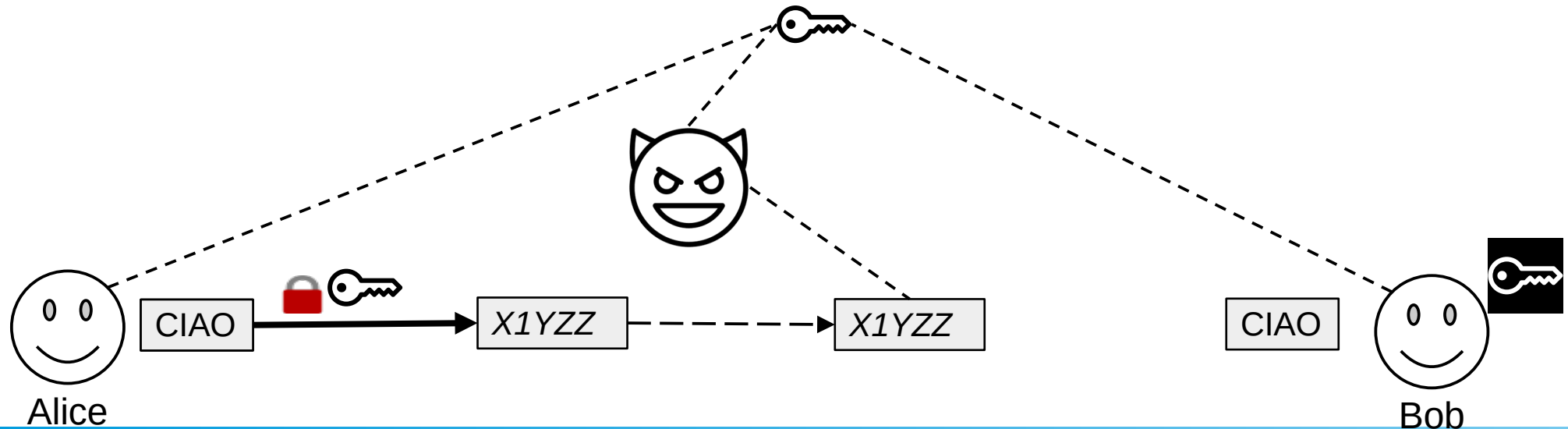
- 1) Alice vuole mandare un messaggio confidenziale a Bob.
- 2) Tutti gli utenti conoscono la chiave pubblica di Bob, compresa Alice.



Crittografia asimmetrica - confidenzialità

Un messaggio cifrato con la chiave pubblica può essere decifrato solo con la chiave privata.

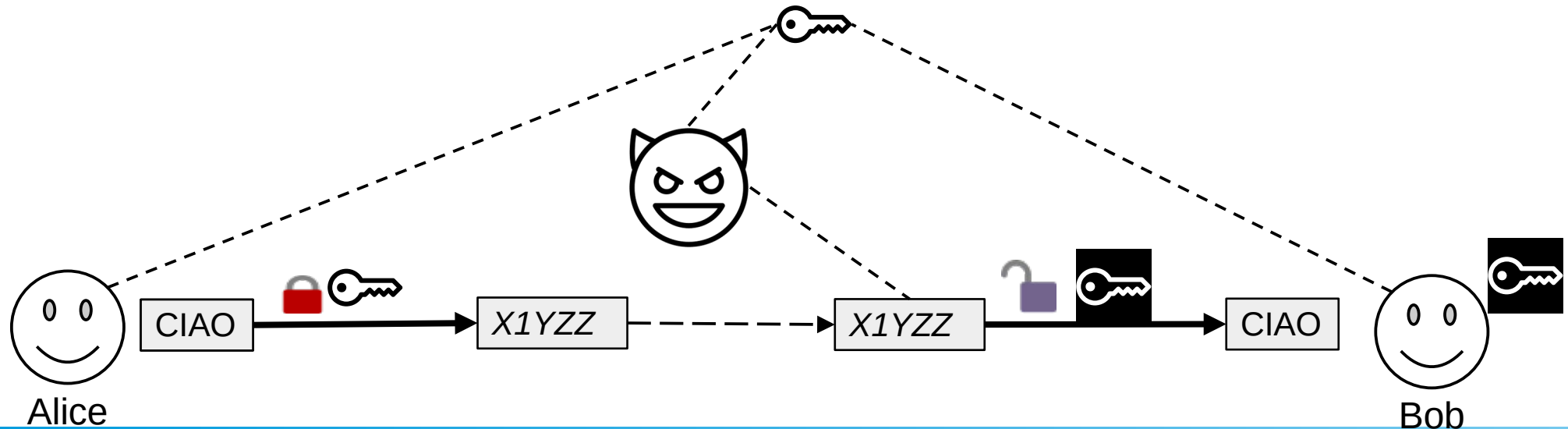
- 1) Alice vuole mandare un messaggio confidenziale a Bob.
- 2) Tutti gli utenti conoscono la chiave pubblica di Bob, compresa Alice.
- 3) Alice cifra il messaggio per Bob utilizzando questa chiave, e lo invia a Bob.



Crittografia asimmetrica - confidenzialità

Un messaggio cifrato con la chiave pubblica può essere decifrato solo con la chiave privata.

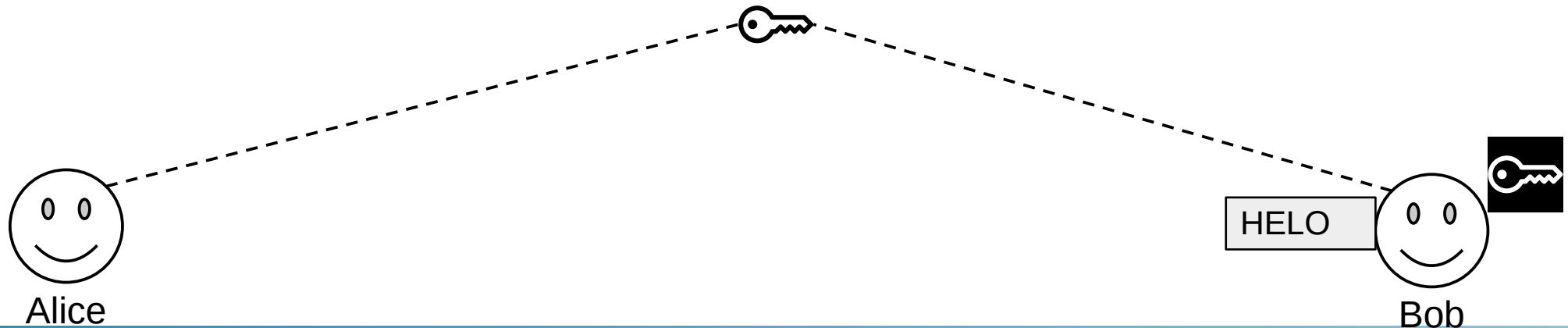
- 1) Alice vuole mandare un messaggio confidenziale a Bob.
- 2) Tutti gli utenti conoscono la chiave pubblica di Bob, compresa Alice.
- 3) Alice cifra il messaggio per Bob utilizzando questa chiave.
- 4) Solo Bob conosce la propria chiave privata, e quindi può decifrare il messaggio



Crittografia asimmetrica - autenticità

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.

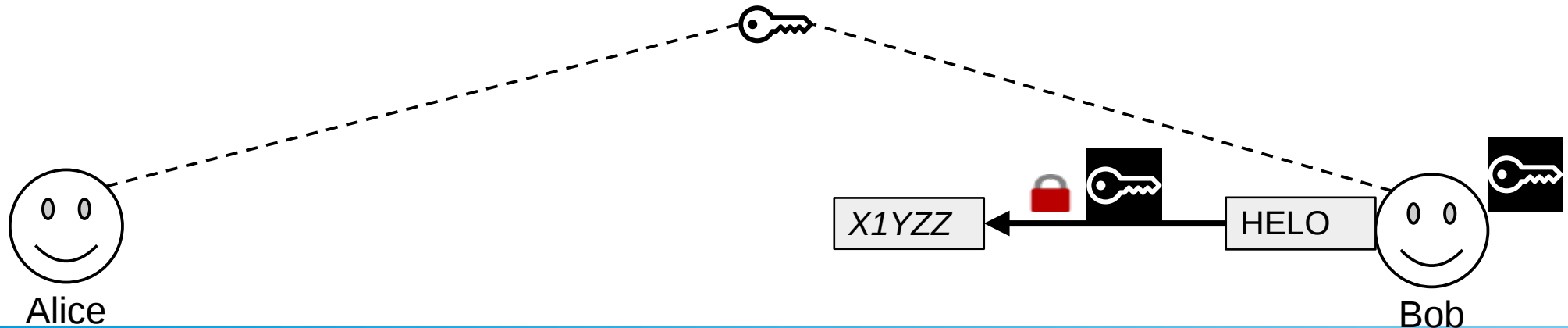
1) Bob vuole mandare un messaggio ad Alice, ma tale che Alice possa verificare il mittente.



Crittografia asimmetrica - autenticità

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.

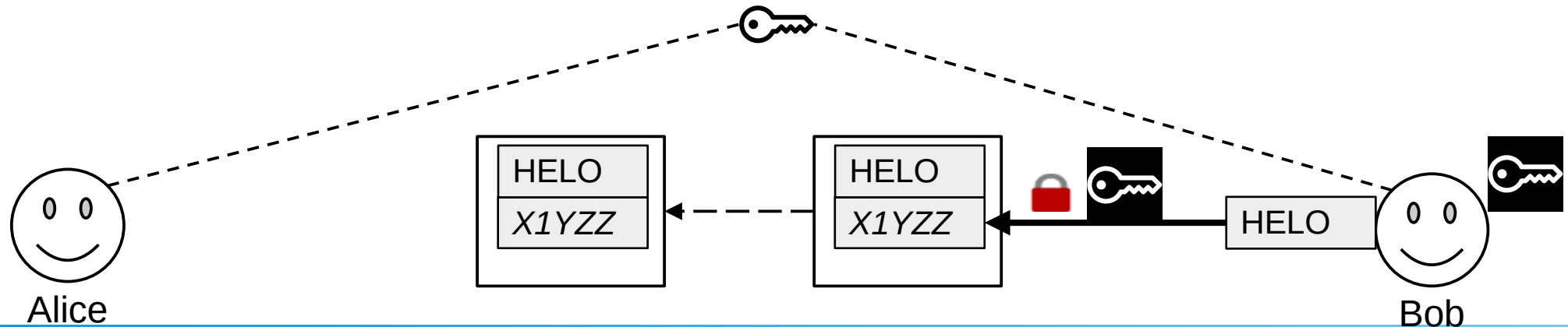
- 1) Bob vuole mandare un messaggio ad Alice, ma tale che Alice possa verificare il mittente.
- 2) Bob cifra il messaggio usando la propria chiave privata (Bob **firma** il messaggio).



Crittografia asimmetrica - autenticità

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.

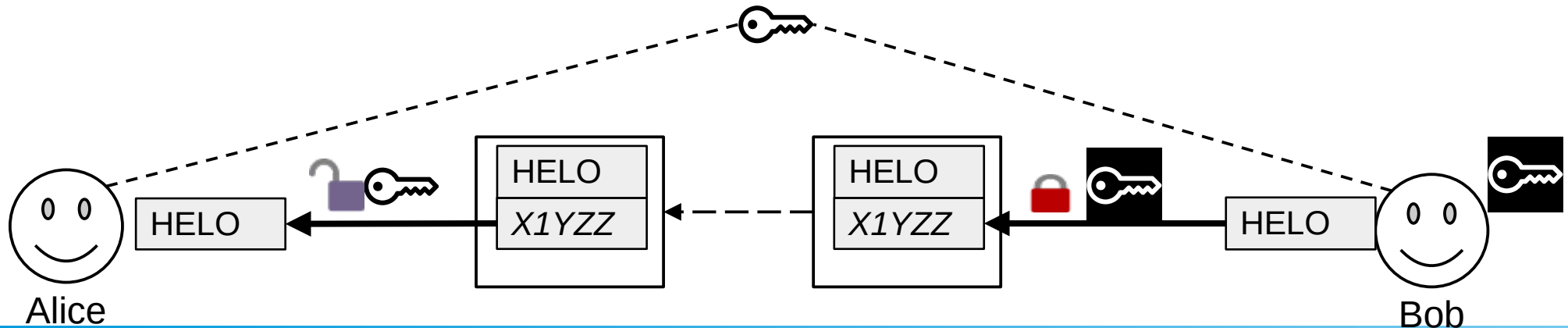
- 1) Bob vuole mandare un messaggio ad Alice, ma tale che Alice possa verificare il mittente.
- 2) Bob cifra il messaggio usando la propria chiave privata (Bob **firma** il messaggio).
- 3) Invia poi ad Alice sia il messaggio cifrato che il testo in chiaro.



Crittografia asimmetrica - autenticità

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.

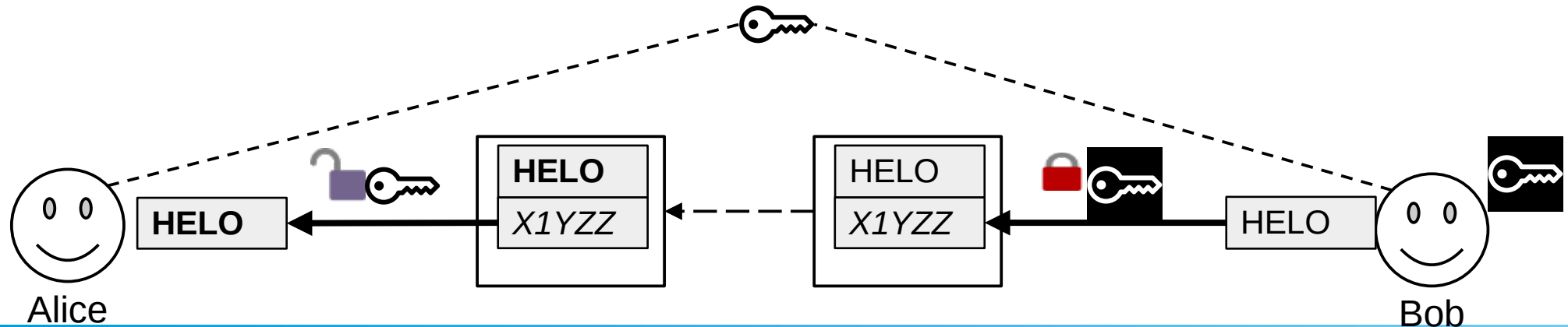
- 1) Bob vuole mandare un messaggio ad Alice, ma tale che Alice possa verificare il mittente.
- 2) Bob cifra il messaggio usando la propria chiave privata (Bob **firma** il messaggio).
- 3) Invia poi ad Alice sia il messaggio cifrato che il testo in chiaro.
- 4) Alice decifra il messaggio cifrato usando la chiave pubblica di Bob



Crittografia asimmetrica - autenticità

Un messaggio cifrato con la chiave privata deve essere decifrato con la chiave pubblica.

- 1) Bob vuole mandare un messaggio ad Alice, ma tale che Alice possa verificare il mittente.
- 2) Bob cifra il messaggio usando la propria chiave privata (Bob **firma** il messaggio).
- 3) Invia poi ad Alice sia il messaggio cifrato che il testo in chiaro.
- 4) Alice decifra il messaggio cifrato usando la chiave pubblica di Bob e
- 5) verifica che coincide col messaggio in chiaro. **Solo chi conosce la chiave privata di Bob avrebbe potuto generare il messaggio cifrato.**



RSA

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti.

RSA

1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti

1983 – Al Massachusetts Institute of Technology, Rivest, Shamir e Adleman brevettano il sistema di crittografia asimmetrica RSA, basato sull'utilizzo di numeri primi *grandi*.

RSA

1973 – In un documento (segreto) dei servizi segreti britannici, Clifford Cocks descrive un sistema di crittografia asimmetrica simile a RSA.

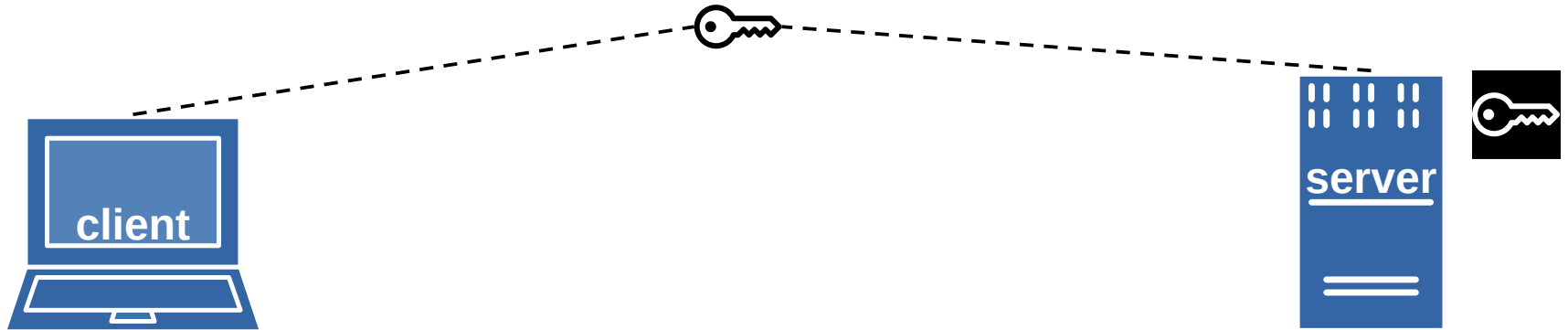
1976 – Diffie e Hellman teorizzano un sistema di crittografia **asimmetrica** basato su un sistema di chiavi ognuna costituita da due parti.

1983 – Al Massachusetts Institute of Technology, Rivest, Shamir e Adleman brevettano il sistema di crittografia asimmetrica RSA, basato sull'utilizzo di numeri primi *grandi*.

Transport Layer Security (TLS)

Il protocollo Transport Layer Security (TLS, RFC 8446) è un protocollo per le comunicazioni *sicure* nelle reti di computer, solitamente usato con TCP/IP.

1) Il *client* (chi inizia la connessione) deve conoscere la chiave pubblica del *server*.

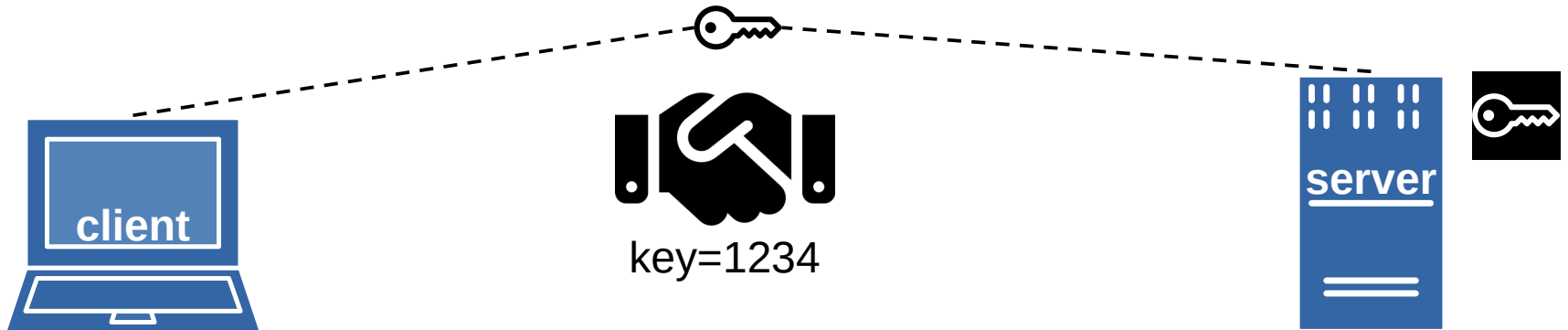


Transport Layer Security (TLS)

Il protocollo Transport Layer Security (TLS, RFC 8446) è un protocollo per le comunicazioni *sicure* nelle reti di computer, solitamente usato con TCP/IP.

1) Il *client* (chi inizia la connessione) deve conoscere la chiave pubblica del *server*.

2) **Handshake**: usando questa, client e server concordano su una **chiave simmetrica**.



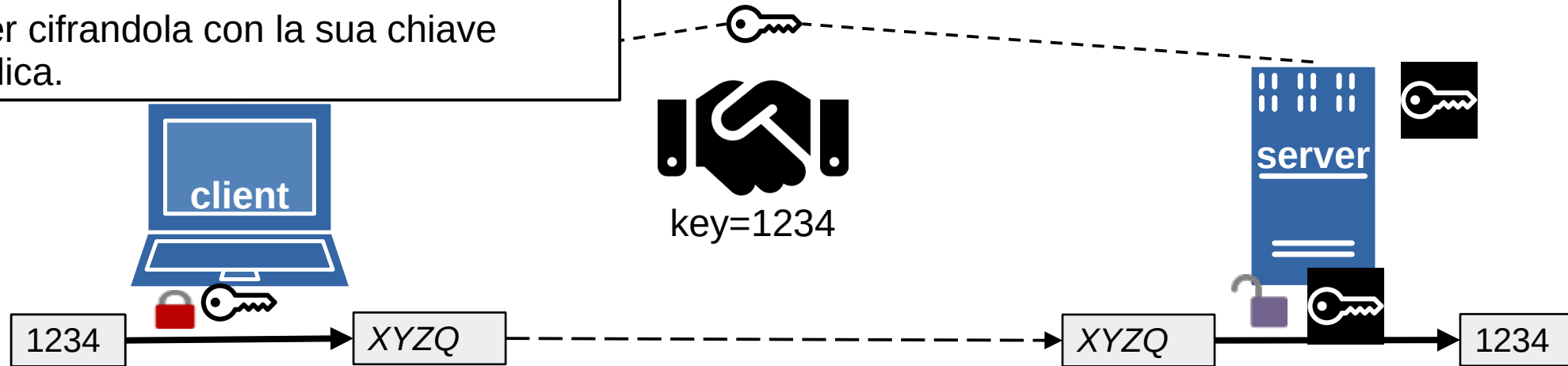
Transport Layer Security (TLS)

Il protocollo Transport Layer Security (TLS, RFC 8446) è un protocollo per le comunicazioni *sicure* nelle reti di computer, solitamente usato con TCP/IP.

1) Il *client* (chi inizia la connessione) deve conoscere la chiave pubblica del *server*.

2) **Handshake**: usando questa, client e server concordano su una **chiave simmetrica**.

Ad esempio, il client genera una chiave simmetrica casualmente e la invia al server cifrandola con la sua chiave pubblica.



Font Awesome, CC BY 4.0, via Wikimedia Commons

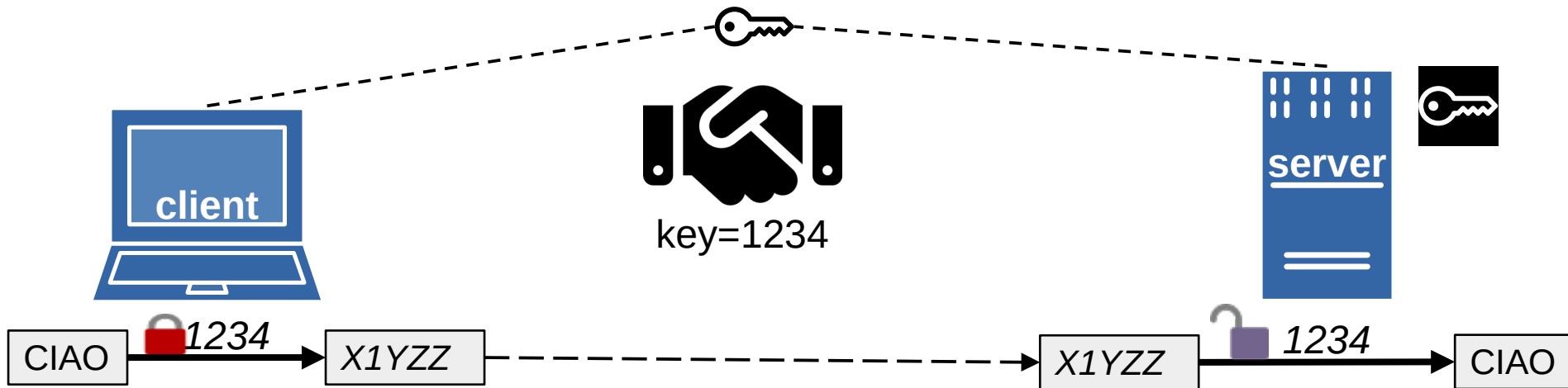
Transport Layer Security (TLS)

Il protocollo Transport Layer Security (TLS, RFC 8446) è un protocollo per le comunicazioni *sicure* nelle reti di computer, solitamente usato con TCP/IP.

1) Il *client* (chi inizia la connessione) deve conoscere la chiave pubblica del *server*.

2) **Handshake**: usando questa, client e server concordano su una **chiave simmetrica**.

3) I messaggi inviati saranno codificati con questa.



Font Awesome, CC BY 4.0, via Wikimedia Commons

HTTPS

HTTP Over TLS (HTTPS, RFC9110) = HTTP + TLS

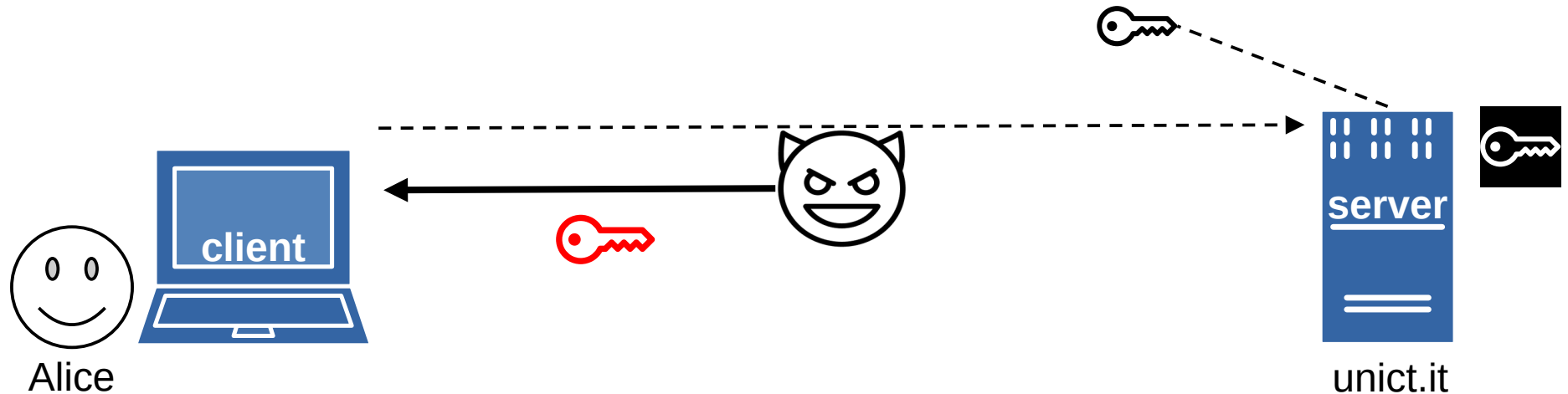
Offre le seguenti garanzie al client

- **confidenzialità** - i dati inviati in una form possono essere letti solo dal server
- **autenticità** – I dati ricevuti sono stati sicuramente generati dal server

Distribuzione delle chiavi

Per poter utilizzare la crittografia simmetrica è necessario che il client prima ottenga la chiave pubblica del server.

Farsela inviare su internet **non** è una buona idea.

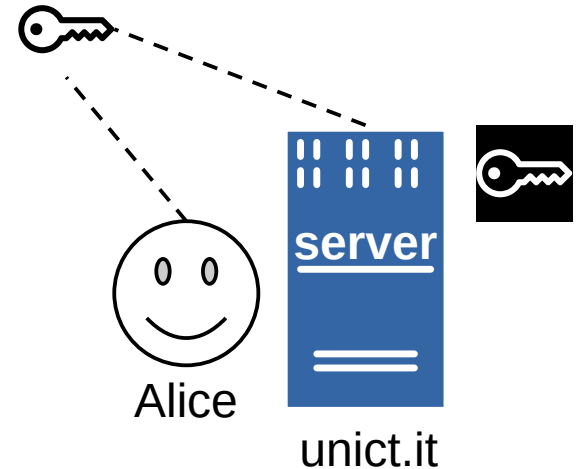


Distribuzione delle chiavi

Per poter utilizzare la crittografia simmetrica è necessario che il client prima ottenga la chiave pubblica del server.

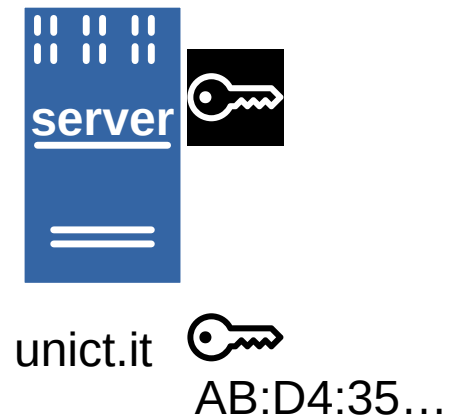
Farsela inviare su internet **non** è una buona idea.

Meglio andarla a prendere di persona.



Certificati RSA

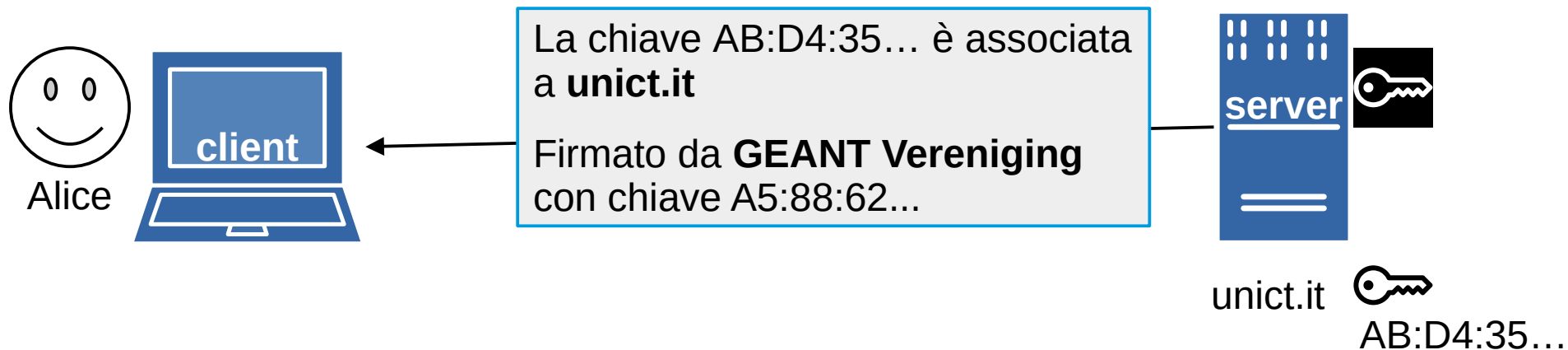
Usando HTTPS, la chiave pubblica è legata al nome di dominio.



Certificati RSA

Usando HTTPS, la chiave pubblica è legata al nome di dominio.

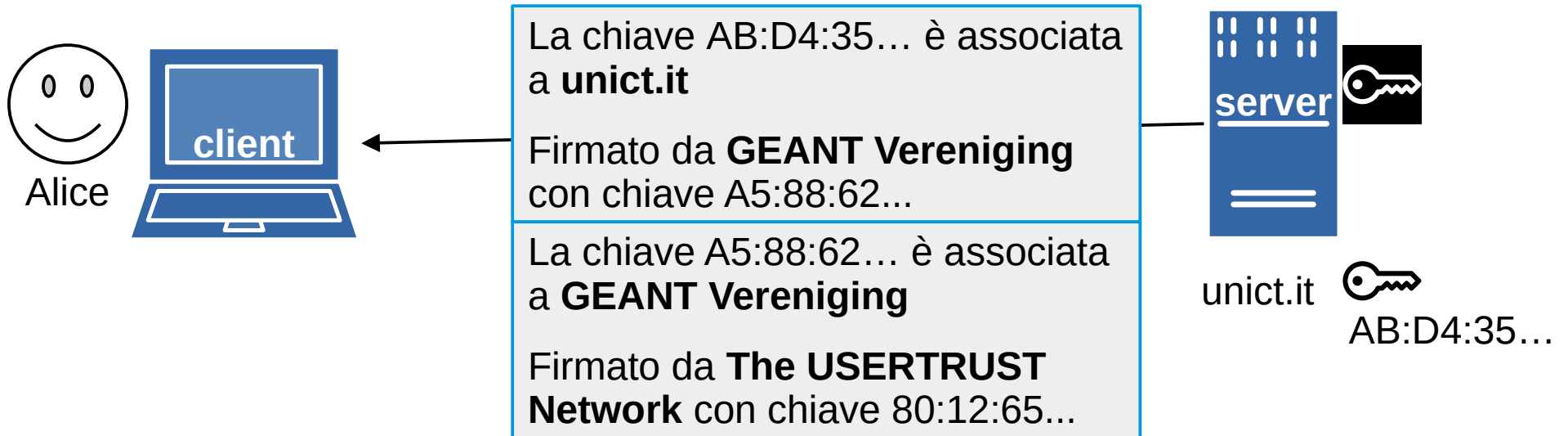
Il server rilascia un certificato, firmato da una terza parte, che attesta che la chiave pubblica è associata ad uno specifico nome di dominio.



Certificati RSA

Usando HTTPS, la chiave pubblica è legata al nome di dominio.

Il server rilascia un certificato, firmato da una terza parte, che attesta che la chiave pubblica è associata ad uno specifico nome di dominio. Può essere una **catena** di certificati.



Certificati RSA

Usando HTTPS, la chiave pubblica è legata al nome di dominio.

Il server rilascia un certificato, firmato da una terza parte, che attesta che la chiave pubblica è associata ad uno specifico nome di dominio. Può essere una **catena** di certificati.

Il client possiede un elenco di chiavi pubbliche associate ad **autorità** ben note.

