



WIRELESS COMMUNITY NETWORK

PGP - Crittografia per tutti

Fusolab 21.01.2012



marco.giuntini@gmail.com



Crittografia

✓ L'arte di nascondere informazioni

- Molto antica (Egizi, Giulio Cesare, etc.)

✓ Di solito:

- Mittente (Alice) → cifra un messaggio
- Destinatario (Bob) → decifra il messaggio



✓ Per decifrare un messaggio cifrato, il destinatario ha bisogno di:

- Algoritmo
- Chiave

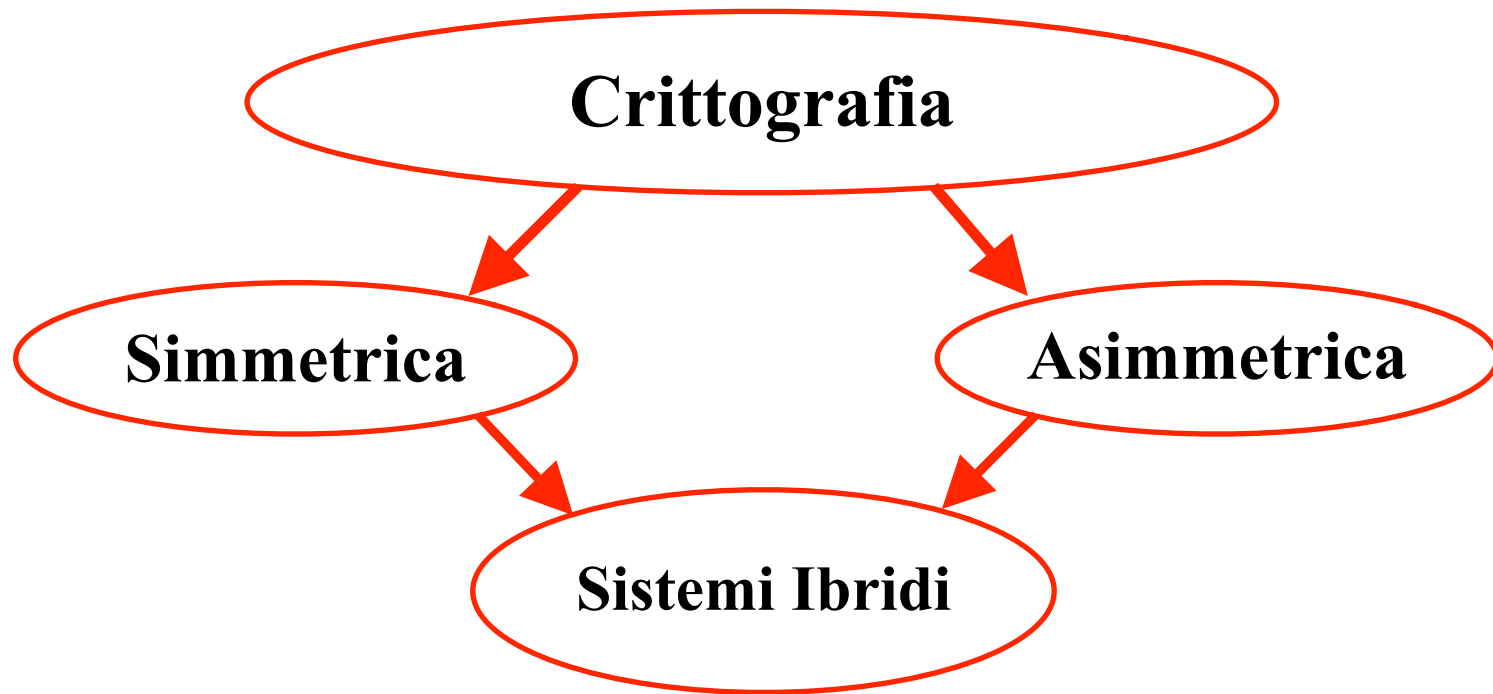


Crittografia - Esempio

1. Algoritmo: sostituisci ogni lettera del messaggio con quella che si trova k posti dopo nell'alfabeto inglese (chiave = k)
2. Messaggio in chiaro (cleartext): “ciao mondo”
3. Chiave = 2
4. Messaggio cifrato (ciphertext): “ekcq oqpfq”

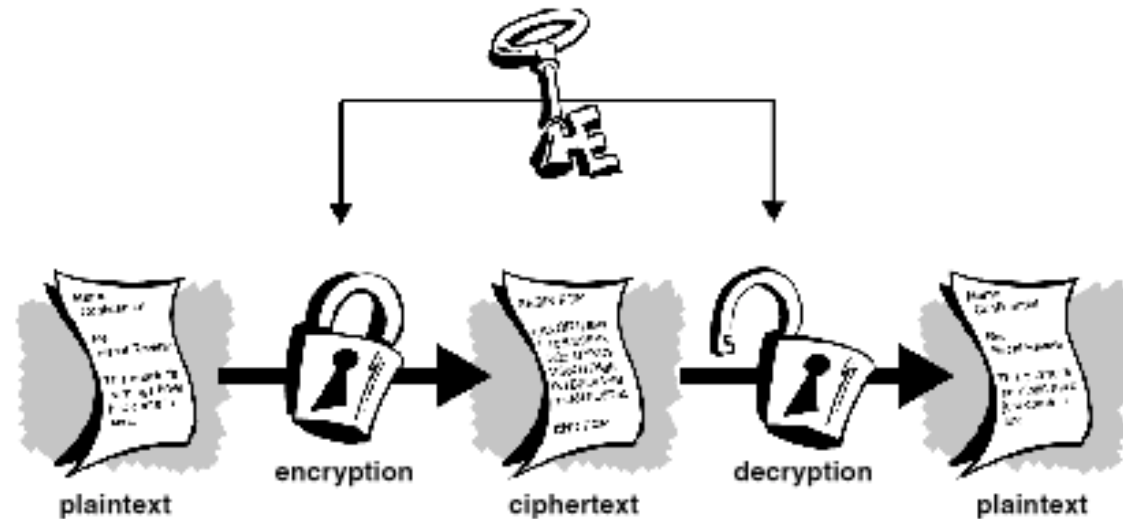


Crittografia



Crittografia Simmetrica

Chiave singola per cifrare/decifrare

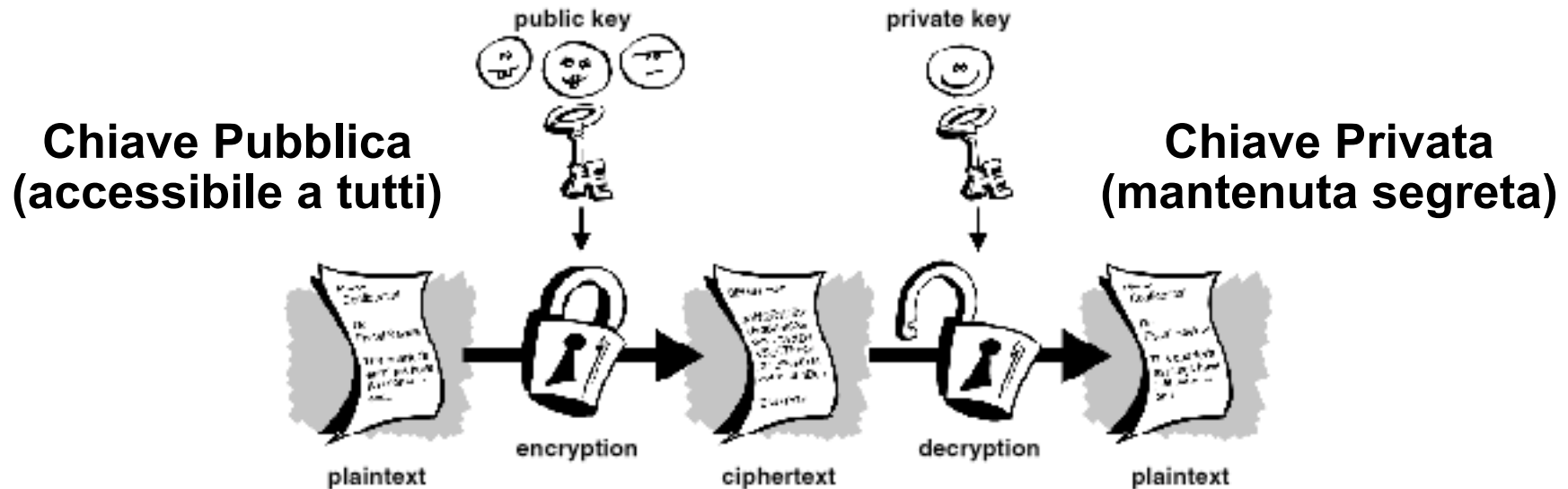


- ✓ La serratura può essere chiusa/aperta con la stessa chiave
- ✓ La chiave deve essere duplicata/scambiata tra gli interlocutori
- ✓ Occorre una chiave per ogni coppia di corrispondenti
- ✓ Nasce il problema della trasmissione in modo sicuro della chiave



Crittografia Asimmetrica

Coppia di chiavi correlate



- ✓ La serratura può essere chiusa con una chiave ma aperta solo con l'altra (e viceversa)
- ✓ Non è possibile ricavare la chiave privata dalla corrispondente chiave pubblica
- ✓ Sparisce il problema della trasmissione di chiavi
- ✓ Lenta se applicata a chiavi di grandi dimensioni



Sistemi Ibridi

- ✓ Sono sicuramente i più efficienti
- ✓ Sfruttano i pregi di entrambe:
 - La sicurezza della Crittografia Asimmetrica
 - La velocità della Crittografia Simmetrica
- ✓ Evitano i difetti:
 - La lentezza della Crittografia Asimmetrica
 - Il problema della trasmissione della chiave nella Crittografia Simmetrica
- ✓ PGP e OpenPGP si basano su un sistema ibrido.



PGP - Pretty Good Privacy

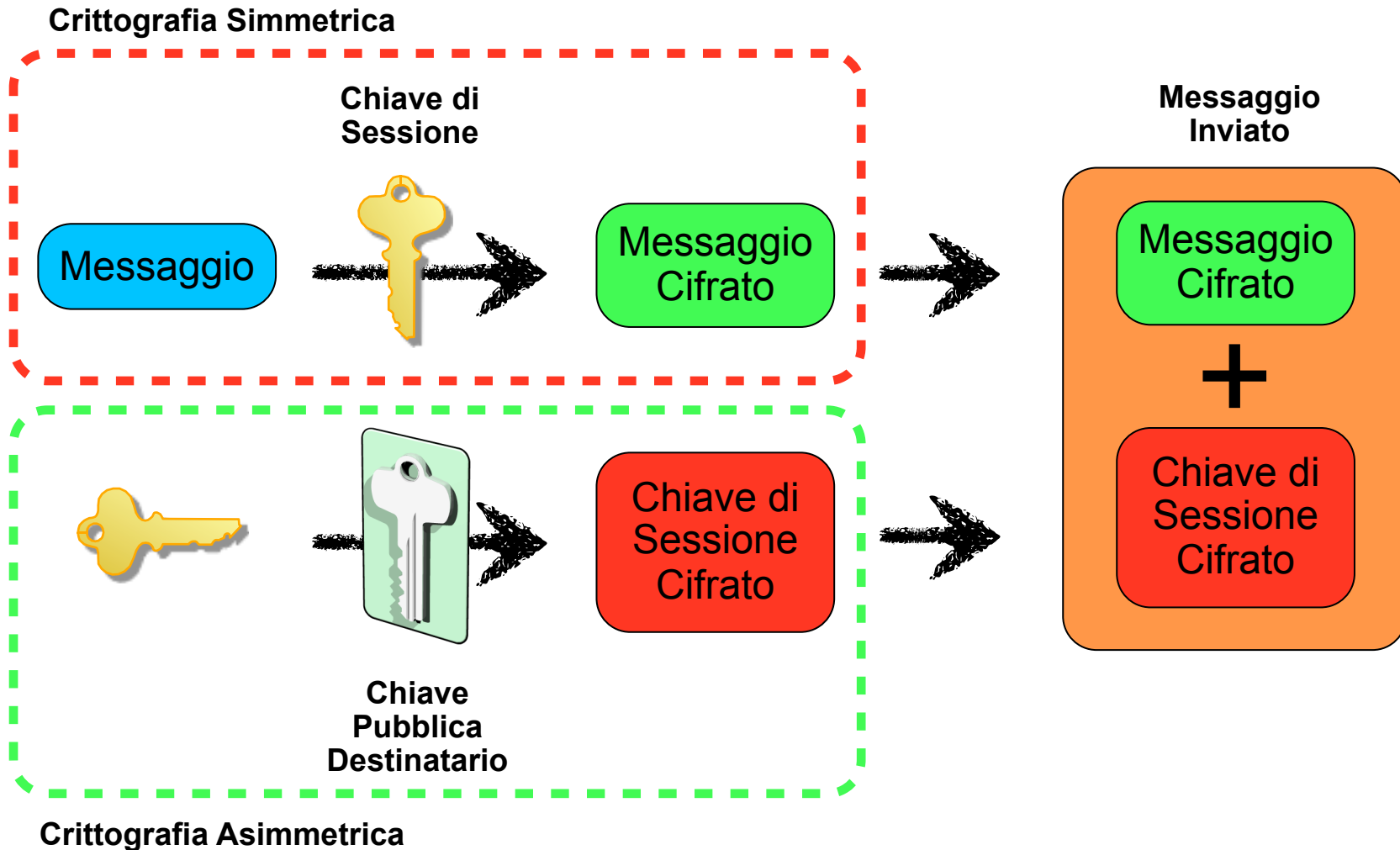
- ✓ **PGP** è un programma di crittografia e firma digitale ideato e sviluppato da **Phil Zimmermann** nel 1991
 - Uno dei crittosistemi più usati al mondo
 - Divenuto un prodotto commerciale della PGP corp.
- ✓ **OpenPGP** è uno standard Internet (RFC 4880) che è stato pubblicato sulla base della specifica originale di PGP
- ✓ **GPG** (GNU Privacy Guard) è un'implementazione open-source (licenza GPL) dello standard OpenPGP



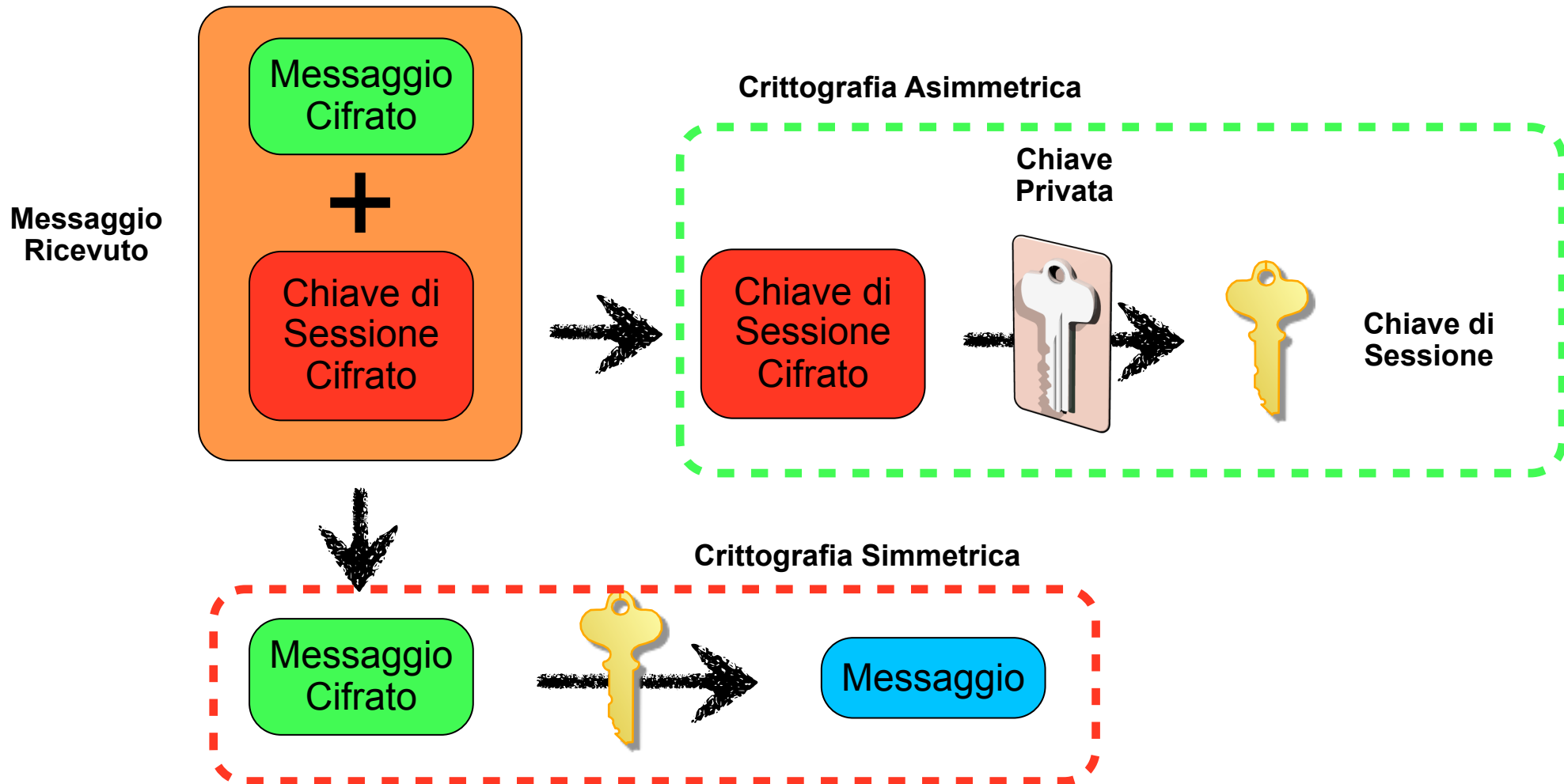
Phil
Zimmermann



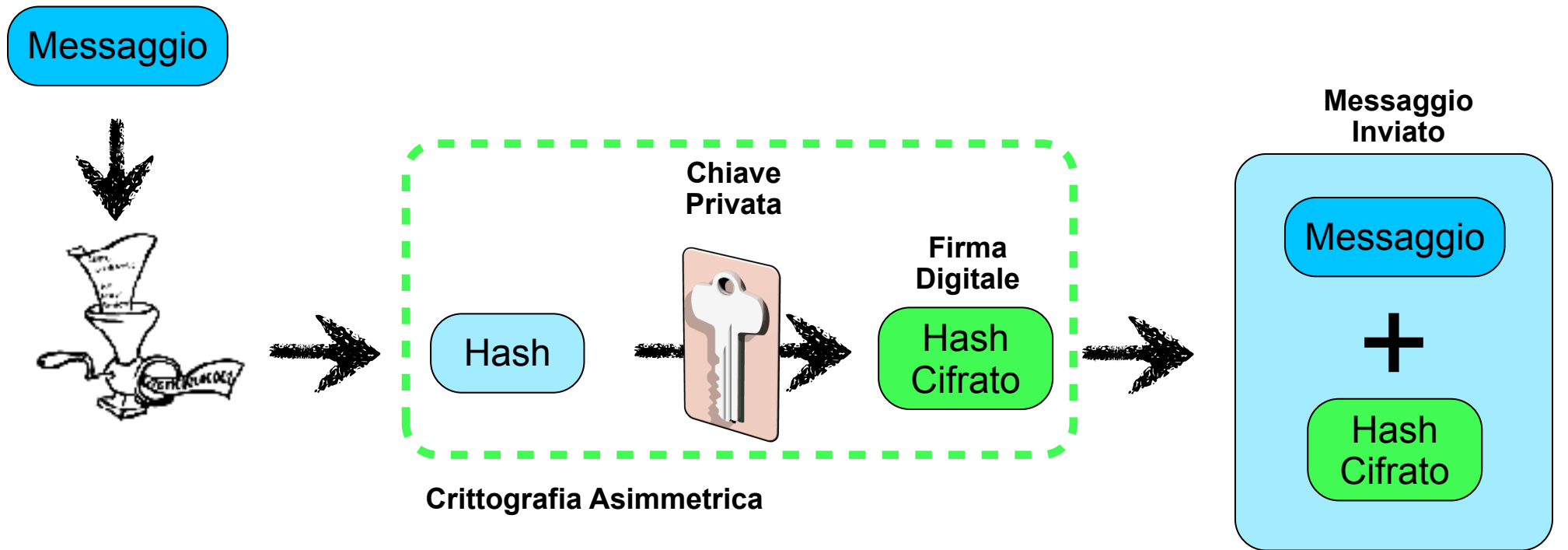
Cifratura Messaggio



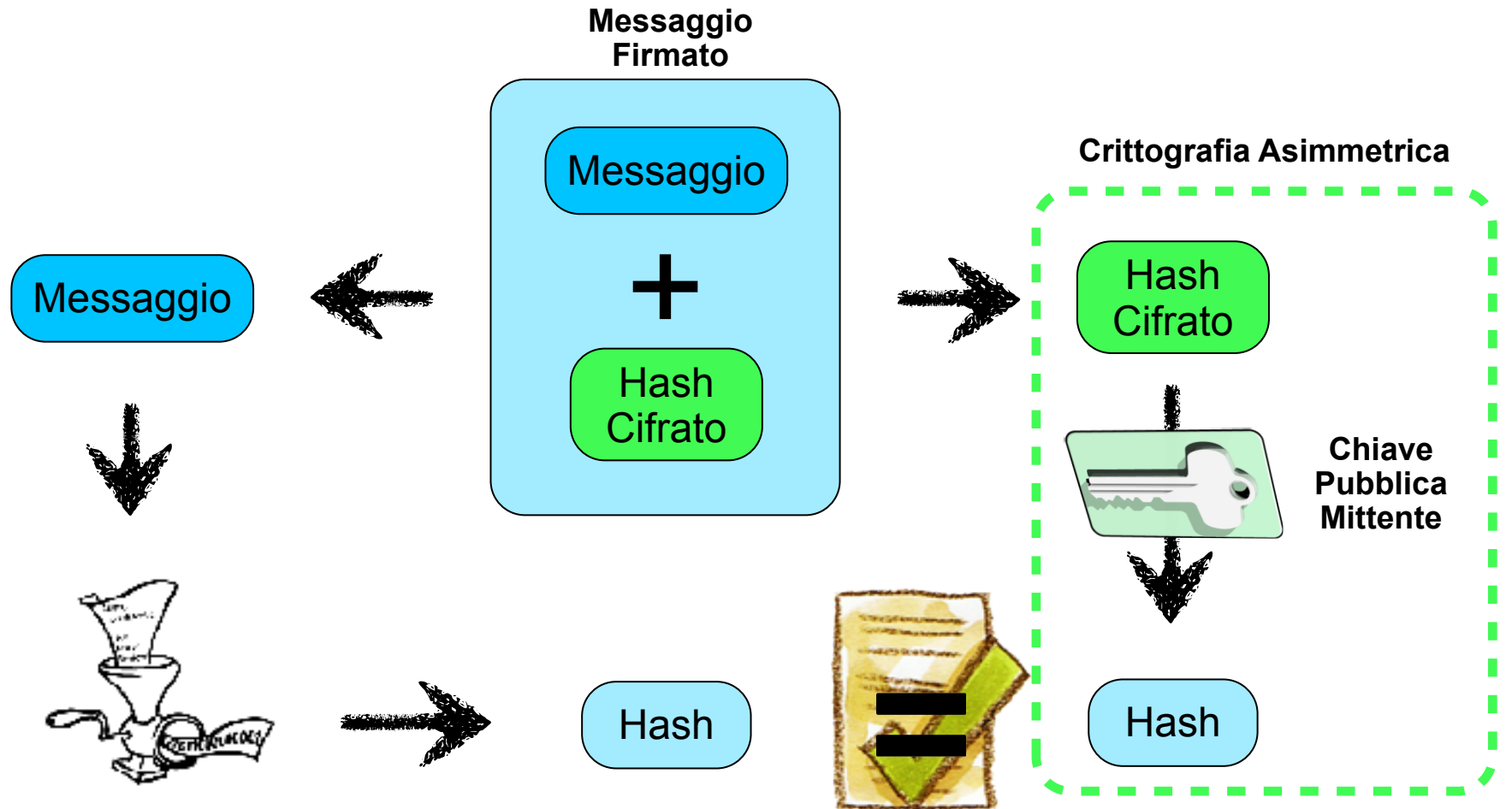
Decifratura Messaggio



Firma



Verifica della Firma



Riassumendo

Siamo riusciti ad ottenere:

- Riservatezza (cifrando i messaggi)
- Autenticazione e Integrità (firmando i messaggi)

Nascono alcuni problemi:

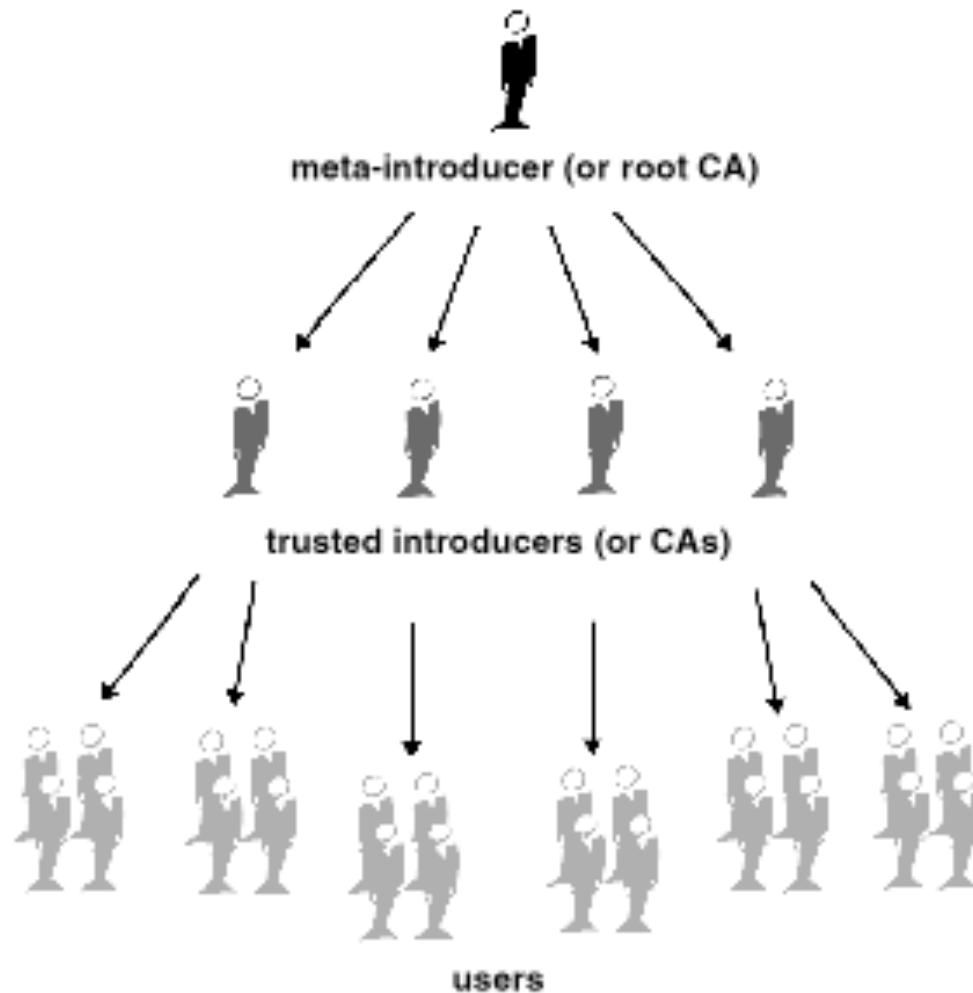
- Come si può ottenere la chiave pubblica di una persona?
- Come si può essere realmente certi che una certa chiave appartenga ad una certa persona?

Soluzione:

- **Certificati Digitali e PKI**
- **Web Of Trust**

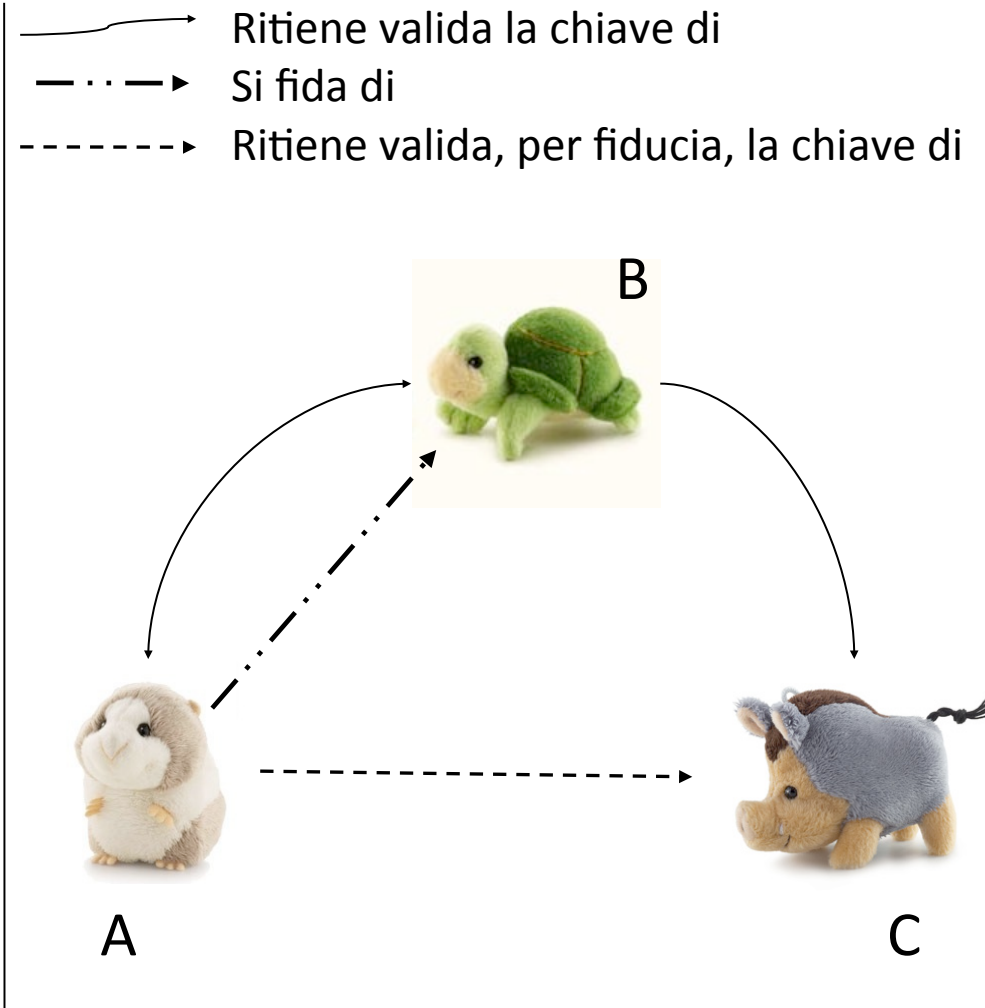


PKI - Public Key Infrastructure



Web of Trust

- L'utente A conosce solo B
 - ✓ Ha verificato l'identità di B e ha firmato la sua chiave
 - ✓ Si fida di B
- B conosce C
 - ✓ Ha verificato l'identità di C e ha firmato la sua chiave
 - ✓ Invia ad A la chiave di C firmata
- Dato che A si fida nella capacità di B di verificare chiavi, accetta la chiave di C come valida
 - ✓ Questo non implica che A si debba fidare di C!

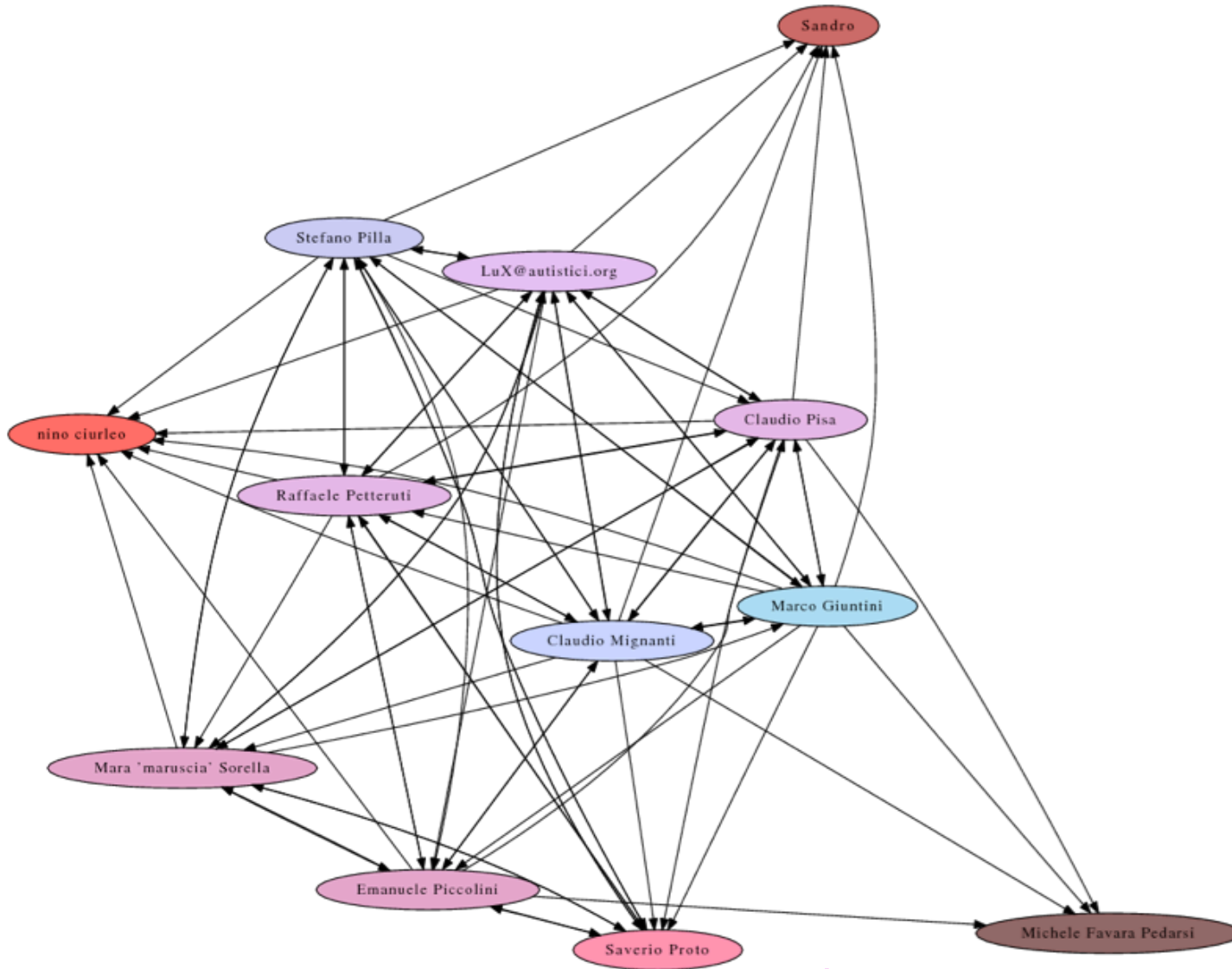


Signing Party

- Un **Key Signing Party** è una riunione di persone che usano il sistema di crittografia PGP
- Ogni partecipante ha la possibilità verificare l'identità e firmare la chiave degli altri
- Estendere la propria rete della fiducia (**Web Of Trust**)
- Inoltre offrono un'opportunità per discutere di questioni sociali e politiche che riguardano la crittografia



Ninux Web Trust



Bibliografia

- <http://www.gnupg.org>
- <http://www.gnupg.org/gph/en/manual.html>
- <http://www.pgpi.org/doc/pgpintro/>
- <http://wiki.tzunami.it/doku.php?id=keysigning>
- <http://wiki.ninux.org/PGPSigningParty>

