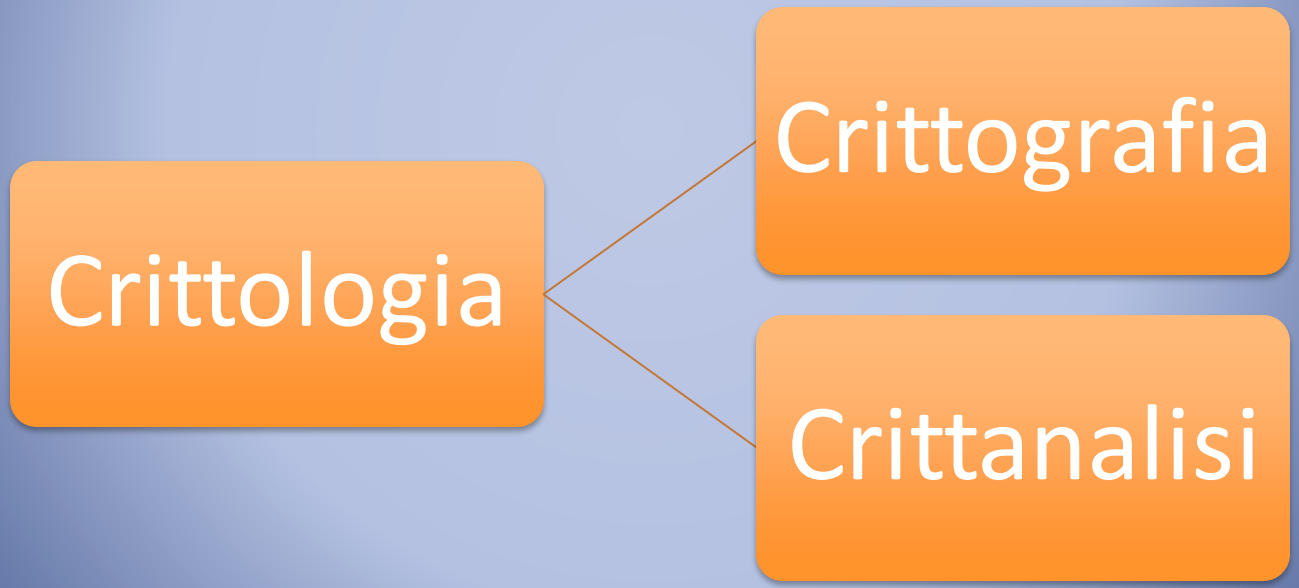
Crittografia

Crittologia

- Kriptòs (nascosto) + logos (discorso)



Crittografia - Introduzione

- Kryptós (nascosto) + graphía (scrittura)
- Garantire la confidenzialità dei dati
- Impedire attacchi informatici ai dati sensibili

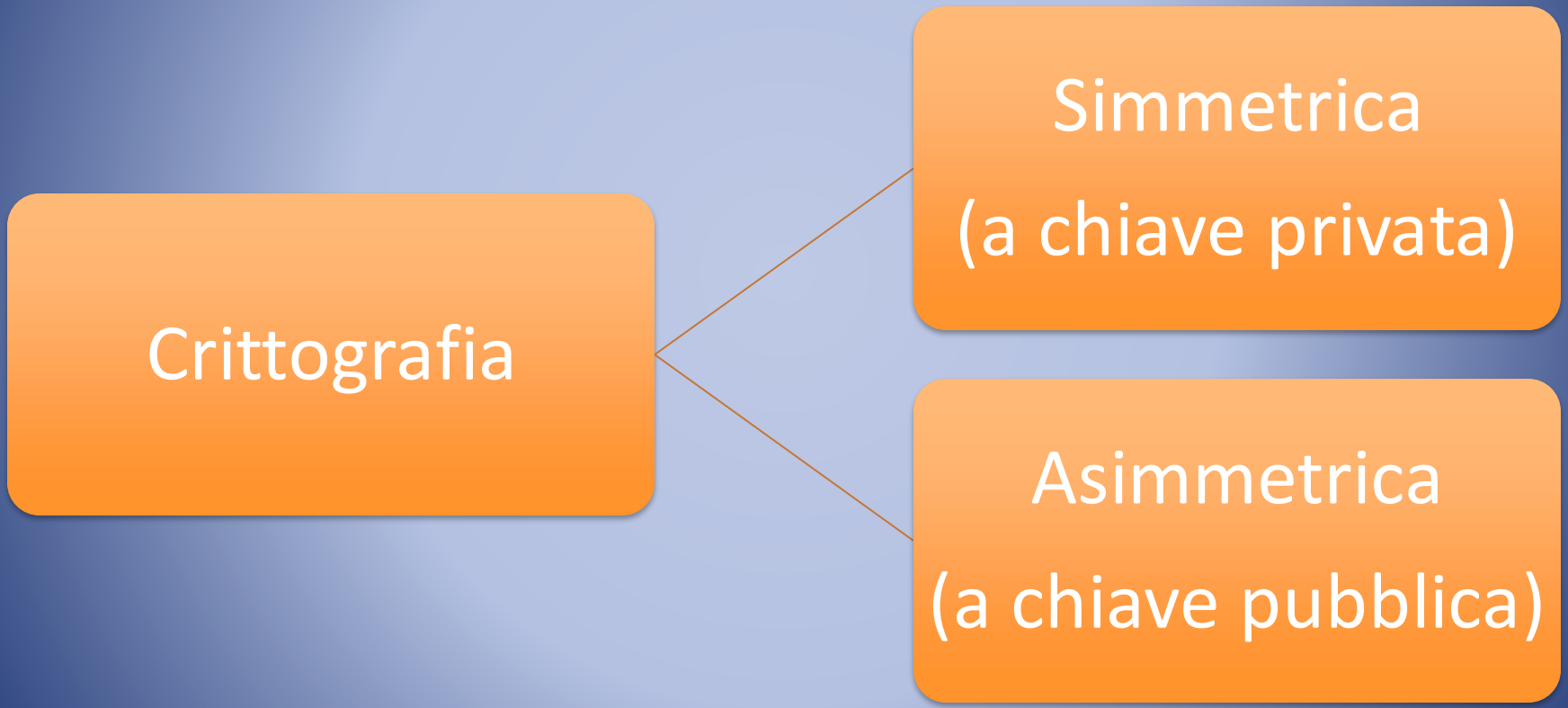
Sistema sicuro

- Può anche essere violabile
- Incidenza del fattore tempo
- Unica tecnica sicura in senso assoluto: *Cifrario di Vernam*

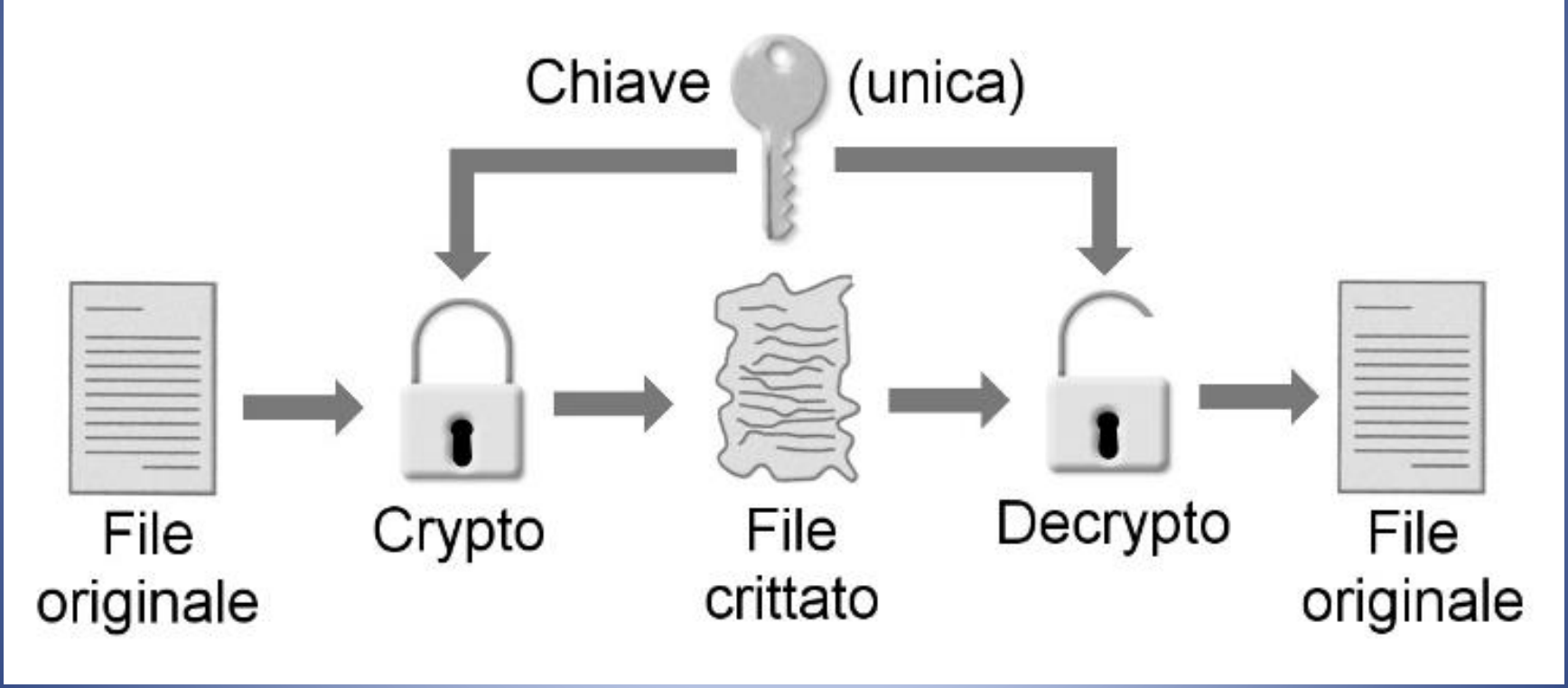
Cifrario di Vernam

- Chiave lunga quanto il testo
- Chiave non riutilizzabile
- “Cifrario perfetto”
- *Esempio*

Tipi di Crittografia



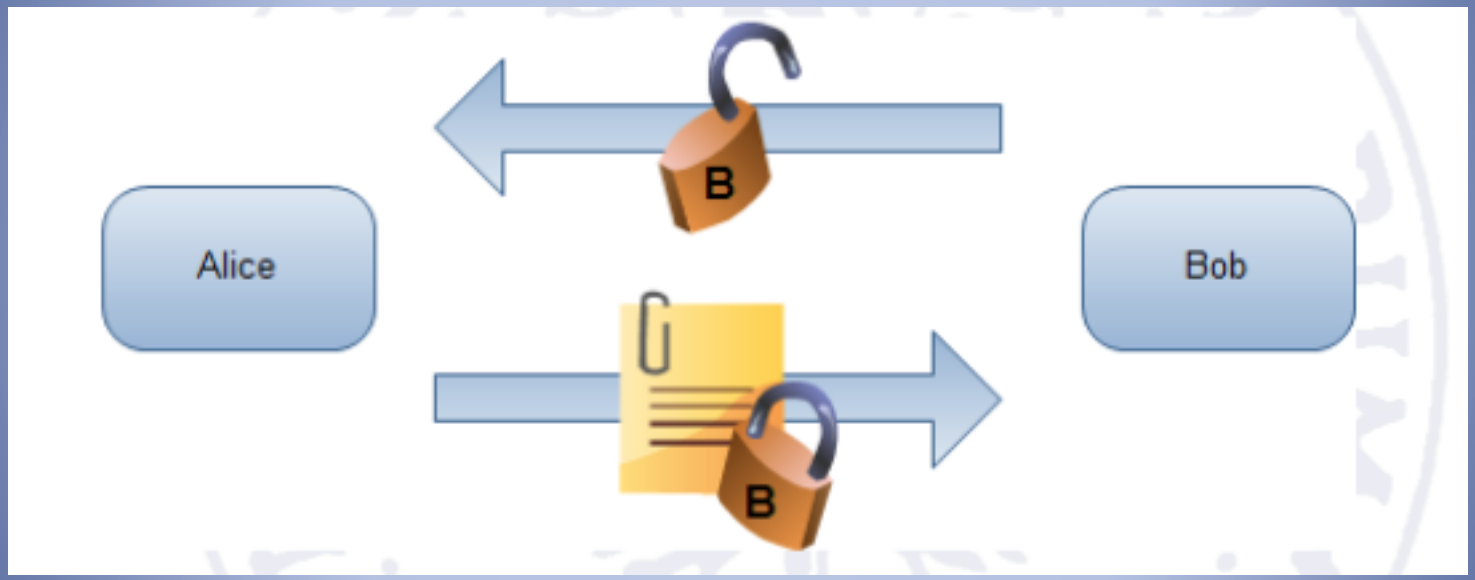
Crittografia Simmetrica



Crittografia Simmetrica

- Vantaggi
  - Velocità di funzionamento
  - Possibilità di utilizzare chiavi lunghe
- Svantaggi
  - Aumento velocità processori
  - Uso ripetuto della stessa chiave
  - Distribuzione delle chiavi

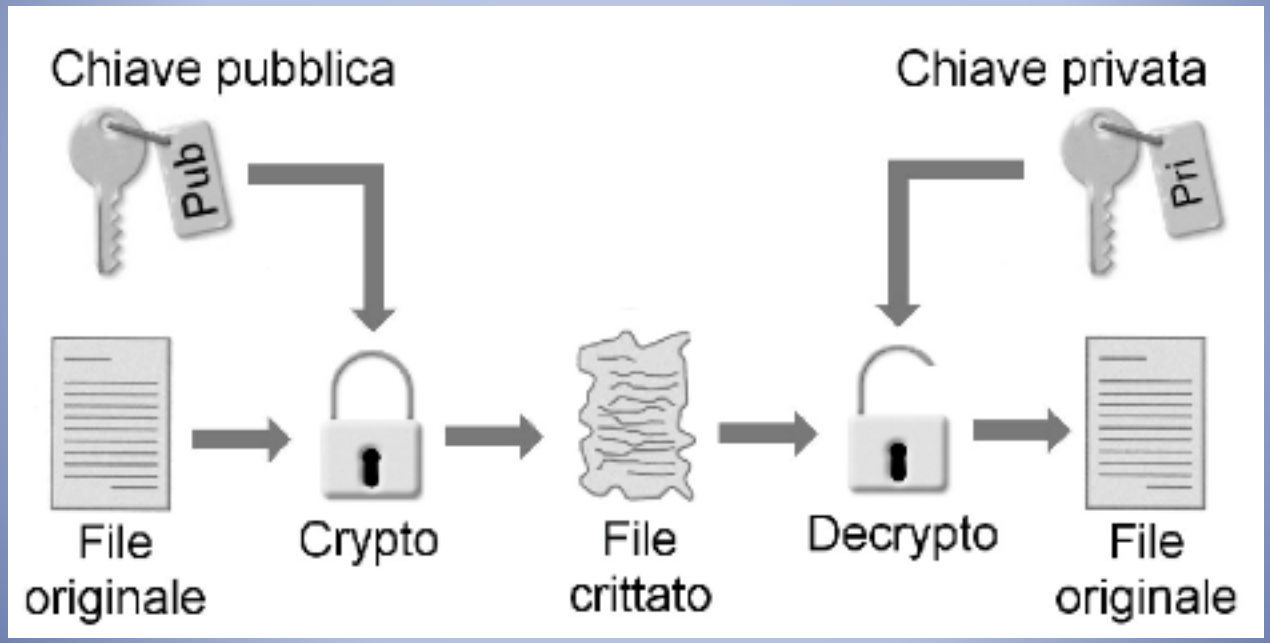
Crittografia Asimmetrica



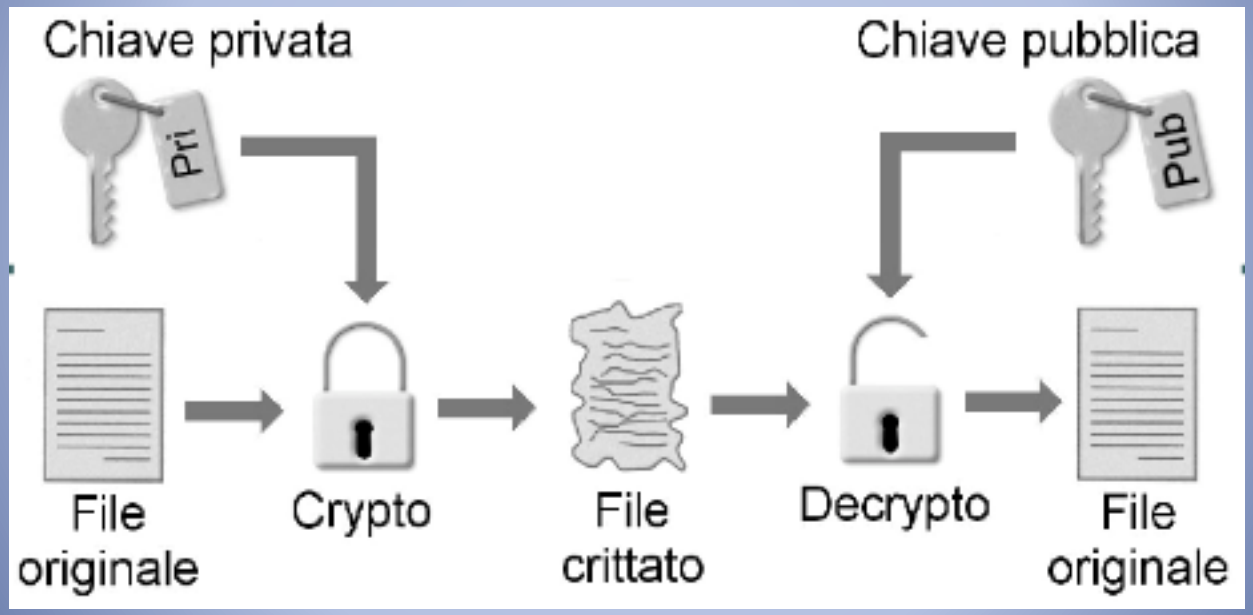
Crittografia Asimmetrica

- Due chiavi diverse
- Una chiave per crittografare: chiunque può vedere/possedere
- Una chiave per decifrare in possesso soltanto del destinatario
- Le chiavi sono invertibili

Crittografia Asimmetrica - 1



Crittografia Asimmetrica - 2



Crittografia Asimmetrica – modalità di funzionamento

- Modalità autenticazione: solo il possessore della chiave privata può aver cifrato il file. Non è garantita la riservatezza.
- Modalità confidenziale: solo il possessore della chiave privata può decifrare il file

Algoritmi simmetrici: DES e AES

- Data Encryption Standard:
  - Sviluppato da IBM e definito dal Governo degli Stati Uniti come standard ufficiale. (1974-1976)
  - Chiave a 64 bit (56 effettivi)
- Advanced Encryption Standard:
  - Adottato come standard ufficiale dagli USA nel 2001
  - Chiave a 128, 192 o 256 bit

RSA

- Ronald Rivest, Adi Shamir, Leonard Adleman
- Necessario usare chiavi di almeno 2048 bit
- Si basa sulla fattorizzazione in numeri primi

Firma Digitale

- Il mittente firma il messaggio con la propria chiave privata
- La firma è verificabile e non falsificabile
- Non ripudio
- Autorità di certificazione