

# CIFRARI ASIMMETRICI: INTRODUZIONE

21/03/2023

Non abbiamo ancora parlato del problema dello **SCAMBIO DI CHIAVI** (**KEY DISTRIBUTION**) che va a "braccetto" con quello dell' **INTEGRITÀ** e dell' **AUTENTICAZIONE**.

Tutti questi problemi ci danno la motivazione per iniziare il nuovo argomento della **CRITTOGRAFIA ASIMMETRICA** o, anche detta, a **CHIAVE PUBBLICA**. Tutto questo ci aiuterà nei problemi sopra citati e ci darà una nuova visione del mondo:

**CIFRARI ASIMMETRICI**  $\longrightarrow$  Le **CHIAVI** per (DE)CIFRARE sono **DIVERSE**



Tutto ciò può sembrare molto contro intuitivo (rispetto a quanto visto nelle scorse lezioni) ... ma, come vedremo le chiavi  $K_1$  e  $K_2$  sono legate da una (complessa) relazione matematica.

Per il nostro avversario sarà impossibile risalire ad una delle due chiavi conoscendo l'altra. non è possibile ottenere  $K_2$  da  $K_1$  e viceversa.

I **CIFRARI ASIMMETRICI** si basano sulla **DIFFICOLTÀ COMPUTAZIONALE**:

**NOI**  $\longrightarrow$  **COMPLESSITÀ LINEARE** (al più **POLINOMIALE**)  
**AVVERSARIO**  $\longrightarrow$  **COMPLESSITÀ ESPONENZIALE**

Poiché richiediamo più risorse computazionali sia per cifrare e decifrare, sia per generare le chiavi, i **CIFRARI ASIMMETRICI** non sostituiscono le strategie viste fino ad ora, bensì si affiancano.

# IDEA GENERALE

$K_1$  la CHIAVE PUBBLICA (+)

$K_2$  la CHIAVE PRIVATA (-)



A CIFRA  $K(A)^-$

B DECIFRA  $K(A)^+$

Analogamente se B vuole rispondere:

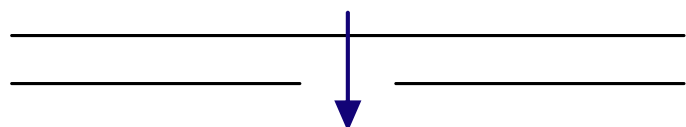
B CIFRA  $K(B)^-$

A DECIFRA  $K(B)^+$



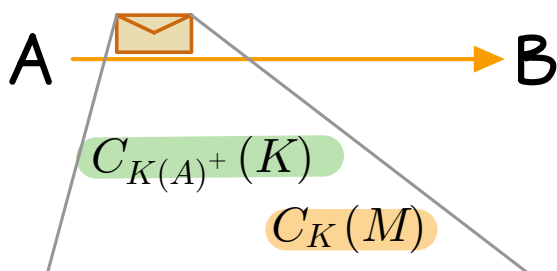
Im totale quindi avrò 4 chiavi. Come suggerisce il nome ogni coppia di chiave è generata dai rispettivi mittenti.

## DIGITAL ENVELOPE: (BUSTA DIGITALE)



È un modo efficiente per inviare in maniera sicura dei dati.

(soprattutto nel caso di grosse dimensioni)



Uso un CIFRARIO ASIMMETRICO per cifrare la chiave del CIFRARIO SIMMETRICO.

Più nello specifico, A:

- Genero una CHIAVE SIMMETRICA  $K$  (es: 128b AES)
- Cifro  $K$  con CHIAVE ASIMMETRICA  $K(A)^-$

B: Decifra con CHIAVE ASIMMETRICA  $K(A)^+$  ottenendo  $K$

Il resto della comunicazione avverrà tramite CIFRARIO SIMMETRICO (es: AES)

Si parla di BUSTA DIGITALE in senso metaforico: premendo la busta e ci metto dentro la chiave cifrata e il messaggio cifrato.