Crittografia

Tommaso Vitali e Andrea Maenza

A.S. 2015/16

1 Introduzione

La crittografia è un sottoinsieme della crittologia che ha il compito di nascondere e criptare un messaggio agli utenti non autorizzati a leggerlo. Le tecniche di cifratura principali sono:

- Crittografia Simmetrica
- Crittografia Asimmetrica
- Crittografia Quantistica

Tutte le tre tecniche di cifratura citate sopra fanno parte delle tecniche di cifratura basate su chiave.

2 Crittografia a chiavi segrete o simmetriche

La crittografia simmetrica era l'unica tecnica di cifratura utilizzata fino a qualche anno fa. Consiste nell'utilizzo di un'unica chiave per cifrare e decifrare, che deve chiaramente rimanere sconosciuta a tutti tranne che ai due interlocutori.

Questo tipo di crittografia è molto **efficiente** e **sicuro**, ma presenta un grande problema: la necessità di disporre di un canale sicuro per la trasmissione della chiave.

3 Crittografia a chiavi pubbliche o asimmetriche

Una tecnica più moderna rispetto alla precedente è la crittografia asimmetrica.

Consiste nell'utilizzo di due chiavi diverse: una per cifrare e l'altra per decifrare. Una delle due chiavi è pubblica e conosciuta da tutti, mentre l'altra è privata. Entrambe le chiavi possono essere usate sia per cifrare che per decifrare,

ma se una è stata usata per cifrare allora non può essere utilizzata anche per decifrare.

Questa tecnica viene anche chiamata crittografia a coppia di chiavi o crittografia a chiave pubblica/privata, proprio perchè esistono due tipologie di chiavi differenti: la chiave pubblica (accessibile a chiunque) e la chiave privata (personale e segreta).

In questa maniera la trasmissione viene resa più **sicura** e **affidabile** rispetto alla crittografia simmetrica, sopratutto per il fatto che non necessita di condividere la chiave con il destinatario.

L'unico problema di questo tipo di crittografia è il fatto che sia **poco efficiente** (lentezza nel cifrare e decifrare).

4 La soluzione moderna

Una delle soluzioni utilizzate al giorno d'oggi consiste nell'utilizzare entrambi i tipi di crittografia: vengono utilizzate le **chiavi asimmetriche** per lo scambio delle **chiavi segrete (simmetriche)**, con cui si può utilizzare la crittografia a chiavi simmetriche (più efficiente).

5 Esercizi

1. AUTENTICITÀ: A deve mandare M1 a B garantendo l'autenticità del messaggio

   - M2 = cifra(M1, pr_A) →A cifra M1 con la propria chiave privata
   - M2 trasmesso da A a B
   - M1 = decifra(M2, pu_A) →B decifra M2 con la chiave pubblica di A

   Il messaggio si decifra con la chiave pubblica di A, quindi è stato per forza cifrato con la chiave privata di A: AUTENTICITÀ GARANTITA!

2. RISERVATEZZA: A deve mandare M1 a B garantendo la riservatezza del messaggio

   - M2 = cifra(M1, pu_B) →A cifra M1 con la chiave pubblica di B
   - M2 trasmesso da A a B
   - M1 = decifra(M2, pr_B) →B decifra M2 con la propria chiave privata

   La chiave privata di B è conosciuta esclusivamente da B, quindi è garantita la RISERVATEZZA!

3. AUTENTICITÀ e RISERVATEZZA: A deve mandare M1 a B garantendo autenticità e riservatezza del messaggio

   - M2 = cifra(cifra(M1, pr_A), pu_B) →A cifra M1 con la propria chiave privata e con la chiave pubblica di B

- M2 trasmesso da A a B
- M1 = decifra(decifra(M2, pr_B), pu_A) →B decifra M2 con la chiave pubblica di A e con la propria chiave privata

Sono garantite sia AUTENTICITÀ che RISERVATEZZA: il messaggio può essere aperto esclusivamente da B (è necessaria la sua chiave privata), ma al contempo si apre solo con la chiave pubblica di A, quindi può essere stato cifrato solo da A (con la sua chiave privata).

4.
- decifra(cifra(M, pr_A), pu_A) = **M**
- (decifra(cifra(M, pr_A) ,pu_A) == decifra(cifra(M, pu_A) ,pr_A)) = **TRUE**