University of Pisa

Department of Information Engineering

Foundation Of Cybersecurity

Nicolò Mariano Fragale

March 2025

Contents

Information

These notes are intended for educational purposes only and cover essential concepts in the field of data systems and security. The aim is to provide a comprehensive understanding of topics such as system vulnerabilities, protection techniques, and defense strategies in cybersecurity.

This document includes topics related to access control, authentication mechanisms, database security, cryptographic methods, and advanced persistent threats, with a particular focus on practical applications in real-world scenarios.

1 Symmetric cryptography

2 Asymmetric cryptography

2.1 RSA

2.2 Diffie-Hellman exchange

Necessary Definitions:

- **Groups:**
- **Sub-Groups:**
- **Finite Groups:**
- **Ciclic Groups:**

$\mathbb{Z}_p^*$:

Il protocollo di **Diffie-Hellman Key Exchange** permette a due parti di concordare una chiave segreta condivisa su un canale insicuro. Vediamo il processo con un esempio pratico.

Parametri pubblici

Prima di tutto, Alice e Bob scelgono un numero primo pubblico p (modulo) e una base (o generatore) g:

- Numero primo pubblico: $p = 23$
- Generatore pubblico: $g = 5$

Questi valori sono conosciuti da tutti e possono essere intercettati senza problemi.

Scelta delle chiavi private

Alice e Bob scelgono ciascuno una chiave privata segreta:

- Chiave privata di Alice: $a = 6$
- Chiave privata di Bob: $b = 15$

Calcolo delle chiavi pubbliche

Entrambi calcolano le rispettive chiavi pubbliche usando la formula:

$$X = g^a \mod p$$

- Alice calcola: $A = 5^6 \mod 23 = 8$
- Bob calcola: $B = 5^{15} \mod 23 = 19$

Ora Alice e Bob si scambiano pubblicamente A e B.

Calcolo della chiave segreta condivisa

Alice e Bob ora utilizzano il valore pubblico ricevuto per calcolare la chiave segreta condivisa:

- Alice calcola: $S = B^a \mod p = 19^6 \mod 23 = 2$

- Bob calcola: $S = A^b \mod p = 8^{15} \mod 23 = 2$

Entrambi arrivano alla stessa chiave segreta 2, che ora può essere usata per cifrare la comunicazione!

Considerazioni sulla Sicurezza

Un attaccante che intercetta i messaggi vede solo p, g, A e B, ma per calcolare S dovrebbe risolvere il problema del logaritmo discreto, che è computazionalmente difficile se i numeri sono sufficientemente grandi. Per questo motivo è fondamentale usare un numero che sia molto grande (migliaia di bit) e primo.

Diffie-Hellman protocol:

Man-in-the-middle attack:

Man-in-the-middle solution: