Sicurezza delle Reti e Crittografia

Concetti Fondamentali

Principi di Base

1. **Principio di Kerckhoff**
   - Algoritmi pubblici
   - Solo le chiavi devono essere segrete
   - Sicurezza per design, non per oscurità
   - Chiavi lunghe per aumentare complessità
2. **Ridondanza**
   - Necessaria in tutti i messaggi cifrati
   - Facilita verifica integrità
   - Supporta rilevazione manipolazioni
3. **Attualità**
   - Verifica freshness dei messaggi
   - Prevenzione replay attack
   - Timestamp o nonce

Crittografia Simmetrica

Caratteristiche Generali

- Stessa chiave per cifratura e decifratura
- Velocità di elaborazione elevata
- Problema distribuzione chiavi
- Necessità canale sicuro iniziale

Algoritmi Principali

1. DES (Data Encryption Standard)

- Struttura:
  - Blocchi da 64 bit
  - Chiave effettiva 56 bit
  - 19 passaggi totali
- Componenti:
  - P-Box: permutazioni bit
  - S-Box: sostituzioni non lineari

    - Funzioni della chiave per ogni round
- Limitazioni:
    - Chiave troppo corta per standard moderni
    - Vulnerabile a brute force
    - Obsoleto per applicazioni critiche

2. Triple DES

- Funzionamento:
    1. Cifratura con chiave K1
    2. Decifratura con chiave K2
    3. Cifratura finale con K1
- Caratteristiche:
    - Retrocompatibile con DES
    - Sicurezza aumentata
    - Performance ridotte
    - Chiave effettiva 112 bit

3. AES (Advanced Encryption Standard)

- Specifiche:
    - Blocchi da 128/256 bit
    - Chiavi da 128/256 bit
    - Standard dal 1997
- Vantaggi:
    - Sicurezza elevata
    - Prestazioni ottimizzate
    - Implementazione efficiente

Modalità Operative Cifrari a Blocchi

1. Electronic Code Book (ECB)

- Funzionamento:
    - Divisione in blocchi indipendenti
    - Cifratura separata di ogni blocco
    - Stessa chiave per tutti i blocchi
- Problemi:
    - Pattern riconoscibili
    - Vulnerabile a replay
    - No propagazione errori

2. Cipher Block Chaining (CBC)

- Meccanismo:
  - XOR con blocco cifrato precedente
  - IV per primo blocco
  - Concatenazione risultati
- Caratteristiche:
  - Maggiore sicurezza
  - Propagazione errori
  - Necessità IV casuale

3. Feedback Mode

- Utilizzo:
  - Cifratura byte a byte
  - Registro shift ausiliario
  - IV iniziale per registro
- Processo:
  1. Cifratura registro
  2. XOR con byte input
  3. Shift registro con output

4. Counter Mode (CTR)

- Funzionamento:
  - Cifratura contatore + IV
  - XOR risultato con plaintext
  - Incremento contatore
- Vantaggi:
  - Parallelizzabile
  - No propagazione errori
  - Accesso random ai blocchi

Crittografia Asimmetrica

Concetti Base

- Coppia chiavi: pubblica e privata
- Chiave pubblica per cifratura
- Chiave privata per decifratura
- Impossibilità pratica derivazione chiave privata

RSA (Rivest-Shamir-Adleman)

1. Generazione Chiavi

4. Scelta numeri primi p, q molto grandi
5. Calcolo n = p × q
6. Calcolo φ(n) = (p-1)(q-1)
7. Scelta e coprimo con φ(n)
8. Calcolo d tale che (e×d) mod φ(n) = 1

2. Processo di Cifratura

- Chiave pubblica: {e, n}
- Formula: C = M^e mod n
- M deve essere < n

3. Processo di Decifratura

- Chiave privata: {d, n}
- Formula: M = C^d mod n
- Basato su proprietà numeri primi

4. Sicurezza

- Basata su fattorizzazione numeri grandi
- Complessità computazionale
- Chiavi tipicamente 2048+ bit