

# CIFRARIO a CHIAVE SIMMETRICA

Il mittente e il destinatario condividono una chiave in comune, tutti i classici algoritmi sono a chiave simmetrica.

• CIFRARIO A FLUSSO: cifrario in cui la lunghezza del blocco è 1 bit o un bite.

• CIFRARIO A BLOCCHI: suddivide il messaggio in blocchi di lunghezza fissa e poi li crittografa un blocco alla volta.

In teoria necessita di una tabella di  $2^n$  voci per un blocco di  $n$  bit mentre la lunghezza della chiave è di  $n \cdot 2^n$

## PROPRIETÀ di SHANNON

Un algoritmo di ciphatura per essere considerato robusto deve avere queste due proprietà: (vengono dette reti S-P)

• CONFUSIONE

La relazione tra chiavi e testo cifrato deve essere meno correlata possibile, in modo che sia difficile ricavare la chiave partendo dal testo cifrato.

• DIFFUSIONE

La capacità di distribuire le correlazioni statistiche lungo tutto l'alfabeto, rendendo così difficile gli attacchi statistici.

• RETE di FEISTEL: È un algoritmo di cifratura a blocchi con una particolare struttura, esso infatti rispetta le proprietà di confusione e diffusione usando una serie di round multipli di una funzione di permutazione/diffusione P-BOX e una funzione di confusione/sostituzione S-BOX.

La crittografia e la decrittografia sono identiche, anche se nella decrittografia viene usata la chiave inversa.

---

## EFFETTO VALANGA

È una proprietà desiderabile per un buon algoritmo di crittografia, essa consiste nel causare il cambiamento di circa la metà dei bit di output, al cambiamento di un solo bit di input (chiavi o testo in chiaro).

## DES:

Algoritmo DES ha diverse fasi di diffusione e confusione, questo perché è formato da diversi round di rete di Feistel.

L'algoritmo DES ha un buon effetto valanga, ma anche se la chiave sembra abbastanza lunga a causa dei recenti progressi può essere vittima di attacchi a forza bruta, per questo motivo è considerato insicuro ed è consigliato usare 3DES il quale ha chiavi più lunghe.

### INPUT:

- testo in chiaro (block da 64)
- chiave a 56 bit ( $2^{56}$  chiavi)

### PASSI:

- suddivisione di ogni blocco in due sottoblocki da 32 bit
- schedulazione della chiave in 16 sottochiavi da 48 bit.
- 16 round tra i due sottoblocki e le sottochiavi mediante XOR, sostituzione e permutazioni (FEISTEL).

### OUTPUT:

- testo cifrato (block da 64).

L'algoritmo  $\text{DES}^{-1}$  applica gli stessi passi invertendo i due sottoblocki e usando le sottochiavi in ordine inverso.

# DISTRIBUZIONE delle CHIAVI

Gli schemi simmetrici necessitano della condivisione della chiave segreta comune, e questo ovviamente crea dei problemi nel distribuire le chiavi in modo sicuro, difatti spesso è questo a determinare il fallimento di un sistema sicuro.

L'unico metodo sicuro per distribuire le chiavi è fisicamente, oppure criptare con una chiave che è stata comunicata in precedenza fisicamente ed inviare la nuova.

## GERARCHIA di CHIAVI

- **CHIAVE SESSIONE:** usata per la crittografia dei dati per una sessione logica
- **CHIAVE MASTER:** usata per criptare le sessioni condivise dall'utente e dal centro di distribuzione chiavi.