# Confusione, Diffusione e Teorema di Shannon

## Concetti fondamentali della crittografia moderna

Prof. Fedeli Massimo - IIS Fermi Sacconi Cpia

# Il modello di un cifrario

Un sistema di cifratura classico può essere visto come una funzione:

$$C = E_K(P)$$

Dove:

- $P$ è il testo in chiaro (plaintext),
- $K$ è la chiave segreta,
- $C$ è il testo cifrato (ciphertext).

L'obiettivo è rendere difficile risalire a $P$ o a $K$ partendo da $C$.

# Il problema dell'analisi crittografica

Un attaccante cerca di sfruttare:

- regolarità del linguaggio,
- schemi ripetitivi,
- relazioni semplici tra testo in chiaro e testo cifrato.

La crittografia moderna mira a eliminare o mascherare queste debolezze.

# Esempio di analisi crittografica

Supponiamo di intercettare il seguwhile testo cifrato:

$$XQZZQXQZZQXQZZQ$$

Un attaccante può ipotizzare che:

- il messaggio contenga parole ripetute,
- il cifrario non elimini le ripetizioni,
- lettere uguali nel testo in chiaro producano lettere uguali nel testo cifrato.

Questo tipo di osservazione permette di formulare ipotesi sul testo originale o sulla chiave.
La crittografia moderna evita questi attacchi tramite confusione e diffusione.

# Confusione: idea intuitiva

La **confusione** ha lo scopo di:

> *Rendere complessa e non intuitiva la relazione tra la chiave segreta e il testo cifrato.*

In presenza di confusione, anche una piccola variazione della chiave produce un risultato apparentemente imprevedibile.

# Esempio di confusione

Supponiamo di cifrare una lettera usando una sostituzione dipendente dalla chiave:

- Chiave $= 3 \rightarrow CifrariodiCesareA \rightarrow D$
- B $\rightarrow E$

Se la chiave cambia (ad esempio 4 invece di 3), l'intero schema di sostituzione cambia.
La confusione aumenta quando la sostituzione è complessa e non lineare.

# Diffusione: idea intuitiva

La **diffusione** ha lo scopo di:

> *Distribuire l'informazione del testo in chiaro su molte parti del testo cifrato.*

In questo modo, una piccola modifica del messaggio originale produce molte modifiche nel testo cifrato.

# Esempio di diffusione

Consideriamo un messaggio binario:
[ P = 10100010 ]
Dopo una buona diffusione:

- ogni bit di $P$ influenza molti bit di $C$,
- non è possibile individuare direttamente la posizione dei bit originali.

Questo principio è noto come *effetto valanga*.

# Confusione e diffusione insieme

Un cifrario sicuro combina:

- confusione, per nascondere il ruolo della chiave,
- diffusione, per eliminare strutture e regolarità.

I moderni algoritmi a blocchi applicano questi principi in più cicli (round).

# Claude Shannon e la crittografia

Claude Shannon è considerato il padre della teoria dell'informazione.
Nel 1949 formulò i principi fondamentali della crittografia moderna, introducendo i concetti di confusione e diffusione.

# Il teorema di Shannon (idea di base)

Il teorema di Shannon afferma che:

> *La sicurezza di un sistema crittografico dipende esclusivamente dalla segretezza della chiave, non dall'algoritmo.*

Questo principio è noto come *Kerckhoffs-Shannon*.

# Conseguenze del teorema di Shannon

Da questo principio derivano alcune conseguenze importanti:

- l'algoritmo può essere pubblico,
- la chiave deve essere segreta e sufficientemente lunga,
- la sicurezza non deve basarsi sull'"oscurità" del metodo.

# Sicurezza perfetta

Shannon dimostrò che esiste una condizione di sicurezza perfetta:

*Il testo cifrato non fornisce alcuna informazione sul testo in chiaro.*

Un esempio teorico è il *one-time pad*, in cui:

- la chiave è lunga quanto il messaggio,
- la chiave è casuale,
- la chiave è usata una sola volta.

# Limiti pratici

Sebbene la sicurezza perfetta sia teoricamente possibile, nella pratica:

- la gestione delle chiavi è complessa,
- si preferiscono sistemi computazionalmente sicuri,
- confusione e diffusione diventano fondamentali.

# Riepilogo finale

- La confusione nasconde il ruolo della chiave.
- La diffusione elimina le strutture del messaggio.
- Il teorema di Shannon stabilisce le basi teoriche della crittografia moderna.

Questi concetti sono alla base di tutti i sistemi crittografici utilizzati oggi.