Confusione, Diffusione e Teorema di ShannonConcetti
fondamentali della crittografia moderna

Prof. Fedeli Massimo IIS Fermi Sacconi CPIA

1 Introduzione

La crittografia è la disciplina che studia i metodi per proteggere le informazioni da accessi non autorizzati. I sistemi crittografici moderni si basano su solidi principi matematici e teorici, tra cui spiccano i concetti di confusione, diffusione e il teorema di Shannon.

2 Il modello di un cifrario

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

$$C = E_K(P)$$

Dove:

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

L'obiettivo della cifratura è rendere computazionalmente difficile risalire al testo in chiaro P o alla chiave K partendo dal solo testo cifrato C.

3 Il problema dell'analisi crittografica

Un attaccante che tenta di violare un sistema crittografico cerca di sfruttare:

- le regolarità del linguaggio naturale,
- la presenza di schemi ripetitivi,
- relazioni semplici tra testo in chiaro e testo cifrato.

La crittografia moderna nasce proprio con l'obiettivo di eliminare o mascherare queste debolezze strutturali.

4 Esempio di analisi crittografica

Supponiamo di intercettare il seguente testo cifrato:

[`XQZZQ XQZZQ XQZZQ`]

Un attaccante può ipotizzare che il messaggio originale contenga parole ripetute e che il cifrario utilizzato non sia in grado di nascondere tali ripetizioni. In questo caso, lettere uguali nel testo in chiaro producono lettere uguali nel testo cifrato, rendendo possibile formulare ipotesi sul messaggio originale o sulla chiave.

La crittografia moderna contrasta questi attacchi attraverso l'uso sistematico di confusione e diffusione.

5 Confusione

La **confusione** ha lo scopo di rendere complessa e non intuitiva la relazione tra la chiave segreta e il testo cifrato. In presenza di un alto livello di confusione, anche una piccola variazione della chiave produce un risultato apparentemente imprevedibile.

5.1 Esempio di confusione

Un esempio semplice è il cifrario di Cesare, in cui la sostituzione delle lettere dipende da una chiave numerica. Se la chiave è pari a 3, la lettera A viene cifrata come D e la B come E. Cambiando la chiave, l'intero schema di sostituzione cambia. Nei cifrari moderni, la confusione è ottenuta tramite operazioni non lineari molto più complesse.

6 Diffusione

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.

6.1 Esempio di diffusione

Consideriamo un messaggio binario: [P = 10100010]

Dopo un'efficace operazione di diffusione, ogni bit del messaggio originale influenza molti bit del testo cifrato. Questo fenomeno è noto come *effetto valanga*.

7 Confusione e diffusione nei cifrari moderni

Un cifrario sicuro combina sistematicamente confusione e diffusione. Gli algoritmi crittografici moderni, come i cifrari a blocchi, applicano questi principi in più cicli successivi, detti round, aumentando progressivamente la sicurezza.

8 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 formalmente i concetti di confusione e diffusione.

9 Il teorema di Shannon

Il teorema di Shannon afferma che la sicurezza di un sistema crittografico deve dipendere esclusivamente dalla segretezza della chiave e non dalla segretezza dell'algoritmo. Questo principio è noto come principio di Kerckhoffs-Shannon.

9.1 Conseguenze

Da questo principio derivano alcune conseguenze fondamentali:

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

10 Sicurezza perfetta

Shannon dimostrò che esiste una condizione di sicurezza perfetta, in cui il testo cifrato non fornisce alcuna informazione sul testo in chiaro. Un esempio teorico è il *one-time pad*, nel quale la chiave è casuale, lunga quanto il messaggio e utilizzata una sola volta.

11 Limiti pratici

Nonostante la sicurezza perfetta sia teoricamente possibile, nella pratica la gestione delle chiavi risulta complessa. Per questo motivo si preferiscono sistemi computazionalmente sicuri, nei quali confusione e diffusione giocano un ruolo centrale.

12 Conclusione

I concetti di confusione, diffusione e il teorema di Shannon costituiscono le fondamenta teoriche della crittografia moderna e sono alla base dei sistemi di sicurezza utilizzati quotidianamente nelle comunicazioni digitali.