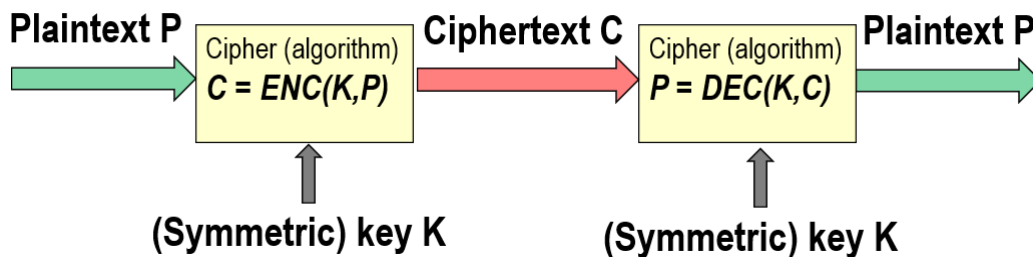


Crittografia Simmetrica, Generatori di Numeri Pseudocasuali e Sicurezza

Introduzione

La crittografia è fondamentale per garantire la **riservatezza dei dati**: il suo scopo è trasformare le informazioni in modo che risultino incomprensibili a chi non possiede le necessarie autorizzazioni. Un requisito chiave è che tale trasformazione sia reversibile, solo dal legittimo possessore della chiave.



Crittografia Simmetrica: Concetti di Base

Nel *sistema simmetrico*, la stessa chiave viene usata sia per cifrare che per decifrare il messaggio. La sicurezza di questi sistemi non risiede nell'algoritmo — che deve essere pubblico — ma nella segretezza della chiave. Solo chi conosce la chiave deve essere in grado di effettuare le operazioni di cifratura e decifratura.

- **Algoritmo di cifratura:** dato un testo in chiaro P e una chiave segreta K , produce il testo cifrato $C = Enc_K(P)$
- **Algoritmo di decifratura:** dato C e la stessa chiave K , si ottiene il testo originale $P = Dec_K(C)$

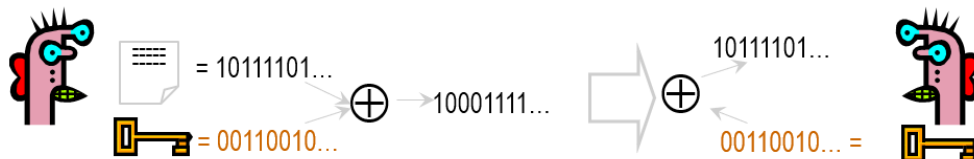
Limiti dei Cifrari Semplici: Analisi di Frequenza

Cifrari classici come la sostituzione semplice sono vulnerabili all'analisi di frequenza: se una lettera viene cifrata sempre con lo stesso simbolo, la frequenza delle lettere cifrate riflette quella del testo originale. Gli attaccanti possono quindi sfruttare questa proprietà per risalire alla chiave.

Esempio di Cifrario a Sostituzione

Viene proposto un esempio pratico in cui un testo italiano viene cifrato con sostituzione lettera per lettera. L'analisi delle frequenze delle lettere cifrate consente spesso di decifrarlo, soprattutto conoscendo le caratteristiche statistiche della lingua italiana, come la frequenza delle vocali e delle consonanti.

Cifrari Perfetti: One Time Pad (Vernam)





$$CT = ENC(K, M) = M \oplus K$$

$$M = DEC(K, CT) = CT \oplus K$$

Il cifrario di Vernam, o One Time Pad, rappresenta un caso teoricamente perfetto:

- La chiave è una sequenza di bit totalmente casuale, lunga quanto il messaggio.
- Ogni bit del testo in chiaro viene combinato (XOR) con il corrispondente della chiave.
- La sicurezza è “incondizionata”: anche un attaccante con mezzi infiniti non può risalire al messaggio senza la chiave.

	\oplus			
Secret bit		Random bit		
Probability: 0=p 1=(1-p)		Probability: 0=1/2 1=1/2		
Secret bit	Random bit	XOR result bit		
0	0	0		p/2
0	1	1		p/2
1	0	1		(1-p)/2
1	1	0		(1-p)/2

Tuttavia, questa soluzione presenta limiti pratici insormontabili:

- La chiave deve essere lunga quanto il messaggio.
- Non deve essere mai riutilizzata: il riuso facilita attacchi banali.
- Nessuna integrità: un attaccante può modificare il testo cifrato e il destinatario decifrerà un messaggio alterato.

Numeri Casuali e Pseudo-Casuali in Crittografia

PRNG - Pseudo-Random Number Generator

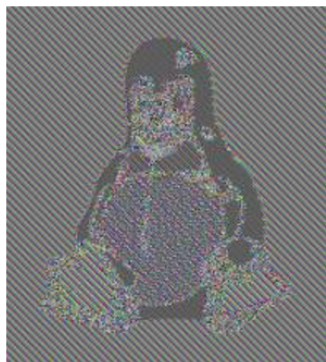
Per motivi pratici, si usano generatori di numeri pseudo-casuali (PRNG): algoritmi che producono sequenze di bit “sembra” casuali a partire da un piccolo seme segreto. Tuttavia, la sicurezza dipende da tre proprietà fondamentali:

- **Proprietà statistiche:** la sequenza prodotta deve “sembrare” casuale.
- **Imprevedibilità:** dato un pezzo della sequenza, non si deve riuscire a predire il successivo.
- **Periodo:** la sequenza non deve ripetersi su scale ragionevoli.

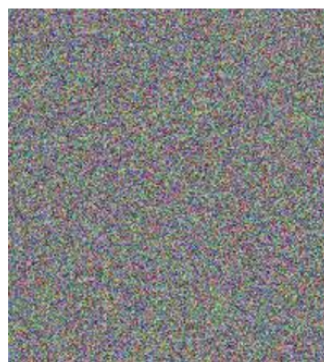
In crittografia tutte e tre devono essere garantite. Un generatore debole mette a rischio l'intero sistema. I veri generatori casuali hardware (*TRNG* — *True Random Number Generator*), basandosi su fenomeni fisici (rumore termico, radioattivo, ecc.), producono sequenze realmente imprevedibili, ma sono più costosi e meno diffusi.

Sicurezza Formale: Che cosa significa “sicuro”?

Le definizioni informali (*un cifrario è sicuro se nasconde i messaggi oppure trasforma ogni byte dell'originale in uno diverso*) sono spesso fuorvianti. Serve una definizione rigorosa: il cifrario deve resistere anche se l'attaccante sceglie liberamente i messaggi da cifrare e osserva i corrispondenti cifrati (cosiddetto attacco chosen plaintext, IND-CPA).



Substitution Cipher



Semantically secure Cipher

Definizione di Sicurezza IND-CPA

Un cifrario è semanticamente sicuro (IND-CPA) se, dato un cifrato ottenuto scegliendo casualmente tra due messaggi (noti all'attaccante), l'attaccante non ha alcun vantaggio rispetto a una scelta casuale nel determinare quale dei due sia stato cifrato. Conseguenze fondamentali:

- La cifratura deve essere randomizzata: lo stesso messaggio deve cifrarsi sempre in modo diverso.
- Se una sequenza si ripete, la sua versione cifrata deve essere differente ogni volta.

Conclusione

La sicurezza dei sistemi di cifratura si basa sull'impossibilità pratica, dimostrabile matematicamente, di violare la riservatezza dei messaggi anche in presenza di attacchi sofisticati. Fondamentale è l'uso corretto di strumenti matematici e algoritmici adeguati, e la gestione sicura delle chiavi e dei generatori di numeri casuali.