

Un canale per essere affidabile deve rispettare queste 3 proprietà.

RISERVATEZZA: Le informazioni trasmesse rimangono segrete

INTEGRITÀ: Le informazioni non vengono alterate.

AUTENTICAZIONE: I committenti sanno con chi stanno parlando.

La sicurezza deve dipendere sempre dalla segretezza della chiave e mai dall'algoritmo, la crittografia e la decrittografia devono essere semplici se le chiavi sono note.

SICUREZZA INCONDIZIONATA: Il sistema è sicuro anche se l'avversario ha una potenza di calcolo illimitata, essa si misura con la teoria della informazione.

SICUREZZA CONDIZIONATA: Il sistema può essere violato in linea di principio, ma ciò richiede una potenza di calcolo irrealistica, essa si misura con la teoria della complessità.

CRITTOANALISI: Scienza del recupero del testo in chiaro e la chiave a partire dal testo cifrato.

Due tipologie di attacchi:

• **FORZA BRUTA**.

È sempre possibile, basta provare ogni chiave esistente, il suo costo dipende ovviamente dalla lunghezza della chiave.

• **CRITTOANALITICO**

Un sistema è sicuro se un qualsiasi avversario ha la probabilità di vincere trascurabile.

CIFRARI a SOSTITUZIONE

Si sostituiscono i caratteri con altri caratteri

- CIFRARIO DI CESARE: Ogni lettera viene traslata di 3 lettere rispetto l'alfabeto, è molto facile da rompere anche senza utilizzare complicate analisi di frequenza.
- CIFRARIO MONOALFABETICO: Generalizzazione cifrario di Cesare con 26!

LIMITE dei CIFRARI a SOSTITUZIONE

Analisi della frequenza, tutte le lettere hanno una frequenza diversa, è quindi facile ricostruire una frase in base alle frequenze delle lettere cibrate, questo è molto difficile con testi lunghi ed atipici.

CIFRARIO a CHIAVE SIMMETRICA

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

- CIFRARIO A BLOCCHI: suddivide il messaggio in blocchi di lunghezza fissa e poi li crittografa un blocco alla volta.
- CIFRARIO A FLUSSO: cifrario in cui la lunghezza del blocco è 0.
- FEISTEL: