Nozioni di sicurezza

Codici vs Cifrari

- In un codice, le parole o alcune combinazioni di simboli sono sostituite da parole chiave

  Esempi: 03680C → *delivered to*
  36276C → *delivered by*
  50302C → *sent from*

- I codici non consentono l'uso di parole inaspettate.

- Un cifrario non tiene conto delle strutture linguistiche del messaggio.

- Un cifrario cripta ogni stringa significativa o non significativa con un qualche algoritmo

Nozioni di sicurezza

- La crittografia risponde al paradigma della **sicurezza computazionale**
- Con essa si intende che, senza la conoscenza del segreto (chiave), la decifratura richiede uno sforzo computazionale (**work factor**) che supera le capacità dell'attaccante
- Si parla di ***provable security*** quando si può dimostrare che decifrare in assenza del segreto equivale a risolvere un particolare problema matematico provatamente difficile
- Tale approccio si contrappone alla ***unconditional security*** (o *information-theoretic security*) che basa la sicurezza su argomenti statistici, senza fare alcuna ipotesi sulle capacità computazionali dell'attaccante

Livello di sicurezza

- Per stimare il livello di **computational security** supponiamo che l'attaccante scelga il miglior algoritmo di attacco possibile
- Il numero di operazioni binarie richieste in media dall'algoritmo per terminare con successo si definisce **work factor**, ed è direttamente proporzionale al tempo di attacco
- Il livello di sicurezza è definito come il **minimo work factor per un attaccante**
- L'algoritmo di attacco più ovvio e sempre praticabile consiste nel tentare di scoprire il segreto enumerando tutte le possibilità: **attacco a forza bruta**
- **Esempio**: chiave lunga 16 bit $\rightarrow$ ci sono 2^{16} chiavi possibili
  chiave lunga 56 bit $\rightarrow$ ci sono $2^{56} \approx 7.2 \cdot 10^{16}$ chiavi possibili

Lunghezza della chiave

- **Esempio**: $D = 10^{30}$ possibili chiavi
  eseguendo 10^9 calcoli/secondo
  occorrono $3 \cdot 10^{13}$ anni per completare la ricerca

- Tuttavia l'attacco a forza bruta fornisce solo un **limite superiore** al livello di sicurezza, perché spesso esistono algoritmi di attacco più efficienti.

- Ad esempio, il **paradosso del compleanno** stabilisce che con un numero di tentativi $\approx D^{1/2}$ la probabilità di trovare la chiave corretta è > 1/2

- La maggior parte dei cifrari possono essere attaccati con tecniche diverse dalla forza bruta oppure non usano efficientemente i bit della chiave

- Due algoritmi con chiavi di uguale lunghezza possono avere livelli di sicurezza diversi

- Ad esempio, il *cifrario a sostituzione* ha $26! = 4 \cdot 10^{26}$ possibili chiavi, eppure è uno dei cifrari più semplici da attaccare

Lunghezza della chiave (cont.)

- Il fatto che un algoritmo sia sicuro oggi non comporta necessariamente che lo sarà anche in futuro
- Si deve sempre tener conto:
  - delle debolezze causate da implementazioni scadenti
  - dei progressi tecnologici (aumento delle capacità di calcolo)
  - Ad esempio, DES ha resistito **20 anni** prima di essere attaccato con successo da un computer parallelo ben progettato
- La continua ricerca nell'ambito del **quantum computing** modificherà radicalmente le basi dei futuri algoritmi crittografici
- Ad esempio, il cifrario asimmetrico **RSA**, basato sulla fattorizzazione di numeri interi molto grandi ed oggi molto usato, è suscettibile ad attacchi basati su computer quantistici

Ulteriori aspetti

- Matematicamente è possibile aumentare la sicurezza incrementando (anche di poco) la lunghezza della chiave ma, in pratica, ciò non sempre è possibile.
- Se un microchip gestisce parole di 64 bit, per aumentare la lunghezza della chiave da 64 a 65 bit può essere necessario riprogettare l'hardware, che è un'operazione costosa.
- Il progetto di un buon crittosistema deve basarsi su considerazioni sia matematiche che ingegneristiche.

Requisiti di un sistema crittografico

- **Riservatezza (Confidenzialità)**: solo il ricevitore autorizzato deve essere in grado di decifrare il messaggio
- **Autenticazione**: il ricevitore deve essere certo dell'origine del messaggio, l'identità di chi lo ha inviato deve essere certificata
- **Integrità**: il messaggio non deve essere stato in alcun modo modificato durante la trasmissione
- **Non ripudiabilità**: né il mittente né il destinatario possono negare di avere, rispettivamente, inviato e ricevuto il messaggio