One-Time Pad

Cifrario perfetto.

messaggio $m \in \{0,1\}^n$;

chiave $k \in \{0,1\}^n$, cambiata per ogni messaggio;

cifratura $c = m \oplus k$;

decifrazione $m = c \oplus k$.

Scambio delle chiavi

Le chiavi sono molto lunghe, e scambiarle è un problema. Possibilità:

- gli utenti si scambiano il seed di un generatore (problema: il crittoanalista può sferrare un attacco sul seed, e le chiavi generate avranno un periodo);
- utilizzare un file accessibile ad entrambi (anche pubblico);
- quantum key distribution.

Dimostrazione

Ipotesi:

- tutti i messaggi hanno lunghezza n, altrimenti aggiungiamo padding o dividiamo in blocchi lunghi n;
- tutte le sequenze di n bit sono messaggi possibili – si assegna una probabilità molto bassa ma > 0 alle sequenze prive di significato (ogni tanto vanno inviate anche se non significano niente);
- la chiave è scelta a caso per ogni messaggio

One-Time Pad è perfetto e usa un numero minimale di chiavi.

minimale per il teorema di Shannon $N_m \leq N_k$, e qui $N_m = N_k$;

perfetto mostriamo che $P(M = m \mid C = c) = P(M = m)$.

Fissato m, chiavi diverse producono crittogrammi diversi, quindi $\exists! k$ chiave che porta m in un certo crittogramma c.

$P(C = c) =$ probabilità di scegliere a caso l'unica k che porta m in $c = \frac{1}{2^n}$ – non dipende da m.

$$\begin{aligned} P(M = m \mid C = c) &= \frac{P(M = m \cap C = c)}{P(C = c)} \\ &= \frac{P(M = m)P(C = c)}{P(C = c)} \quad (M = m \text{ e } C = c \text{ indipendenti}) \\ &= P(M = m). \end{aligned}$$

Rimuovendo la seconda ipotesi: in inglese α^n sequenze significative, con $\alpha \simeq 1.1$ $N_k \geq N_m = \alpha^n < 2^n$, quindi possiamo descrivere le chiavi con $t < n$ bit.

$$2^t \geq \alpha^n \iff t \geq n \log_2 \alpha \simeq 0.12n$$

quindi ci serve solo un decimo dei bit per la chiave. Tuttavia torna ad essere possibile un attacco brute-force. È opportuno fare in modo che ci siano molte coppie distinte (m, k) che producono lo stesso crittogramma:

$$\#\text{coppie } (m,k) \gg \#\text{crittogrammi}$$

Usando chiavi di t bit casuali:

$$\alpha^n 2^t \gg 2^n \implies n \log_2 \alpha + t \gg n$$

$$\implies t \gg n - n \log_2 \alpha \simeq n(1 - 0.12) = 0.88n$$

quindi non il risparmio sulla dimensione della chiave è minimo se vogliamo essere resistenti ad attacchi esaustivi.