One-time Pad

Paolo D'Arco
pdarco@unisa.it

Università di Salerno

Elementi di Crittografia

Contenuti

Esempio

Esempio 2.7. Il cifrario di Vigenere, per certi parametri, non è perfettamente indistinguibile.

Consideriamo un cifrario di Vigenere per uno spazio di messaggi M di stringhe di due caratteri, ed in cui la lunghezza della chiave (periodo) è scelta uniformemente in $\{1, 2\}$.

Mostreremo un Adv A per cui $Pr[PrivK^{eav}_{A,\Pi} = 1] > \frac{1}{2}$.

Adv A

1. Costruisce $m_0 = aa$ ed $m_1 = ab$ e li dà a C
2. Dopo aver ricevuto dal challenger C il cifrato $c = c_1 c_2$
    - se $c_1 = c_2$ dà in output $b' = 0$;
    - altrimenti, dà in output $b' = 1$.

Esempio

Calcoliamo la probabilità di successo di **A**.

$$
\begin{aligned}
Pr[PrivK^{eav}_{A,\Pi} = 1] &= \frac{1}{2} \cdot Pr[PrivK^{eav}_{A,\Pi} = 1 | b = 0] + \frac{1}{2} \cdot Pr[PrivK^{eav}_{A,\Pi} = 1 | b = 1] \\
&= \frac{1}{2} \cdot Pr[A \text{ dà } 0 | b = 0] + \frac{1}{2} \cdot Pr[A \text{ dà } 1 | b = 1]
\end{aligned}
$$

Valutiamo i due termini separatamente:

$Pr[A \text{ dà } 0 | b = 0]$ solo se

- viene scelta una chiave di lunghezza 1 (prob. $\frac{1}{2}$)
- viene scelta una chiave di lunghezza 2 (prob. $\frac{1}{2}$) con due valori uguali (prob. $\frac{1}{26}$)

Pertanto,

$$Pr[A \text{ dà } 0 | b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26} \approx 0.52.$$

Esempio

D'altra parte, poichè $Pr[A \text{ dà } 0|b = 1]$ solo se

- viene scelta una chiave di lunghezza 2 (prob. $\frac{1}{2}$) ed il primo valore vale uno più del secondo (prob. $\frac{1}{26}$)

Pertanto,

$$Pr[A \text{ dà } 1|b = 1] \quad = \quad 1 - Pr[A \text{ dà } 0|b = 1] = 1 - \frac{1}{2} \cdot \frac{1}{26} \approx 0.98.$$

Mettendo assieme le varie parti, risulta

$$\begin{aligned} Pr[PrivK^{eav}_{A,\Pi} = 1] &= \frac{1}{2} \cdot (\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}) + \frac{1}{2} \cdot (1 - \frac{1}{2} \cdot \frac{1}{26}) \\ &= \frac{1}{2} \cdot (\frac{1}{2} + 1) = \frac{3}{4} = 0.75 > 0.5 = \frac{1}{2} \end{aligned}$$

Quindi, lo schema **non** è perfettamente indistinguibile.

One-time Pad

Brevettato da Vernam nel 1917. Circa 25 anni più tardi Shannon dimostrò che è perfettamente segreto.

Costruzione 2.8

Sia $\ell > 0$ un intero. Siano $M = K = C = \{0,1\}^\ell$.

- Gen: sceglie $k \in \{0,1\}^\ell$ *uniformemente* a caso
- Enc: dati $k \in \{0,1\}^\ell$ ed $m \in \{0,1\}^\ell$, dà in output il cifrato

$$c := k \oplus m$$

- Dec: dati $k \in \{0,1\}^\ell$ e $c \in \{0,1\}^\ell$, dà in output il messaggio

$$m := k \oplus c$$

È facile verificare che:

$$\forall k, \forall m \text{ risulta } Dec_k(Enc_k(m)) = (k \oplus (k \oplus m)) = m.$$

One-time Pad

Teorema 2.9. Lo schema di cifratura one-time pad è perfettamente segreto.

Dim. Prima di tutto, calcoliamo $Pr[\mathsf{C} = c | \mathsf{M} = m']$ per un arbitrario $c \in C$ ed $m' \in M$. Risulta:

$$\begin{aligned} Pr[\mathsf{C} = c | \mathsf{M} = m'] &= Pr[Enc_{\mathsf{K}}(m') = c] \\ &= Pr[m' \oplus \mathsf{K} = c] \\ &= Pr[\mathsf{K} = m' \oplus c] = 2^{-\ell}, \end{aligned}$$

poichè k è una chiave scelta uniformemente a caso in $\{0,1\}^{\ell}$.
Per ogni $c \in C$, abbiamo:

$$\begin{aligned} Pr[\mathsf{C} = c] &= \sum_{m' \in M} Pr[\mathsf{C} = c | \mathsf{M} = m'] \cdot Pr[\mathsf{M} = m'] \\ &= \sum_{m' \in M} 2^{-\ell} \cdot Pr[\mathsf{M} = m'] = 2^{-\ell} \cdot \sum_{m' \in M} Pr[\mathsf{M} = m'] \\ &= 2^{-\ell} \cdot 1 = 2^{-\ell}, \end{aligned}$$

One-time Pad

dove la somma è calcolata su tutti gli $m' \in M$ tali che $Pr[\mathsf{M} = m'] > 0$.

Applicando allora il Teorema di Bayes, otteniamo:

$$\begin{aligned} Pr[\mathsf{M} = m | \mathsf{C} = c] &= \frac{Pr[\mathsf{C} = c | \mathsf{M} = m] \cdot Pr[\mathsf{M} = m]}{Pr[\mathsf{C} = c]} \\ &= \frac{2^{-\ell} \cdot Pr[\mathsf{M} = m]}{2^{-\ell}} \\ &= Pr[\mathsf{M} = m]. \end{aligned}$$

Pertanto, lo schema di cifratura one-time pad è perfettamente segreto.

Limitazioni della segretezza perfetta

Si noti che, nello schema one-time pad

- la chiave è **tanto lunga quanto il messaggio** che si intende cifrare
- è sicuro per **un uso soltanto**
  - per esempio, dati $c = m \oplus k$ e $c' = m' \oplus k$, risulta

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m',$$

    ovvero un Adv può calcolare la differenza tra i due messaggi (molta informazione)!

- L'esempio è sufficiente per dire che il one-time pad **non** è perfettamente segreto per qualsiasi nozione di segretezza perfetta per messaggi multipli.

Purtroppo i limiti del one-time pad sono limiti *intrinseci* alla segretezza perfetta.

Limitazioni della segretezza perfetta

Faremo vedere che ogni schema perfettamente segreto deve avere uno spazio delle chiavi *almeno* tanto grande quanto lo spazio dei messaggi.

Da cui, discende che :

- se in uno schema perfettamente segreto tutte le chiavi sono della stessa lunghezza
- e se lo spazio dei messaggi consiste di tutte le stringhe di una data lunghezza

$$\Downarrow$$

la chiave è almeno tanto lunga quanto il messaggio

$$\Downarrow$$

lo schema di cifratura one-time pad è ottimale rispetto alla lunghezza della chiave.

Teorema 2.10. Se (Gen, Enc, Dec) è uno schema di cifratura perfettamente segreto con spazio dei messaggi M e spazio delle chiavi K, allora

$$|K| \geq |M|.$$

Dim. Mostriamo che, se fosse $|K| < |M|$, lo schema non potrebbe essere perfettamente segreto.

Sia $|K| < |M|$. Sia M *distribuita uniformemente* e sia $c \in C$ tale che $Pr[\mathrm{C} = c] > 0$. Definiamo

$$M(c) \stackrel{def}{=} \{m | m = Dec_k(c), \text{ per qualche } k \in K\}.$$

Chiaramente $|M(c)| \leq |K|$. Se $|K| < |M|$, allora $\exists m' \in M$ tale che $m' \notin M(c)$. Ma allora risulta:

$$Pr[\mathrm{M} = m' | \mathrm{C} = c] = 0 \neq Pr[\mathrm{M} = m'] = \frac{1}{|M|}.$$

Pertanto lo schema non è perfettamente segreto. Quindi deve essere $|K| \geq |M|$.

È uno strumento utile per provare la segretezza perfetta di uno schema di cifratura.

Teorema 2.11. Sia (Gen, Enc, Dec) uno schema di cifratura con spazio dei messaggi M per cui $|M| = |K| = |C|$. Lo schema è perfettamente segreto **se e solo se**:

1. Gen sceglie ogni chiave $k \in K$ con probabilità uguale a $\frac{1}{|K|}$
2. per ogni $m \in M$ ed ogni $c \in C$, esiste un'unica chiave $k \in K$ tale che $Enc_k(m) = c$.

Dim. Si consulti il libro di testo.

Domande

Relativamente alla segretezza perfetta, che cosa possiamo dire di:

1. uno shift cipher usato per cifrare un messaggio di *un solo* carattere?
2. un cifrario di Vigenere di periodo t per cifrare *un solo* messaggio di lunghezza t?
3. un one-time pad in cui, invece dell' xor (che è una somma mod 2 sulle cifre 0 e 1), il messaggio è una sequenza di cifre decimali, la chiave è una sequenza di cifre decimali tanto lunga quanto il messaggio e l'operazione è la somma mod 10?
4. un one-time pad in cui messaggio e chiave sono della stessa lunghezza, sono costituiti di caratteri appartenenti ad un alfabeto di taglia m e l'operazione è la somma modulo m?