Digital Signature Algorithm

Mattia Biral

2024-03-09

1 Introduzione

Il **Digital Signature Algorithm** è un sistema crittografico a chiave pubblica e uno *standard federale per l'elaborazione delle informazioni* La chiave privata è utilizzata per generare la firma, mentre la chiave pubblica per verificarla.
E' basato sul problema matematico del logaritmo discreto.

1.1 Firma digitale

La firma digitale fornisce:

- Autenticazione: so chi ha inviato il messaggio
- Integrità: so che il documento non è stato modificato dopo la firma
- Non-ripudio: l'autore non può dire di non essere stato lui a firmare (side-effect dell'autenticazione)

1.2 Operazioni

DSA si svolge in quattro operazioni:

- Generazione delle chiavi
- Distribuzione delle chiavi
- Firma
- Verifica della firma

2 Algoritmo

2.1 Generazione delle chiavi

2.1.1 Parametri

I parametri dell'algoritmo sono (p, q, g)

- H funzione crittografica di hash di lunghezza $|H|$ bit (se $|H|$ è maggiore della lunghezza del modulo N solo gli N bit più significativi dell'output saranno utilizzati)
- L lunghezza della chiave
- N lunghezza del modulo tale che $N < L \wedge N \leq |H|$
- q primo di N bit
- p primo di L bit tale che $q \mid p - 1$
- h casuale in $\{2, ..., p-2\} = F_p^* - \{1, p-1\}$
- $g := h^{p-1/q} \mod p$ (se $g = 1$ è necessario generare un nuovo h)