

Checksum

Rossi Andrea – 5AS



Struttura della presentazione

1. Introduzione al checksum
2. Esempi di algoritmi:
 - a. Checksum semplice
 - b. CRC
3. Funzioni di hash
 - a. MDx
 - b. SHA
4. SHAttered



Cos'è il *checksum*?

Piccola introduzione

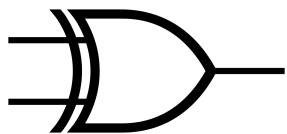
- In italiano, “somma di controllo”
- Parte dell’header di un pacchetto
- Sequenza di bit per verificare l’integrità di un pacchetto che potrebbe essersi alterato durante la trasmissione
- Utilizzato per i download su internet per controllare che un file non sia stato manomesso
- Meno *collisioni* ci sono, migliore è l’algoritmo



Esempio

Checksum semplice

- Le parti si mettono d'accordo su un *generatore*
- Il mittente fa la somma dei numeri e lo divide per il generatore e invia il messaggio con il resto della divisione
- Il destinatario riceve il messaggio e fa gli stessi calcoli
- Se il resto risulta uguale a quello che ha ricevuto, probabilmente il messaggio è corretto



Esempio

CRC: Cyclic Redundancy Check

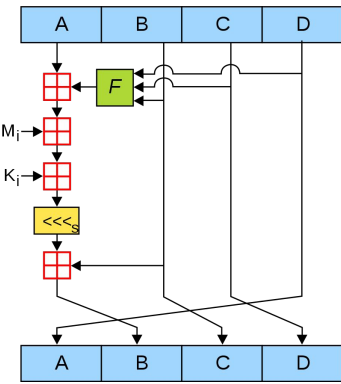
- Controllo a ridondanza ciclica: i dati di uscita sono ottenuti elaborando i dati di ingresso che vengono fatti scorrere ciclicamente in una rete logica
- Algoritmo per rilevare gli errori, non correggerli
- Inefficace per verificare la correttezza dei dati in caso di manomissione intenzionale



Funzioni di hash

Crittografia

- Funzioni matematiche che hanno come argomento dati di lunghezza arbitraria e li “trasformano” in stringhe univoche dalle quali non si può risalire ai dati originali
- Vengono usate su internet per verificare che un file non sia stato manomesso o non si sia corrotto
- Il cambiamento, anche minimo, di qualsiasi parte del dato comporta un risultato completamente diverso



MDx

Message-Digest

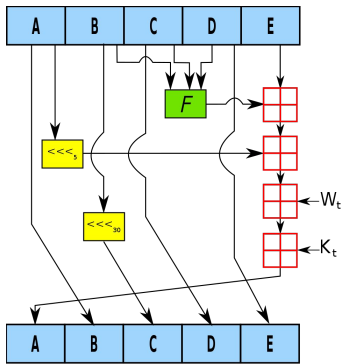
Serie di funzioni crittografiche di hash composta da MD4, MD5 e MD6

La stringa “Ciao” ad esempio diventa con MD5:

16272a5dd83c63010e9f67977940e871

La stringa “ciao” sempre con MD5:

6e6bc4e49dd477ebc98ef4046c067b5f



SHA

Secure Hashing Algorithm

SHA è una famiglia di funzioni crittografiche di hash, dove le più conosciute sono SHA-1, SHA-256 e SHA-512

Funzioni sviluppate dall'NSA a partire dal 1993

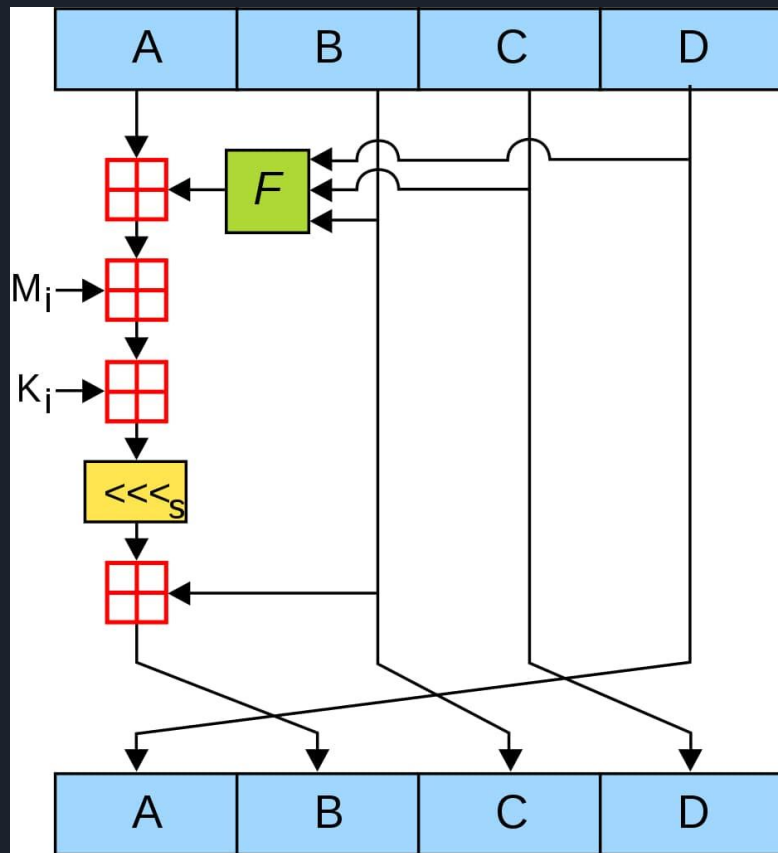
La stringa "Ciao" ad esempio diventa con SHA-1:

a810368ec47867e1c68e2d02a9293a2c04cd314c

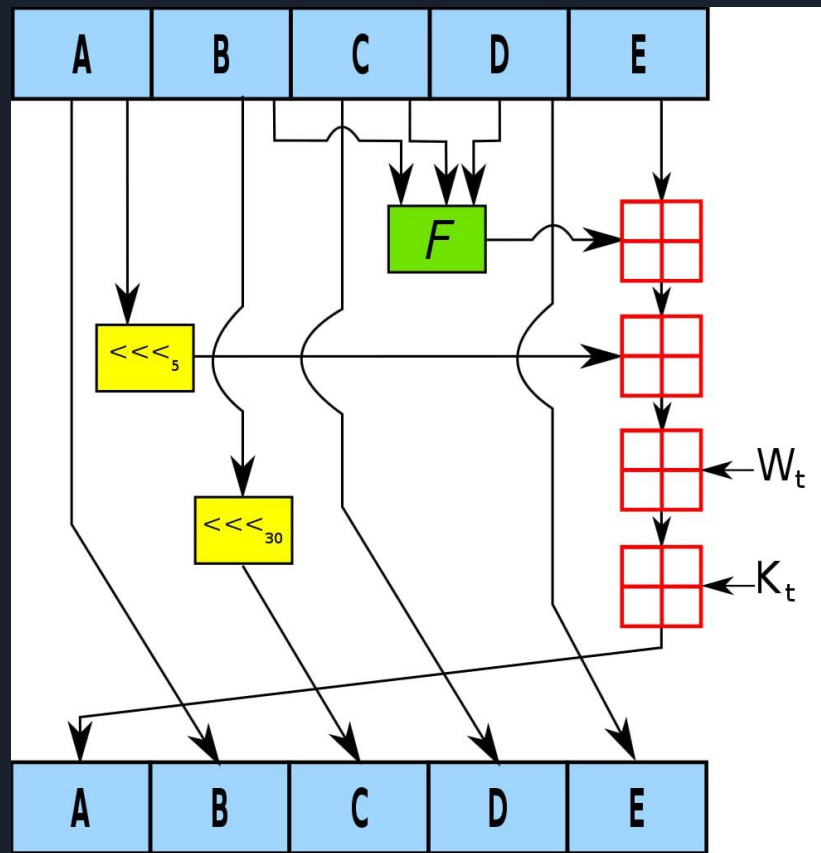
La stringa "ciao" sempre con SHA-1:

1e4e888ac66f8dd41e00c5a7ac36a32a9950d271

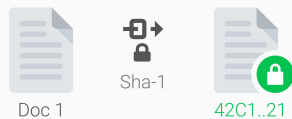
MD5



SHA-1



Expected behavior: **different** hashes



SHAttered

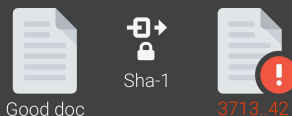
Dimostrazione che SHA-1 non è più un algoritmo sicuro

9.223.372.036.854.775.808 hash SHA-1 calcolati

6.500 anni di computazioni con una sola CPU

110 anni di computazioni con una sola GPU

Collision attack: **same** hashes



Expected behavior: **different** hashes



Doc 1



Sha-1



42C1..21



Doc 2



Sha-1



3E2A..AE

Collision attack: **same** hashes



Good doc



Sha-1



3713..42



Bad doc



Sha-1



3713..42

SHattered

The first concrete collision attack against SHA-1
<https://shattered.io>



Marc Stevens
Pierre Karpman



Elie Bursztein
Ange Albertini
Yarik Markov

SHattered

The first concrete collision attack against SHA-1
<https://shattered.io>



Marc Stevens
Pierre Karpman



Elie Bursztein
Ange Albertini
Yarik Markov

```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 2.pdf
```

```
└─ /tmp/sha1
└─ sha256sum *.pdf
```

```
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf
```

0.64G 8-11h

Fine

Grazie per l'attenzione