Funzioni hash con OpenSSL

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

http://www.dia.unisa.it/professori/ads

Aprile 2017

Funzioni Hash in OpenSSL

- OpenSSL fornisce numerose funzioni hash (o Message Digest), tra le quali MD2, MD4, MD5, MDC2, SHA1, RIPEMD-160, etc.
  - Mediante il seguente comando è possibile visualizzare alcune delle funzioni hash fornite da OpenSSL

```
openssl list-message-digest-commands
```

- Si ricorda che alcune funzioni hanno problemi di sicurezza, e si deve valutare se utilizzarle

Funzioni Hash in OpenSSL

(Il comando dgst)

- Mediante il comando **dgst** è possibile accedere alle funzioni hash fornite da OpenSSL
  - Tale comando opera su dati letti dallo standard input (oppure su uno o più file)
- Se alla funzione hash viene passato più di un file, viene calcolato un hash separato per ciascun file
- L'hash calcolato è scritto in formato esadecimale sullo standard output
  - A meno che non sia specificato un file di output

Funzioni Hash in OpenSSL

Opzioni principali del comando dgst

```
openssl dgst args file
```

- **args**
  - **-sha|-sha1|-mdc2|-ripemd160|-sha224|-sha256|-sha384|-sha512|-md2|-md4|-md5|-dss1**
    - Funzione hash da usare per il calcolo del message digest
  - **-out filename**
    - File in cui scrivere l'output della funzione. Altrimenti l'output viene scritto sullo standard output
  - **-hmac key**
    - Crea un hashed MAC usando una determinata chiave
- **file**
  - File (uno o più) su cui deve essere applicata la funzione hash

Funzioni Hash in OpenSSL

Opzioni principali del comando dgst

```
openssl dgst args file
```

- **args**
  - **-sha|-sh|-sha256|-sha384|-sha512|-**
    - Funzio… message digest
  - **-out filename**
    - File in cui scrivere l'output della funzione. Altrimenti l'output viene scritto sullo standard output
  - **-hmac key**
    - Crea un hashed MAC usando una determinata chiave
- **file**
  - File (uno o più) su cui deve essere applicata la funzione hash

Per ottenere la lista completa delle opzioni del comando **dgst** è possibile utilizzare **man dgst**

Funzioni Hash in OpenSSL

(Esempio Calcolo Hash ed HMAC)

Mediante il seguente comando è possibile calcolare la funzione hash (SHA512 nell'esempio) di un file preso in input (**file.txt**), scrivendo il risultato su un file di output (**DigestOutput.txt**)

```
openssl dgst -sha512 -out DigestOutput.txt file.txt
```

Mediante il seguente comando è possibile calcolare l'HMAC di un file preso in input (**file.txt**), scrivendo il risultato su un file di output (**HMACOutput.txt**) ed utilizzando la stringa **P1pp0B4udo** come chiave

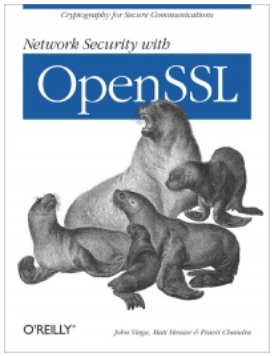
```
openssl dgst -sha512 -out HMACOutput.txt -hmac P1pp0B4ud0 file.txt
```

HMAC-SHA512(file.txt)=
7ff9e2a6d40177e962bedd54c35a1b56e7cc557d73167451f59d27ed8ef9c26678bfbf
c250333af4f9d9a5c78d376e71b04818e94b137ec61a8df6d764267e31

Contenuto del file HMACOutput.txt

Bibliografia

- Network Security with OpenSSL
  Pravir Chandra, Matt Messier and John Viega (2002), O'Reilly
  - Cap. 2.2
  - Appendix A. Command-Line Reference



- Documentazione su OpenSSL
  - https://www.openssl.org/docs/

OpenSSL
Cryptography and SSL/TLS Toolkit

Domande?