Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ

Εργαστήριο-Hash functions in OpenSSL

A. θα χρησιμοποιήσουμε το εργαλείο openssl για να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε δεδομένα χρησιμοποιώντας hash functions και μνήματα digest. Με το τέλος αυτού του εργαστήριου οι φοιτητές θα μπορούν να:
   A. υπολογίζουν ένα μήνυμα digest χρησιμοποιώντας διάφορους αλγορίθμους
   B. παρατηρήσουν με μια μικρή αλλαγή στα δεδομένα τα αποτελέσματα
   C. παρατηρήσουν μια πραγματική σύγκρουσή

- Περισσότερες πληροφορίες για το OPENSSL μπορείτε να βρείτε στον σύνδεσμο,
- https://www.openssl.org/docs/manmaster/man1/enc.html.

- Το openssl υποστηρίζει 7 διαφορετικούς αλγορίθμους (md2, md4,.., sha1).
- Θα τους χρησιμοποιήσουμε όλους για να υπολογίσουμε το digest ενός αρχείου κωδικών π.χ . Passwd
- Επίσης δοκιμάστε την εντολή:
- **OpenSSL> openssl dgst -help**

- **Χρήση MD5 & SHA256**
- **$ openssl md5 passwd**
- MD5(passwd)= 5e7f80888f3d491c4963881364048c24
- **$ openssl dgst -sha256 passwd**
- SHA256(passwd)=
- 39c487734fed185cf16217552ed8b451525c240e13d41001b3782b46fdcf4708

SHA256 digest

- Να υπολογίσετε το SHA256 digest:
- **$ openssl dgst -sha256 passpwd**
- SHA256**passpwd**)= f4e709b87daf4ddea6278669224b8dd2f6b4b15ebf3d65c404d97b2fab2dfcf9
- Να ανοίξετε το αρχείο **passpwd** με gedit και να αλλάξετε ένα byte. Να το ξανατρέξετε.
- **$ openssl dgst -sha256 passpwd**
- SHA256(**passpwd**)=
- 614a2a0303e1bad7b1e6c57bf5d68bc6c4213c0ca26e4935d579c6aa7a3cf16b

- Ανοίξετε τα δυο αρχεία pdf π.χ test-1.pdf και test -2.pdf με pdf viewer και βεβαιωθείτε ότι είναι διαφορετικά.
- Εκτελεστέ τις πιο κάτω εντολές για να υπολογίσετε το SHA256 digests.

  - **$openssl dgst -sha256 test-1.pdf**
  - SHA256(test-1.pdf)= 2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0
  - **$openssl dgst -sha256 test-2.pdf**
  - SHA256(test-2.pdf)= d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff
  - **Step 7 / Βήμα 7:**
  - Να εκτελεστέ τις πιο κάτω εντολές για να υπολογίσετε το **SHA-1** digests.

  - **$ openssl dgst -sha1 test-1.pdf**
  - SHA1(test-1.pdf)= 38762cf7f55934b34d179ae6a4c80cadccbb7f0a
  - **$ openssl dgst -sha1 test-2.pdf**
  - SHA1(test-2.pdf)= 38762cf7f55934b34d179ae6a4c80cadccbb7f0a
- Βάση των αποτελεσμάτων που έχετε από τις δυο πιο πάνω εντολές τι συμπέρασμα βγάζετε.