Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita

Uputstvo za korištenje OpenSSL alata - simetrični algoritmi, kodovanje

OpenSSL predstavlja skup biblioteka za rad sa najznačajnijim kriptografskim tehnikama. U okviru standardne distribucije OpenSSL-a nalazi se i alat koji omogućava korištenje funkcija dostupnih u bibliotekama putem komandne linije. OpenSSL može da se koristi na različitim operativnim sistemima.

Funkcijame OpenSSL alata je moguće koristiti na dva načina:

1. direktno putem komandne linije, pri čemu se koristi sljedeća sintaksa:
   `openssl komanda –opcija1 –opcija2 ....`
2. prelaskom u OpenSSL način rada (unosom komande `openssl`), nakon čega nije potrebno unositi ključnu riječ `openssl` prije svake naredbe.

1. Enkripcija simetričnim kriptoalgoritmima

- komanda koja se koristi: svaki algoritam ima svoju komandu (npr. `des3`, `aes-256-cbc`, itd.). Nazivi komandi se mogu dobiti komandom `openssl ?`,
- opcije:
  - `in` *`nazivFajla`* – naziv ulazne datoteke,
  - `out` *`nazivFajla`* – naziv izlazne datoteke,
  - `d` – dekripcija (ako se ne navede, smatra se da se radi o enkripciji),
  - `base64` – za smještanje rezultata koristi *base64* kodovanje,
  - `nosalt` – kriptovanje/dekriptovanje bez korištenja *salt*-ovanja,
  - `k` – ključ,
- primjeri:
  `openssl idea-ecb –in ulaz.txt –out izlaz.txt –k kljuc` (enkripcija datoteke ulaz.txt)
  `openssl idea-ecb –in ulaz.txt –out izlaz.txt –k kljuc –base64` (enkripcija datoteke ulaz.txt, sa base64 kodovanjem rezultata)
  `openssl rc4 –d –in ulaz.txt –out izlaz.txt –k kljuc` (dekripcija datoteke izlaz.txt)

2. Kodovanje

- komanda koja se koristi: `enc`,
- opcije:
  - `base64` – upotreba *base64* kodovanja,
  - `in` – naziv ulazne datoteke,
  - `out` – naziv izlazne datoteke,
  - `d` – dekodovanje,
- primjeri:
  `openssl enc –base64 –in ulaz.bin –out izlaz.txt`
  `openssl enc –base64 –d –in ulaz.txt –out binarni.bin` (dekodovanje datoteke)

3. **Mjerenje performansi sistema enkripcijom**

- komanda koja se koristi: `speed`,
- opcije:
  - naziv kriptoalgoritma koji se koristi za testiranje (`-des`, `-des-cbc`, `-rc4`, ...)
  - ako se ova opcija ne navede, testiraju se svi algoritmi