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

Uputstvo za korištenje OpenSSL alata - integritet poruka, asimetrični algoritmi

1. **Rad sa lozinkama**
   - komanda koja se koristi: `passwd`,
   - opcije:
     `crypt` – *crypt* algoritam za generisanje otiska lozinki (podrazumijevan),
     `1` – algoritam za generisanje otiska lozinki baziran na md5 algoritmu,
     `apr1` – drugačija (tzv. *Apache*) implementacija algoritma za generisanje otiska lozinki bazirana na md5 algoritmu,
     `salt` – opcija koja omogućava upotrebu unaprijed definisane vrijednosti *salt*-a (umjesto slučajno generisane).
   - primjeri:
     `openssl passwd lozinka` (generisanje *salt*-ovanog otiska lozinke „lozinka“ korištenjem *crypt* algoritma),
     `openssl passwd -1 lozinka` (generisanje *salt*-ovanog otiska lozinke „lozinka“ korištenjem md5 algoritma),
     `openssl passwd -1 -salt vrijednosti_salta lozinka` (verifikacija ispravnosti lozinke).

2. **Rad sa hash funkcijama i digitalni potpisi**
   - komanda koja se koristi: `dgst`,
   - opcije:
     svaka funkcija ima odgovarajuću opciju (`-sha1`, `-md5`, itd.),
     `out` *`nazivFajla`* – izlazna datoteka,
     `sign` *`fajlSaKljucem`* – signalizira aplikaciji da u izlaznoj datoteci treba da se nalazi digitalni potpis kreiran na osnovu privatnog ključa iz datoteke,
     `keyform` *`format`* – format ključa (DER, PEM, itd.),
     `dss1` – heš funkcija koja se preporučuje za korištenje sa DSA algoritmom, iako nije jedina koja je podržana u novijim verzijama. Predstavlja implementaciju SHA-1 funkcije,
     `signature` *`nazivFajla`* – naziv fajla sa potpisom (ako je potrebno izvršiti verifikaciju),
     `verify` *`nazivFajla`* – naziv fajla u kojem se nalazi javni ključ za verifikaciju,
     na kraju se navodi naziv ulaznog fajla,
   - primjeri:
     `openssl dgst -sha1 -out izlaz.txt ulaz.txt` (izračunavanje otiska fajla ulaz.txt i upis vrijednosti u izlaz.txt)
     `openssl dgst -sha1 -sign kljuc.txt -keyform DER -out potpis.txt ulaz.txt` (potpisivanje dokumenta ulaz.txt)
     `openssl dgst -sha1 -verify javniKljuc.txt` –signature potpis.txt ulaz.txt (validacija potpisa)

3. **Generisanje ključeva za RSA algoritam**
   - komande koje se koriste: `genrsa`,
   - opcije:

`out` – naziv izlazne datoteke,

`des3` *`duzinaModula`* – omogućava enkripciju generisanog para ključeva 3DES algoritmom sa modulom dužine `duzinaModula`,

- primjeri:

`openssl genrsa -out izlaz.key` (generisanje para ključeva u datoteci izlaz.key)

`openssl genrsa -out izlaz.key -des3 2048` (generisanje para ključeva u datoteci izlaz.key i njihovo kriptovanje 3DES algoritmom)

Dostupni algoritmi se mogu vidjeti kucanjem komande `openssl ?`.

4. Generisanje ključeva za DSA algoritam

- generisanje ključeva za DSA algoritam se izvodi u dva koraka:
  a) generisanje datoteke koja sadrži parametre za generisanje ključa,
  `openssl dsaparam -out dsaparam.pem 2048`
  b) generisanje ključeva na osnovu parametara,
  `openssl gendsa -des3 -out kljuc.pem dsaparam.pem`
- pregled parametara koji se koriste za generisanje ključa:
  `openssl dsaparam -in dsaparam.pem -noout -text`

5. Rad sa generisanim RSA/DSA ključevima

- komanda koja se koristi: `rsa` (za RSA algoritam), `dsa` (za DSA algoritam),
- opcije:

`in` *`naziv`* – naziv ulazne datoteke,

`text` – ispis sadržaja datoteke sa generisanim ključevima u tekstualnoj formi,

`noout` – ispis izlaza komande samo na ekran,

`inform` *`formatFajla`* – format ulazne datoteke (PEM, DER, itd.),

`outform` *`formatFajla`* – format izlazne datoteke (PEM, DER, itd.),

`pubin` – signalizira aplikaciji da se u ulaznoj datoteci nalazi samo javni ključ,

`pubout` – signalizira aplikaciji da se u izlaznoj datoteci treba nalaziti samo javni ključ,

- primjeri:

`openssl rsa -in fajlsakljucevima -inform PEM -noout -text` (ispis podataka o generisanom ključu u tekstualnoj formi),

`openssl rsa -in fajlsakljucevima -inform PEM -out izlaznifajl -outform DER` (konverzija datoteke sa parom ključeva iz PEM formata u DER format),

`openssl rsa -in fajlsakljucevima -inform PEM -pubout -out izlaznifajl` (izdvajanje javnog ključa iz datoteke sa parom ključeva u PEM formatu).

6. Upotreba generisanih RSA ključeva

- komanda koja se koristi: `rsautl`
- opcije:

`encrypt` – enkripcija,

`decrypt` – dekripcija,

`in` *`nazivFajla`* – ulazna datoteka,

`out` *`nazivFajla`* – izlazna datoteka,

`inkey` *`fajlSaKljucem`* – naziv fajla koji sadrži ključ za enkripciju (podrazumijeva se da se radi o privatnom ključu),

`pubin` – signalizira aplikaciji da se u fajlu navedenom kao argument inkey opcije nalazi javni ključ,

- primjeri:
  `openssl rsautl –encrypt –in ulazIzvorni –out izlazSifrat –inkey fajlSaKljucem –pubin` (enkripcija ulaznog fajla javnim ključem)
  `openssl rsautl –decrypt –in ulazSifrat –out izlazIzvorni –inkey fajlSaPrivKljucem` (dekripcija privatnim ključem)