Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 27.08.2025. godine

Zadaci[1]

1. U pratećim materijalima je dat šifrat dobijen primjenom nepoznatog monoalfabetskog supstitucionog šifarskog algoritma na nepoznat ulazni tekst. Dekriptovati dati šifrat korištenjem leksičke analize. Kao rješenje je dovoljno odrediti 10 ispravnih zamjena.

2. U pratećim materijalima je dat niz ulaznih datoteka, kao i šifrat dobijen kriptovanjem jedne od ulazih datoteka AES algoritmom koji radi u ECB modu, pri čemu je dužina ključa 256 bita. Ključ koji je korišten za enkripciju odgovara `SHA3-256` otisku sadržaja tražene ulazne datoteke. Dodatno, dat je i `SHA3-512` otisak tražene ulazne datoteke (`kontrolni_hash.txt`), koji se može iskoristiti za validaciju ispravnosti dekripcije. Odrediti o kojoj ulaznoj datoteci se radi i izvršiti dekripciju šifrata.

3. Odrediti koji od digitalnih potpisa u pratećim materijalima je dobijen potpisivanjem datoteke `ulaz.txt` ako je korišten ključ koji je takođe dat u pratećim materijalima. Korišten je `SHA-256` algoritam prilikom generisanja potpisa. Potpisi su dati u PEM ili DER formatu.

4. U pratećim materijalima je dat niz digitalnih envelopa, kao i niz RSA ključeva. Samo jedan ključ se može iskoristiti za dekripciju jedne envelope. Odrediti o kojim datotekama se radi i prikazati (smislen) sadržaj digitalne envelope.

5. Tekst ovog zadatka se nalazi na web serveru čija adresa je data u prilogu zadatka (datoteka `zadatak.txt`). Za prijavu na web server je potrebna klijentska autentikacija. Za klijentsku autentikaciju potrebno je koristiti PKCS#12 format sertifikata. Sertifikat (x509) potreban za klijentsku autentikaciju, kao i par ključeva je takođe dat u pratećim materijalima (samo jedan ključ odgovara datom klijentskom sertifikatu). U materijalima je dat i sertifikat CA tijela koje je izdalo klijentski sertifikat.

6. U pratećim materijalima je data konfiguraciona datoteka za OpenSSL, jedan CA sertifikat, kao i datoteke sa ključevima. CA sertifikatu odgovara ključ čiji je otisak dat u materijalima (korišten je jedan od SHA algoritama). Na osnovu konfiguracione datoteke implementirati okruženje za CA tijelo. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
- sertifikat `s1.cer` (0x9A) mora biti potpisan na 60 dana, pri čemu kao svrha upotrebe ključa mora biti neporecivost i serverska autentikacija. Sertifikat ne smije biti označen kao CA sertifikat.
- sertifikat `s2.cer` (0x11) mora biti potpisan na 10 godina, pri čemu kao dozvoljena upotreba ključa mora biti navedeno potpisivanje CRL lista, klijentska I serverska autentikacija. Sertifikat mora biti označen kao CA sertifikat.

[1]**NAPOMENE**: - na moodle postaviti samo rješenja zadataka koji su rađeni
- u okviru skripte, u komentar upisati pronađeno rješenje (npr. naziv datoteke)