Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 30.08.2023. 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. Odrediti koji od digitalnih potpisa u pratećim materijalima je dobijen potpisivanjem datoteke `ulaz.txt` i koji ključ iz pratećih materijala je korišten za potpisivanje. Korišten je SHA-1 algoritam prilikom potpisivanja.

3. U pratećim materijalima je data datoteka sa šifratom dobijenim kriptovanjem nepoznate ulazne datoteke jednim od `AES` algoritama sa dužinom ključa od 256 bita (koji su dostupni u OpenSSL-u), tri puta. U pratećim materijalima su date i datoteke sa ključevima, pri čemu je za svako kriptovanje korišten različit ključ. U materijalima su data i tri otiska koja odgovaraju ključevima korištenim za kriptovanje, respektivno. Otisci su kreirani pomoću jedne od verzija MD5 algoritma za heširanje lozinki, koje OpenSSL podržava. Odrediti ključeve korištene za kriptovanje i odrediti (smislen) sadržaj ulazne datoteke.

4. U pratećim materijalima dat je CA sertifikat i niz sertifikata od kojih je određeni broj potpisan datim CA sertifikatom. Odrediti koji od datih sertifikata su dobijeni potpisivanjem zahtjeva datim CA sertifikatom.

5. Implementirati serversku i klijentsku autentikaciju za Tomcat web server, pri čemu je potrebno iskoristiti par ključeva koji se nalazi u jednoj od *keystore* datoteka koje su date u pratećim materijalima. U materijalima je dat i otisak (korišten je jedan od `SHA` algoritama) na osnovu kojeg je moguće odrediti koja od datih *keystore* datoteka je ispravna. Kao rješenje je potrebno navesti komandu kojom je izvršena verifikacija, sve generisane sertifikate i konfiguracione datoteke za Tomcat web server. Potrebno je koristiti zajedničku datoteku za klijentsku i serversku autentikaciju. Omogućiti da se klijent sa alijasom `Klient` može autentikovati kod servera. Za generisanje klijentskog sertifikata, potrebno je iskoristiti okruženje iz 6. zadatka. U rješenjima ostaviti i odgovarajući PKCS#12 sertifikat, kako bi se mogla testirati klijentska autentikacija. Koristiti lozinku sigurnost gdje je potrebno.

6. U pratećim materijalima je data konfiguraciona datoteka za OpenSSL i jedan CA sertifikat sa pripadajućim privatnim ključem. Na osnovu konfiguracione datoteke implementirati okruženje za CA tijelo, pri čemu je u okviru politike sertifikacije dozvoljeno jedino mijenjati vrijednost postojećih polja (nije dozvoljeno dodavati nova, niti brisati postojeća polja iz politike sertifikacije).

   a. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
      - sertifikat `s1.crt` mora biti potpisan na deset godina, pri čemu kao svrha upotrebe ključa mora biti navedena digitalno potpisivanje i neporecivost. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0xA1,
      - sertifikat `s2.cer` mora biti potpisan na četiri mjeseca, pri čemu kao dozvoljena upotreba ključa mora biti navedena enkripcija, serverska i klijentska autentikacija. Redni broj sertifikata mora biti 0xB1. Sertifikat mora biti označen kao CA sertifikat.
   b. Izvršiti suspenziju oba sertifikata (`lista1.crl`, 0x44, 30.09.2023.), pa izvršiti reaktivaciju samo drugog sertifikata (`lista2.crl`, 0x46, 30.10.2023.).
   c. Kreirati dva zahtjeva za sertifikatima koja nije moguće (iz različitih razloga) potpisati pomoću date konfiguracije.

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