Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 23.04.2025. 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 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.

3. U pratećim materijalima je dat niz ulaznih datoteka i niz datoteka sa otiscima dobijenim pomoću različitih hash funkcija. Samo jedan otisak odgovara jednoj od ulaznih datoteka. Odrediti o kojoj ulaznoj datoteci se radi, koji hash algoritam je iskorišten i u kojoj datoteci se nalazi traženi otisak.

4. U pratećim materijalima je data digitalna envelopa, kao i niz JKS datoteka. U jednoj od JKS datoteka se nalazi ključ kojim se može otvoriti digitalna envelopa. Pronaći traženu JKS datoteku i prikazati sadržaj digitalne envelope.

5. Tekst ovog zadatka je dat u jednoj od datoteka u pratećim materijalima. Uz tekstove zadataka je dat i potpis, kao i niz datoteka sa ključevima. Odrediti verifikacijom potpisa koji je ispravan tekst zadatka, a zatim uraditi ono što je u tekstu navedeno. Za potpisivanje je korišten jedan od SHA algoritama. Kao ispravno rješenje je potrebno predati komandu kojom je verifikovan potpis, kao i eventualne datoteke koje su tražene zadatkom.

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, 23.10.2025.), pa izvršiti reaktivaciju samo drugog sertifikata (`lista2.crl`, 0x46, 23.04.2026.).
   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)