Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 25.06.2025. 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 jednim od `CAMELLIA` algoritama (koji su dostupni u OpenSSL-u). Ključ koji je korišten za enkripciju odgovara nazivu tražene ulazne datoteke (uključujući ekstenziju `.txt`). Dodatno, dat je i otisak tražene ulazne datoteke, dobijen pomoću `SHAKE256` algoritma. Odrediti o kojoj ulaznoj datoteci se radi i koji algoritam je korišten prilikom enkripcije.

3. Odrediti koji od digitalnih potpisa u pratećim materijalima je dobijen potpisivanjem datoteke `ulaz.txt` ako je korišten jedan od ključeva koji su takođe dati u pratećim materijalima. Korišten je SHA-224 algoritam prilikom generisanja potpisa.

4. U pratećim materijalima je data digitalna envelopa, kao i niz PKCS#12 datoteka. U jednoj od PKCS#12 datoteka se nalazi ključ kojim se može otvoriti digitalna envelopa. Pronaći traženu PKCS#12 datoteku i prikazati (smislen) sadržaj digitalne envelope.

5. Bob i Alice su uspostavili sigurnu komunikaciju. U folderima *Bob* i *Alice* nalaze se primljene poruke od raznih korisnika, tj. oni služe kao inbox. Među primljenim porukama, u folderu *Bob* nalazi se i jedna poruka od Alice, a u folderu *Alice* nalazi se jedna poruka od Boba. Pronaći date poruke i uraditi ono što se traži u njima. Sesijski ključ je kreirao Bob i poslao ga Alice-i na siguran način, zajedno sa informacijama o korištenom algoritmu (`info.enc`).

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 nije dozvoljena izmjena politike sertifikacije. Obavezno koristiti dati CA sertifikat i pripadajući ključ. Kao rješenje potrebno je predati kompletno okruženje, sa svim direktorijumima i datotekama.

   a. Iskoristiti dati CA sertifikat za potpisivanje sertifikata sa sljedećim osobinama:
      - sertifikat `s1.crt` mora biti potpisan na 2 godine, pri čemu kao svrha upotrebe ključa mora biti navedena neporecivost i razmjena ključeva. Sertifikat mora biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0xFF,
      - sertifikat `s2.crt` mora biti potpisan na 10 godina, pri čemu kao dozvoljena upotreba ključa mora biti navedena klijentska autentikacija i digitalno potpisivanje. Redni broj sertifikata mora biti 0xEE. Sertifikat ne smije biti označen kao CA sertifikat.
   b. Utvrditi da li je dato CA tijelo izdalo dati sertifikat `k2.crt` (obavezno ostaviti dokaz).
   c. Objasniti po jednom rečenicom (u datoteci `OBJASNJENJE.txt`) zašto dati zahtjevi `c1.csr`, `c2.csr` i `c3.csr` ne mogu biti potpisani pomoću date konfiguracije.
   d. Povući sertifikat `s2.crt`, a kao razlog povlačenja navesti kompromitaciju ključa. CRL lista treba da ima serijski broj 0x12, a datum izdavanja sljedeće CRL liste treba da bude 16.03.2025. godine.

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