Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 25.09.2024. 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. Dat je izlazni blok iz SubBytes transformacije četvrte runde (nakon inicijalne) AES-128-ECB algoritma u heksadecimalnom obliku (ispisan po vrstama): `0x47441ebd21c9677d24b5a1776229cf13`. Odrediti ulazni blok u AddRoundKey transformaciju iste runde.

3. U pratećim materijalima je dat niz ulaznih datoteka, kao i šifrat dobijen kriptovanjem jedne od ulazih datoteka jednim od `DES` algoritama (koji su dostupni u OpenSSL-u). Ključ koji je korišten za kriptovanje odgovara nazivu odgovarajuće ulazne datoteke (uključujući ekstenziju `.txt`). Odrediti o kojoj ulaznoj datoteci se radi (sve ulazne datoteke sadrže smislen sadržaj). Dodatno, u materijalima je dat digitalni potpis tražene datoteke i ključ kojim je izvršeno potpisivanje (korišten je SHA-1 algoritam).

4. U pratećim materijalima je dat niz datoteka, pri čemu sadržaj svake datoteke čini otisak dobijen primjenom nekog od algoritama za generisanje otiska lozinki nad nepoznatim ulaznim tekstom. Sadržaj jedne od datoteka odgovara otisku naziva te datoteke (uključujući ekstenziju `.txt`). Odrediti o kojoj datoteci se radi i koji algoritam je iskorišten za kreiranje otiska.

5. Jedan od sertifikata iz pratećih materijala je potpisan od strane vlasnika digitalnog sertifikata koji je iskorišten za implementaciju SSL/TLS komunikacije prema web serveru (adresa na tabli). Pronaći o kojem sertifikatu se radi. Korišteni *hash* algoritam je SHA-224. Nakon toga, izvršiti povlačenje pronađenog sertifikata (razlog povlačenja: promjena organizacije, serijski broj CRL liste: 0x14, datum izdavanja sljedeće liste: 25.9.2025.), pri čemu je potrebno iskoristiti okruženje za rad sa sertifikatima iz šestog zadatka.

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. Kao rješenje potrebno je predati kompletno okruženje, sa svim direktorijumima i datotekama.

a. Kreirati jedan zahtjev za sertifikatom i objasniti zašto taj zahtjev nije moguće potpisati bez dodatnih intervencija.
b. Iskoristiti dati CA sertifikat za potpisivanje sertifikata sa sljedećim osobinama:
   - sertifikat `s1.crt` mora biti potpisan na 5 godina, pri čemu kao svrha upotrebe ključa mora biti navedena samo enkripcija i dekripcija. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0x11,
   - sertifikat `s2.crt` mora biti potpisan na godinu dana, pri čemu kao dozvoljena upotreba ključa mora biti navedena samo serverska i klijentska autentikacija. Redni broj sertifikata mora biti 0xAA. Sertifikat mora biti označen kao CA sertifikat.
   - sertifikat `s3.crt` mora imati dva dodatna polja koja ne postoje u CA sertifikatu. Redni broj sertifikata mora biti 0x21.
c. Utvrditi da li je dato CA tijelo izdalo sertifikat `etf.crt` (obavezno ostaviti dokaz).

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