Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 11.06.2025. 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 simetričnih algoritama (koji su dostupni u OpenSSL-u). Odrediti o kojoj ulaznoj datoteci se radi (izvršiti dekripciju) i koji algoritam je korišten. Naziv korištenog algoritma, kao i ključ simetričnog algoritma, kriptovani su pomoću Play Fair algoritma (korišten ključ `sretno`, null karakter `x`).

3. 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.

4. U pratećim materijalima je dat niz PKCS#12 datoteka, kao i jedna digitalna envelopa. Samo jedna PKCS#12 datoteka sadrži klijentski sertifikat kojem odgovara ključ koji se nalazi u okviru digitalne envelope. Pronaći o kojoj PKCS#12 datoteci se radi. U materijalima je dat i par ključeva (`env_key.key`) pomoću kojeg je kreirana digitalna envelopa.

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. Kreirati samopotpisani CA i tri nova zahtjeva za sertifikatima. Prvi zahtjev nije moguće potpisati pomoću CA tijela. Nakon toga, generisati praznu CRL listu, izvršiti suspenziju drugog i trećeg sertifikata, pa generisati novu CRL listu. Suspendovani sertifikati moraju u okviru DN-a imati tri organizacione jedinice i dva grada, te jedan od njih mora biti označen kao CA sertifikat. Nakon toga, izvršiti reaktivaciju suspendovanog CA sertifikata, pa generisati treću CRL listu. Kao rezultat je potrebno predati CA sertifikat, sve klijentske sertifikate i sve CRL liste. Za rad sa OpenSSL-om, iskoristiti konfiguracionu datoteku datu u materijalima.

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