Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 22.01.2025. 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 DES algoritama (koji su dostupni u OpenSSL-u), tri puta. U pratećim materijalima su date i datoteke sa ključevima, pri čemu je isti ključ korišten za sva tri kriptovanja. Dodatno, dat je i otisak koji odgovara traženom ključu, dobijen jednim od SHA algoritama. Odrediti koji ključ je korišten za enkripcije i odrediti sadržaj ulazne datoteke (sadržaj je smislen).

3. U pratećim materijalima je data ulazna datoteka i datoteke sa hash otiscima. Odrediti koji od otisaka je dobijen heširanjem ulazne datoteke i koji algoritam je tom prilikom korišten.

4. U pratećim materijalima je dat niz ulaznih datoteka, digitalni potpis i PKCS#12 datoteka. Odrediti kojoj ulaznoj datoteci odgovara digitalni potpis, ako je za kreiranje potpisa iskorišten ključ koji odgovara klijentskom sertifikatu koji se nalazi u PKCS#12 datoteci.

5. U pratećim materijalima je dat niz PKCS#12 datoteka, pri čemu se samo jedna od njih može iskoristiti i za serversku i za klijentsku autentikaciju. Pronaći datu PKCS#12 datoteku i iskoristiti je za implementaciju serverske i klijentske autentikaciju na Tomcat web server (datoteka `server.xml`). Dodatno, iskoristiti par ključeva iz pronađene PKCS#12 datoteke za kreiranje samopotpisanog CA tijela i sa njim potpisati dva nova klijentska sertifikata, koja onda treba iskoristiti za klijentsku autentikaciju na Tomcat web serveru. Koristiti lozinku sigurnost gdje je potrebno. Za rad sa OpenSSL-om, iskoristiti konfiguracionu datoteku datu iz 6. zadatka.

6. U pratećim materijalima je data JKS datoteka i niz datoteka sa ključevima. Odrediti koji ključ se nalazi u klijentskom sertifikatu u JKS datoteci. Nakon određivanja ispravnog ključa, iskoristiti ga za kreiranje CA tijela (konfiguracioni fajl dat u materijalima) i generisati 2 CRL liste, pri čemu su na prvoj povučena dva sertifikata (jedan suspendovan, a drugi sa razlogom “prestanak rada”), a na drugoj se nalazi samo drugi sertifikat, dok je prvi vraćen iz suspenzije.

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