Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 27.01.2023. 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 dat je CA sertifikat i niz sertifikata od kojih je određeni broj potpisan datim CA sertifikatom. Odrediti koji od datih sertifikata su dobijeni potpisivanjem zahtjeva datim CA sertifikatom.

4. U pratećim materijalima date su ulazne datoteke i datoteka sa otiscima. Odrediti koji algoritmi i koje ulazne datoteke su iskorištene za generisanje pojedinih otisaka. Pri tome, ne moraju svi otisci nužno odgovarati nekoj od zadatih datoteka.

5. U pratećim materijalima je data PKCS#12 datoteka i niz datoteka sa ključevima. Odrediti koji ključ se nalazi u klijentskom sertifikatu u PKCS#12 datoteci. Lozinka za otvaranje PKCS#12 datoteke je “sigurnost”. Nakon određivanja ispravnog ključa, iskoristiti ga za kreiranje CA tijela (iskoristiti konfiguracioni fajl iz 6. zadatka) 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.

6. U pratećim materijalima je dat niz JKS datoteka, pri čemu se samo jedna od njih može iskoristiti za serversku autentikaciju. Pronaći datu JKS datoteku i iskoristiti je za serversku autentikaciju na Tomcat web serveru. Dodatno, iskoristiti par ključeva iz pronađene JKS 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. Koristiti istu datoteku za klijentsku i serversku autentikaciju. 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)