Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 29.12.2022. 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 RC2 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. 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 sertifikata i niz CRL lista. Odrediti koji od datih sertifikata nisu povučeni.

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 “promjena organizacije”), a na drugoj se nalazi samo drugi sertifikat, dok je prvi vraćen iz suspenzije.

6. U pratećim materijalima su date dvije PKCS#12 datoteke (cert1.p12 i cert2.p12). Implementirati klijentsku i serversku autentikaciju na Tomcat web serveru tako da se za serversku autentikaciju koristi ključ (i pripadajući sertifikat) iz datoteke server.p12, a da se za klijentsku autentikaciju koriste dva nova sertifikata (sa alijasima “K1” i “K2”) potpisana ključem koji se nalazi u datoteci klijent.p12. Potrebno je koristiti istu datoteku i za serversku i za klijentsku autentikaciju. Lozinka za pristup PKCS#12 datotekama je sigurnost. Kao rješenje je potrebno priložiti sve korištene datoteke i konfiguracije, kao i jedan sertifikat u PKCS#12 formatu koji se može iskoristiti za testiranje klijentske autentikacije. Koristiti lozinku sigurnost gdje je to potrebno.

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