Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 26.06.2024. 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. 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 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. U pratećim materijalima je dat niz JKS datoteka, pri čemu se samo jedna od njih može iskoristiti i za serversku i za klijentsku autentikaciju. Pronaći datu JKS datoteku i iskoristiti je za implementaciju serverske i klijentske 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 (na dvije godine), 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 u materijalima.

6. U pratećim materijalima je dat niz konfiguracionih datoteka za OpenSSL i otisak naziva jedne od ovih datoteka (uključujući ekstenziju .cnf). Otisak je dobijen pomoću jednog od algoritama za generisanje otiska lozinki, dostupnih u OpenSSL-u. Na osnovu konfiguracione datoteke implementirati okruženje za CA tijelo, pri čemu je u okviru politike sertifikacije dozvoljeno jedino mijenjati vrijednost postojećih polja (nije dozvoljeno dodavati nova, niti brisati postojeća polja iz politike sertifikacije).

a. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
   - sertifikat `s1.crt` mora biti potpisan na pet godina, pri čemu kao svrha upotrebe ključa mora biti navedena potpisivanje CRL lista i digitalno potpisivanje. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0x44,
   - sertifikat `s2.cer` mora biti potpisan na 5 mjeseci, pri čemu kao dozvoljena upotreba ključa mora biti navedena dekripcija, serverska i klijentska autentikacija. Redni broj sertifikata mora biti 0x4A. Sertifikat mora biti označen kao CA sertifikat.

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