Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 28.08.2024. 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 dat šifrat dobijenih kriptovanjem nepoznate ulazne datoteke `ARIA` algoritmom, sa dužinom ključa od 192 bita, u OFB modu rada. Ključ koji je korišten za kriptovanje odgovara otisku naziva jedne od datoteka koje su date u materijalima (uključujući ekstenziju .txt). Otisak je dobijen pomoću algoritma za generisanje otiska lozinki baziranom na SHA-256 algoritmu, pri čemu je salt jednak sadržaju datoteke. Odrediti u kojoj datoteci se nalazi sadržaj na osnovu kojeg se dolazi do ključa i izvršiti dekripciju šifrata (ulazna datoteka sadrži smislen sadržaj).

3. U pratećim materijalima je data digitalna envelopa, kao i niz JKS datoteka. U jednoj od JKS datoteka se nalazi ključ kojim se može otvoriti digitalna envelopa. Pronaći traženu JKS datoteku i prikazati (smislen) sadržaj digitalne envelope.

4. Odrediti vrijednosti ključa za DSA algoritam i izvršiti potpisivanje (i verifikaciju potpisa) date poruke ako su vrijednosti parametara date u jednom od fajlova u pratećim materijalima. Naziv odgovarajućeg fajla je kriptovan pomoću Playfair algoritma (korišten je ključ POSVECENOST), a dobijeni šifrat je dat u materijalima.

5. 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 dekripcija i neporecivost. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0xA7,
      - sertifikat `s2.cer` mora biti potpisan na pet mjeseci, pri čemu kao dozvoljena upotreba ključa mora biti navedena enkripcija, serverska i klijentska autentikacija. Redni broj sertifikata mora biti 0xB6. Sertifikat mora biti označen kao CA sertifikat.

6. Tekst ovog zadatka se nalazi na web serveru čija adresa je data u prilogu zadatka (datoteka `zadatak.txt`). Za prijavu na web server je potrebna klijentska autentikacija. Za klijentsku autentikaciju potrebno je koristiti PKCS#12 format sertifikata. Sertifikat (x509) potreban za klijentsku autentikaciju, kao i par ključeva je takođe dat u pratećim materijalima (samo jedan ključ odgovara datom klijentskom sertifikatu). U materijalima je dat i sertifikat CA tijela koje je izdalo klijentski sertifikat.

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