Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 28.06.2023. godine

Zadaci[1]

1. Dat je izlazni blok iz šeste runde (nakon inicijalne) AES-128-OFB algoritma u heksadecimalnom obliku: `0x499323561223ab4ccd43ca1f2613af12` (ispisan po vrstama). Odrediti izlaz iz MixColumns faze naredne runde algoritma. Dat je i ključ sedme runde (nakon inicijalne), ispisan po kolonama: `0x69db80a34c14437352d39cd531444f5a`.

2. Odrediti koji od digitalnih potpisa u pratećim materijalima je dobijen potpisivanjem datoteke `ulaz.txt` i koji ključ iz pratećih materijala je korišten za potpisivanje. Korišten je SHA-1 algoritam prilikom potpisivanja.

3. U pratećim materijalima je dat niz datoteka sa parovima ključeva za RSA algoritam. U materijalima su date i JKS i PKCS#12 datoteke. Odrediti koji od ključeva se istovremeno nalaze u obe datoteke (i u JKS i u PKCS#12).

4. U pratećim materijalima je dat niz datoteka, pri čemu sadržaj svake datoteke čini otisak dobijen primjenom nekog od algoritama za generisanje otiska lozinki nad nepoznatim ulaznim tekstom. Sadržaj jedne od datoteka odgovara otisku naziva te datoteke (uključujući ekstenziju `.txt`). Odrediti o kojoj datoteci se radi i koji algoritam je iskorišten za kreiranje otiska.

5. Implementirati serversku i klijentsku autentikaciju za Tomcat web server, pri čemu je potrebno iskoristiti par ključeva koji se nalazi u jednoj od *keystore* datoteka koje su date u pratećim materijalima. U materijalima je dat i otisak (korišten je jedan od `SHA` algoritama) na osnovu kojeg je moguće odrediti koja od datih *keystore* datoteka je ispravna. Kao rješenje je potrebno navesti komandu kojom je izvršena verifikacija, sve generisane sertifikate i konfiguracione datoteke za Tomcat web server. Potrebno je koristiti zajedničku datoteku za klijentsku i serversku autentikaciju. Omogućiti da se klijent sa alijasom `Klient` može autentikovati kod servera. Za generisanje klijentskog sertifikata, potrebno je iskoristiti okruženje iz 6. zadatka. U rješenjima ostaviti i odgovarajući PKCS#12 sertifikat, kako bi se mogla testirati klijentska autentikacija. Koristiti lozinku sigurnost gdje je potrebno.

6. U pratećim materijalima je data konfiguraciona datoteka za OpenSSL i jedan CA sertifikat sa pripadajućim privatnim ključem. 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, razmjena ključeva i serverska autentikacija. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0x92,
      - sertifikat `s2.cer` mora biti potpisan na mjesec dana, pri čemu kao dozvoljena upotreba ključa mora biti navedeno potpisivanje CRL lista i klijentska autentikacija. Redni broj sertifikata mora biti 0x78. Sertifikat mora biti označen kao CA sertifikat.
   b. Izvršiti suspenziju oba sertifikata (`lista1.crl`, 0x22, 28.07.2023.), pa izvršiti reaktivaciju samo prvog sertifikata (`lista2.crl`, 0x24, 28.08.2023.).
   c. Kreirati dva zahtjeva za sertifikatima koja nije moguće (iz različitih razloga) potpisati pomoću date konfiguracije.

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