Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 29.03.2022. 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 `CAST` algoritama (koji su dostupni u OpenSSL-u), dva puta. U pratećim materijalima su date i datoteke sa ključevima, pri čemu je za svako kriptovanje korišten različit ključ. U materijalima su data i dva otiska koja odgovaraju ključevima korištenim za kriptovanje, respektivno. Otisci su kreirani pomoću jedne od verzija `MD` algoritma za heširanje lozinki, koje OpenSSL podržava. Odrediti ključeve korištene za kriptovanje i odrediti (smislen) sadržaj ulazne datoteke.

3. Odrediti koji od digitalnih potpisa u pratećim materijalima je dobijen potpisivanjem datoteke `ulaz.txt` ako je korišten jedan od ključeva koji su takođe dati u pratećim materijalima. Korišten je jedan od SHA algoritama.

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 pomoću kojeg je kreirana digitalna envelopa.

5. Bob i Alice su uspostavili sigurnu komunikaciju. U folderima *Bob* i *Alice* nalaze se primljene poruke od raznih korisnika, tj. oni služe kao inbox. Među primljenim porukama, u folderu *Bob* nalazi se i jedna poruka od Alice, a u folderu *Alice* nalazi se jedna poruka od Boba. Pronaći date poruke i uraditi ono što se traži u njima. Sesijski ključ je kreirao Bob i poslao ga Alice-i na siguran način, zajedno sa informacijama o korištenom algoritmu. Odgovarajući sesijski ključ, kao i informacije o korištenom algoritmu, nalaze se u jednom od fajlova u folderu *Razmjena*.

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 nije dozvoljena izmjena politike sertifikacije.

a. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
   - sertifikat `s1.crt` mora biti potpisan na 8 mjesecai, pri čemu kao svrha upotrebe ključa mora biti navedena neporecivost i klijentska autentikacija. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0xA5,
   - sertifikat `s2.cer` mora biti potpisan na 4 godine, pri čemu kao dozvoljena upotreba ključa mora biti navedena enkripcija i dekripcija. Redni broj sertifikata mora biti 0xA7. Sertifikat mora biti označen kao CA sertifikat.

b. U materijalima su dati zahtjevi `r1.csr` i `r2.csr`. Izvršiti potpisivanje datih zahtjeva pomoću datog CA sertifikata. U slučaju neuspješnog potpisivanja, navesti (1-2 rečenice) razlog neuspjeha, kao i šta je potrebno uraditi kako bi se dati zahtjevi mogli potpisati.

c. generisati CRL listu `lista.crl`, na kojoj će se nalaziti sertifikati `s1.crt` i `s2.cer` sa razlozima povlačenja „promjena organizacije“ i „prestanak rada“, respektivno. Serijski broj liste je 0x44, a datum izdavanja sljedeće liste je 29.06.2022. godine.

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