Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 05.02.2025. 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. Odrediti koji ključ će biti korišten u 3. fazi DES algoritma, ako se inicijalni ključ (dat u ASCII formatu) nalazi u jednom od fajlova u pratećim materijalima, pri čemu je otisak naziva odgovarajućeg fajla takođe dat u pratećim materijalima. Otisak je kreiran pomoću jednog od dostupnih algoritama za generisanje otisaka lozinki u OpenSSL-u.

3. U pratećim materijalima je dat skup ključeva i šifrat dobijen kriptovanjem nepoznatog sadržaja asimetričnim algoritmom. Odrediti koji ključ je korišten prilikom enkripcije i izvršiti dekripciju. Ulazna datoteka je sadržavala smislen tekst.

4. U pratećim materijalima je dat niz datoteka sa parovima ključeva za RSA algoritam. U materijalima je data i JKS datoteka. Odrediti koji od datih ključeva se nalaze u klijentskim sertifikatima koji se nalaze unutar JKS datoteke.

5. 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.

6. U pratećim materijalima je data konfiguraciona datoteka za OpenSSL, jedan CA sertifikat, kao i datoteke sa ključevima. CA sertifikatu odgovara ključ čiji je otisak dat u materijalima (korišten je jedan od SHA algoritama). Na osnovu konfiguracione datoteke implementirati okruženje za CA tijelo. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
- sertifikat `s1.cer` (0x90) mora biti potpisan na 180 dana, pri čemu kao svrha upotrebe ključa mora biti razmjena ključeva i serverska autentikacija. Sertifikat ne smije biti označen kao CA sertifikat.
- sertifikat `s2.cer` (0xA1) mora biti potpisan na 100 godina, pri čemu kao dozvoljena upotreba ključa mora biti navedena potpisivanje CRL lista i klijentska autentikacija. 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)