Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 11.09.2024. 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 niz datoteka sa lozinkama, kao i niz datoteka sa otiscima. Odrediti sve parove datoteka (*dat_lozinka*, *dat_otisak*), pri čemu je *dat_lozinka* datoteka sa lozinkom, a *dat_otisak* datoteka sa otiskom koji odgovara lozinki unutar datoteke *dat_lozinka.*

3. U pratećim materijalima je dat niz ulaznih datoteka, kao i šifrat dobijen kriptovanjem jedne od ulazih datoteka jednim od `AES` algoritama (koji su dostupni u OpenSSL-u). Ključ koji je korišten za kriptovanje predstavlja naziv korištenog algoritma (onako kako je naveden u OpenSSL-u). Odrediti o kojoj ulaznoj datoteci se radi (sve ulazne datoteke sadrže smislen sadržaj) i koji algoritam je korišten.

4. U pratećim materijalima je dat niz ulaznih datoteka, digitalni potpis i PKCS#12 datoteka. Odrediti kojoj ulaznoj datoteci odgovara digitalni potpis, ako je za kreiranje potpisa iskorišten ključ koji odgovara CA sertifikatu koji se nalazi u PKCS#12 datoteci.

5. 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. Obavezno koristiti dati CA sertifikat i pripadajući ključ. Kao rješenje potrebno je predati kompletno okruženje, sa svim direktorijumima i datotekama.

a. Objasniti po jednom rečenicom (u datoteci `OBJASNJENJE.txt`) zašto dati zahtjevi `c1.csr`, `c2.csr` i `c3.csr` ne mogu biti potpisani pomoću date konfiguracije.
b. Iskoristiti dati CA sertifikat za potpisivanje sertifikata sa sljedećim osobinama:
   - sertifikat `s1.crt` mora biti potpisan na 6 godina, pri čemu kao svrha upotrebe ključa mora biti navedena samo enkripcija. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0xA1,
   - sertifikat `s2.crt` mora biti potpisan na 6 mjeseci, pri čemu kao dozvoljena upotreba ključa mora biti navedena samo serverska autentikacija. Redni broj sertifikata mora biti 0xB2. Sertifikat mora biti označen kao CA sertifikat.
   - Utvrditi da li je dato CA tijelo izdalo dati sertifikat `k2.crt` (obavezno ostaviti dokaz).

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)