Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 30.11.2023. 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. Dat je izlazni blok iz SubBytes faze pete runde (nakon inicijalne) AES-128-OFB algoritma u heksadecimalnom obliku (ispisan po vrstama): `0xbd266229b1f7c9263bdc797d74c91ac0`. Odrediti izlaz iz ove runde algoritma. Dat je i ključ pete runde (nakon inicijalne), ispisan po vrstama: `0x622e7c4d5f4b98dc3e7de1ae6417c298`

3. U pratećim materijalima je dat niz PKCS#12 datoteka i datoteka dobijena primjenom digitalne envelope na neki (smislen) ulazni tekst. Odrediti PKCS#12 datoteku koja sadrži ključ kojim je moguće otvoriti digitalnu envelopu i prikazati originalni sadržaj ulazne datoteke.

4. 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).

5. U pratećim materijalima dat je CA sertifikat i niz sertifikata od kojih je određeni broj potpisan datim CA sertifikatom. Odrediti koji od datih sertifikata su dobijeni potpisivanjem zahtjeva datim CA sertifikatom.

6. 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. U rješenjima ostaviti i odgovarajući PKCS#12 sertifikat, kako bi se mogla testirati klijentska autentikacija. Koristiti lozinku sigurnost gdje je potrebno.

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