Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 13.09.2023. godine

Zadaci[1]

1. Dat je šifrat dobijen enkripcijom ulaznog teksta korištenjem *Myszkowski* algoritma. Odrediti ulazni sadržaj ako se ključ koji je korišten za enkripciju nalazi u jednom od fajlova u pratećim materijalima, kao i otisak naziva odgovarajućeg fajla. Šifrat:
`EDPSZGIRTTOERIOEASARGMRIFCEERIPVUSEAIKRTAJANKATURTKKRRSIDAIBOPIUZ`

2. Dat je ulazni blok druge runde (nakon inicijalne) AES-128-CBC algoritma u heksadecimalnom obliku: `0xac9323af56ca261213cd494c1f234513` (ispisan po kolonama). Odrediti izlaz iz MixColumns faze iste runde algoritma.

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 se nalazi sertifikat servera (`server.crt`) i Vaš par ključeva (`client.key`), kao i poruke koje je server poslao raznim korisnicima. Osim toga, tu su i fajlovi u kojima se nalaze sesijski ključevi poslani od strane servera, namijenjeni korisnicima sa kojima server komunicira, kao i fajl `info.txt` u koji je server smjestio informacije o korištenom algoritmu. Jedna od tih poruka je namijenjena Vama, kao i odgovarajući sesijski ključ. Pronaći datu poruku i ključ, dekriptovati sadržaj poruke i odgovoriti na pitanje koje se nalazi u poruci. Kao rješenje, priložiti fajl sa odgovorom na pitanje, ali tako da ga samo server može pročitati (i niko drugi ko bi došao u posjed tog fajla ili odgovarajućeg sesijskog ključa). Dodatno, u rješenjima ostaviti dokaz kojim server može potvrditi da ste baš Vi odgovorili na zadato pitanje.

6. U pratećim materijalima je dat niz PKCS#12 datoteka i jedan ključ za RSA algoritam. Odrediti PKCS#12 datoteku koja sadrži sertifikat koji odgovara zadatom RSA ključu. Nakon određivanja PKCS#12 datoteke, iskoristiti je za kreiranje CA tijela (koristiti konfiguracioni fajl dat u materijalima) i generisati sertifikate `s1.cer` (0x21, godina dana, svrha upotrebe - razmjena ključeva, CA sertifikat), `s2.cer` (0x12, 10 godina, svrha upotrebe – digitalno potpisivanje, klijentska i serverska autentikacija, ne smije biti označen kao CA sertifikat) i CRL listu `lista.crl` (suspendovan `s2.cer`).

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