Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 10.02.2023. 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 osme runde (nakon inicijalne) AES-128-ECB algoritma u heksadecimalnom obliku: `0x499323561223ab4ccd43ca1f2613af12` (ispisan po vrstama). Odrediti izlaz iz MixColumns faze devete runde (nakon inicijalne). Dat je i ključ osme runde (nakon inicijalne): `0x69db80a34c14437352d39cd531444f5a`, ispisan po kolonama.

3. U pratećim materijalima je dat šifrat i niz digitalnih envelopa u kojima se nalazi po jedan ključ `CAMELLIA-128-CFB` algoritma. U materijalima su dati i ključevi kojima se mogu otvoriti pojedine envelope. Odrediti datoteku koja sadrži ključ kojim je moguće dekriptovati šifrat (dobijen pomoću `CAMELLIA-128-CFB` algoritma) i izvršiti njegovu dekripciju (ulazna datoteka sadrži smislen sadržaj).

4. Odrediti koji hash algoritam i koja ulazna datoteka su iskorišteni za generisanje otiska, pri čemu su ulazne datoteke i otisci dati u prilogu zadatka.

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 na siguran način od strane servera, namijenjeni korisnicima sa kojima server komunicira, kao i fajl `info.txt` u koji je server smjestio informacije o korištenom algoritmu (server je taj fajl poslao Vama na siguran način). 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 eventualno 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. Jedan od sertifikata iz pratećih materijala je potpisan od strane vlasnika digitalnog sertifikata koji je iskorišten za implementaciju SSL/TLS komunikacije prema web serveru (adresa na tabli). Pronaći o kojem sertifikatu se radi. Korišteni *hash* algoritam je SHA-384. Nakon toga, izvršiti povlačenje pronađenog sertifikata (razlog povlačenja: nepoznat, serijski broj CRL liste: 0x44, datum izdavanja sljedeće liste: 10.08.2023.), pri čemu je potrebno iskoristiti CA sertifikat i konfiguracioni fajl za OpenSSL, koji su dati u folderu CA.

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