Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 07.02.2024. 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. Dat je izlazni blok iz SubBytes faze devete runde (nakon inicijalne) AES-128-OFB algoritma u heksadecimalnom obliku (ispisan po kolonama): `0x3bc9bdf7dc261a7d26627479b129c0c9`. Odrediti izlaz iz MixColumns faze iste runde algoritma. Dat je i ključ iste runde (ispisan po vrstama): `0x69db80a34c14437352d39cd531444f5a`.

3. U pratećim materijalima je data digitalna envelopa, kao i niz JKS datoteka. U jednoj od JKS datoteka se nalazi ključ kojim se može otvoriti digitalna envelopa. Pronaći traženu JKS datoteku i prikazati (smislen) sadržaj digitalne envelope.

4. Dat je šifrat dobijen enkripcijom ulaznog teksta korištenjem *Myszkowski* algoritma. Odrediti ulazni sadržaj ako se ključ koji je korišten za enkripciju nalazi u jednoj od datoteka u pratećim materijalima. U materijalima se nalazi i digitalni potpis odgovarajuće ulazne datoteke, kao i ključ kojim je izvršeno potpisivanje. Prilikom kreiranja potpisa, korišten je SHA algoritam koji generiše izlaz dužine 160 bita. Šifrat: `AIIKGENZEDENZOJUETSIKPFASTNJSTRIRTRIICAKAIAPOIARRS`

5. U pratećim materijalima je dat niz konfiguracionih datoteka za OpenSSL i otisak naziva jedne od ovih datoteka (uključujući ekstenziju .cnf). Otisak je dobijen pomoću jednog od algoritama za generisanje otiska lozinki, dostupnih u OpenSSL-u. Na osnovu konfiguracione datoteke implementirati okruženje za CA tijelo, pri čemu je u okviru politike sertifikacije dozvoljeno jedino mijenjati vrijednost postojećih polja (nije dozvoljeno dodavati nova, niti brisati postojeća polja iz politike sertifikacije).

a. Iskoristiti dati sertifikat za potpisivanje 2 klijentska sertifikata sa sljedećim osobinama:
   - sertifikat `s1.crt` mora biti potpisan na deset godina, pri čemu kao svrha upotrebe ključa mora biti navedena potpisivanje CRL lista i neporecivost. Sertifikat ne smije biti označen kao CA sertifikat. Redni broj sertifikata mora biti 0x37,
   - sertifikat `s2.cer` mora biti potpisan na 12 mjeseci, pri čemu kao dozvoljena upotreba ključa mora biti navedena enkripcija, serverska i klijentska autentikacija. Redni broj sertifikata mora biti 0x36. Sertifikat mora biti označen kao CA sertifikat.

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)