Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 24.01.2024. 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 šifrat dobijenih kriptovanjem nepoznate ulazne datoteke `AES` algoritmom, sa dužinom ključa od 192 bita, u CBC modu rada. Ključ koji je korišten za kriptovanje odgovara otisku naziva (uključujući ekstenziju .txt) jedne od datoteka koje su date u materijalima (otisak je dobijen pomoću algoritma za generisanje otiska lozinki baziranom na MD5 algoritmu (Apache varijanta), pri čemu je salt jednak sadržaju datoteke od čijeg naziva je kreiran otisak). Odrediti u kojoj datoteci se nalazi sadržaj na osnovu kojeg se dolazi do ključa i izvršiti dekripciju šifrata (ulazna datoteka sadrži smislen sadržaj).

3. U pratećim materijalima date su ulazne datoteke i datoteke sa otiscima. Odrediti koji hash algoritmi i koje ulazne datoteke su iskorištene za generisanje datih otisaka.

4. U pratećim materijalima je dat niz PKCS#12 datoteka, kao i jedna digitalna envelopa. Samo jedna PKCS#12 datoteka sadrži klijentski sertifikat kojem odgovara ključ koji se nalazi u okviru digitalne envelope. Pronaći o kojoj PKCS#12 datoteci se radi. U materijalima je dat i par ključeva (`env_key.key`) pomoću kojeg je kreirana digitalna envelopa.

5. U pratećim materijalima je data PKCS#12 datoteka i niz datoteka sa ključevima. Odrediti koji ključ se nalazi u klijentskom sertifikatu u PKCS#12 datoteci. Lozinka za otvaranje PKCS#12 datoteke je “sigurnost”. Nakon određivanja ispravnog ključa, iskoristiti ga za kreiranje CA tijela (konfiguracioni fajl dat u materijalima) i generisati 2 CRL liste, pri čemu su na prvoj povučena tri sertifikata (prvi sa razlogom “prestanak rada”, drugi sa razlogom “kompromitacija ključa”, a treći suspendovan), a na drugoj se nalaze samo prvi i drugi sertifikat, dok je treći vraćen iz suspenzije.

6. Implementirati serversku i klijentsku autentikaciju za Tomcat web server, pri čemu je za serversku autentikaciju potrebno iskoristiti jednu od *keystore* datoteka, kojoj odgovara digitalni potpis dat u pratećim materijalima. Pri kreiranju digitalnog potpisa korišten je jedan od `SHA` algoritama koji generišu izlaz od 512 bita (dat je i ključ kojim je kreiran potpis). Kao rješenje je potrebno navesti komandu kojom je izvršena verifikacija, sve generisane sertifikate i konfiguracione datoteke za Tomcat web server. Potrebno je koristiti odvojene datoteke za klijentsku i serversku autentikaciju, pri čemu se za klijentsku autentikaciju treba kreirati nova *keystore* datoteka. Omogućiti da se klijent sa alijasom `Klient22` može autentikovati kod servera. Za izdavanje klijentskog sertifikata, kreirati samopotpisani CA sertifikat koristeći par ključeva koji se nalazi u pronađenoj *keystore* datoteci. 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)