Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 17.06.2024. 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: `KSIEEVLUREAPKSOLKIAITOTETDIEUSIRTVMSTSTALDAP`

2. Odrediti izlaz iz MixColumns faze u petoj rundi AES algoritma ako je dat izlaz SubBytes faze iz iste runde: `0xc9bd24626747b5297d44a1cf211e7713`. Blok je ispisan po kolonama, a algoritam radi u OFB načinu rada.

3. Odrediti vrijednosti ključa za DSA algoritam i izvršiti potpisivanje (i verifikaciju potpisa) date poruke ako su vrijednosti parametara date u jednom od fajlova u pratećim materijalima, pri čemu je hash odgovarajućeg fajla takođe dat u materijalima (korišten je jedan od SHA algoritama). Vrijednost otiska poruke koja se potpisuje je 12.

4. 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.

5. 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 `Klient33` 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.

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` (0xBA, godina dana, svrha upotrebe - razmjena ključeva, CA sertifikat), `s2.cer` (0xAB, 100 godina, svrha upotrebe – neporecivost, klijentska i serverska autentikacija, ne smije biti označen kao CA sertifikat).

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