Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 26.04.2023. 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. U pratećim materijalima je dat niz šifrata dobijenih kriptovanjem nepoznate ulazne datoteke AES algoritmom u CBC načinu rada. Dužina ključa je 192 bita. Odrediti sadržaj ulazne datoteke ako je za kriptovanje korišten ključ `sigurnost`. U datoteci otisak.hash je dat otisak ulazne datoteke dobijen jednim od SHA algoritama. Kao rješenje je potrebno navesti sadržaj ulazne datoteke, kao i sve korištene komande (ili priložiti skriptu, ako je korištena).

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. Naziv odgovarajućeg fajla je kriptovan pomoću Playfair algoritma (korišten je ključ `POSVECENOST`), a dobijeni šifrat je dat u materijalima.

4. U pratećim materijalima je dat niz sertifikata i niz CRL lista. Odrediti koji od datih sertifikata nisu povučeni.

5. Tekst ovog zadatka je dat u jednoj od datoteka u pratećim materijalima. Uz tekstove zadataka je dat i potpis, kao i niz datoteka sa ključevima. Odrediti verifikacijom potpisa koji je ispravan tekst zadatka, a zatim uraditi ono što je u tekstu navedeno. Za potpisivanje je korišten jedan od SHA algoritama. Kao ispravno rješenje je potrebno predati komandu kojom je verifikovan potpis, kao i eventualne datoteke koje su tražene zadatkom.

6. U pratećim materijalima je dat niz JKS datoteka, pri čemu se samo jedna od njih može iskoristiti i za serversku i za klijentsku autentikaciju. Pronaći datu JKS datoteku i iskoristiti je za implementaciju serverske i klijentske autentikaciju na Tomcat web serveru. Dodatno, iskoristiti par ključeva iz pronađene JKS datoteke za kreiranje samopotpisanog CA tijela i sa njim potpisati dva nova klijentska sertifikata (na dvije godine), koja onda treba iskoristiti za klijentsku autentikaciju na Tomcat web serveru. Koristiti lozinku sigurnost gdje je potrebno. Za rad sa OpenSSL-om, iskoristiti konfiguracionu datoteku datu u materijalima.

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