Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Kriptografija i računarska zaštita
Praktični dio ispita, 14.06.2023. 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 ključeva i datoteka dobijena primjenom digitalne envelope na neki ulazni tekst (korišten je jedan od algoritama obrađen na vježbama i/ili predavanjima). Kao rješenje navesti datoteku koja sadrži ključ kojim je moguće doći do originalnog sadržaja, kao i originalni sadržaj.

3. U pratećim materijalima je dat niz ulaznih datoteka i niz datoteka sa otiscima dobijenim pomoću različitih hash funkcija. Samo jedan otisak odgovara jednoj od ulaznih datoteka. Odrediti o kojoj ulaznoj datoteci se radi, koji hash algoritam je iskorišten i u kojoj datoteci se nalazi traženi otisak.

4. U pratećim materijalima je dat skup ključeva i šifrat dobijen kriptovanjem nepoznatog sadržaja asimetričnim algoritmom. Odrediti koji ključ je korišten prilikom enkripcije. Ulazna datoteka je sadržavala smislen tekst.

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)