Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita
Projektni zadatak

Zadatak

Napisati aplikaciju koja predstavlja jednostavan kviz. Kviz se sastoji od baze sa ukupno 20 pitanja. Kod nekih pitanja je potrebno upisati tačan odgovor, dok se kod nekih bira jedan od ponuđena četiri odgovora. Prilikom učešća u kvizu, korisniku se prikazuje nasumično izabranih 5 pitanja. Svako pitanje u bazi pitanja se čuva u zasebnoj slici, pomoću tehnike steganografije (onemogućiti korisnicima da pročitaju pitanja mimo aplikacije).

Da bi mogao da učestvuje u kvizu, korisnik se prvo mora registrovati. Prilikom registracije, korisnik unosi korisničko ime i lozinku, nakon čega se u okviru aplikacije (automatski) izdaje digitalni sertifikat za tog korisnika (ispisuje se putanja do kreiranog sertifikata). Voditi računa da podaci u sertifikatu budu povezani sa odgovarajućim korisničkim podacima. Svi podaci o korisniku koji su neophodni u sertifikatu se, takođe, unose prilikom registracije. Generisani sertifikat i privatni ključ treba da budu adekvatno zaštićeni.

Nakon toga, korisnik može da se prijavi na sistem uz pomoć generisanog sertifikata. Nakon prijave na sistem, korisniku se prikazuju izabrana pitanja, redom. Na kraju se ispisuje ukupan rezultat. Rezultati svih korisnika se čuvaju u zasebnoj tekstualnoj datoteci, u formatu: *KORISNIČKO_IME VRIJEME REZULTAT*. Sadržaj ove datoteke mogu da vide samo prijavljeni korisnici, u okviru aplikacije.

Potrebno je uspostaviti infrastrukturu CA tijela korištenjem OpenSSL-a ili nekog drugog alata na sljedeći način:

- CA tijelo je implementirano u dva nivoa. U prvom nivou se nalazi ROOT CA, koji je odgovoran za potpisivanje samo 2 sertifikata za podređena CA tijela.
- Podređena CA tijela se koriste (nasumično) za izdavanje digitalnih sertifikata za učesnike kviza.
- Podređena CA tijela izdaju i CRL liste za svoje sertifikate. Smatrati da će, kao i sertifikati, aktuelna CRL lista biti dostupna aplikaciji na fajl sistemu na proizvoljnoj lokaciji. Korisnik ima pravo da učestvuje tri puta u kvizu (tri prijave u aplikaciju). Nakon trećeg učešća, korisnički sertifikat se automatski povlači, a razlog je „prestanak rada“.

Steganografski algoritam definisati na proizvoljan način, ali tako da kvalitet slike bude minimalno narušen. Obratiti pažnju na brzinu aplikacije, u smislu ispravnog korištenja simetričnih i asimetričnih algoritama (iskoristiti onaj algoritam koji će u datom slučaju dati najbolje performanse, a da sigurnost sistema nije narušena).

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Dozvoljena je upotreba proizvoljnog programskog jezika i odgovarajuće biblioteke za realizaciju kriptografskih funkcija (npr. *Bouncy Castle*). Način realizacije korisničkog interfejsa neće biti ocjenjivan.

Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2022. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.