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

## *Zadatak*

Napisati aplikaciju koja simulira rad jednostavnih kriptografskih algoritama. Potrebno je podržati minimalno sljedeće algoritme: *Rail fence*, *Myszkowski* i *Playfair*. Simulacija podrazumijeva enkripciju proizvoljno unesenog teksta. Dekripcija nije neophodna.

Da bi mogao da koristi aplikaciju, korisnik se prvo mora registrovati. Prilikom registracije, korisnik unosi korisničko ime i lozinku, nakon čega se u okviru aplikacije (automatski) izdaje digitalni sertifikat i par RSA ključeva za tog korisnika (ispisuje se putanja do kreiranog sertifikata i ključa). 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.

Korisnici se prijavljuju na sistem kroz dva koraka. U prvom koraku je potrebno unijeti digitalni sertifikat, a u drugom korisničko ime i lozinku. Nakon uspješne prijave, korisniku se prikazuje spisak dostupnih algoritama za simulaciju. Korisnik bira odgovarajući algoritam, nakon čega unosi tekst koji želi enkriptovati (do 100 karaktera), kao i ključ za enkripciju. Nakon izvršene enkripcije, korisniku se prikazuje šifrat. Pored toga, rezultat svake simulacije koju korisnik inicira, čuva se u tekstualnoj datoteci, u formatu: *TEKST* | *ALGORITAM* | *KLJUČ* | *ŠIFRAT*. Na taj način, za svakog korisnika se kreira zasebna datoteka sa istorijom njegovih simulacija. Sadržaj svoje datoteke može da vidi samo prijavljeni korisnik i samo unutar aplikacije. Potrebno je zaštiti tajnost i integritet ovih datoteka u slučaju da im se pokuša pristupiti izvan aplikacije. Aplikacija treba da detektuje svaku neovlaštenu izmjenu datoteke i da o tome obavijesti odgovarajućeg korisnika nakon što se on prijavi u aplikaciju.

Aplikacija podrazumijeva postojanje infrastrukture javnog ključa. Svi sertifikati treba da budu izdati od strane CA tijela koje je uspostavljeno prije početka rada aplikacije. Podrazumijevati da će se na proizvoljnoj lokaciji na fajl-sistemu nalaziti CA sertifikat, CRL lista, sertifikati svih korisnika, kao i privatni ključ trenutno prijavljenog korisnika (nije potrebno realizovati mehanizme za razmjenu ključeva).

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. Aplikacija može bude konzolna ili sa grafičkim interfejsom.

Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2024. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.