Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita (2256) / Kriptografija i kompjuterska zaštita (A810)
Projektni zadatak

Zadatak

Napisati aplikaciju koja treba da omogući zaštitu (obfuskaciju) izvornog koda nekog programskog jezika u proizvoljnom formatu. Korisnik kriptuje datoteku sa izvornim kodom tako da je samo primalac datoteke u mogućnosti da tu datoteku pročita. Aplikacija radi u dva načina rada:

- u prvom načinu rada korisniku je omogućeno kriptovanje datoteke. Korisnik bira datoteku sa izvornim kodom (npr. *.java*) koju želi da kriptuje i sve dodatne parametre koji su potrebni za izvršavanje date operacije. Rezultat je nova datoteka koja sadrži sve što je potrebno da bi sadržaj datoteke bio zaštićen, kao i da bi se po prijemu mogao potvrditi integritet sadržaja. Aplikacija definiše sopstveni proizvoljan format u kojem će biti sačuvan sav potreban sadržaj,
- u drugom načinu rada korisniku je omogućena dekripcija i validacija sadržaja datoteke (tj. potvrda integriteta). Korisnik koji dekriptuje datoteku aplikaciji prosljeđuje putanju do kriptovane datoteke i podatke o pošiljaocu, dok je sve ostalo automatski realizovano unutar aplikacije. Kao rezultat se dobija originalna datoteka i potvrda da je sadržaj validan (ako nije bilo promjene), odnosno upozorenje da je došlo do promjene sadržaja u prenosu ako on nije validan. Nakon uspješne dekripcije, korisniku se nudi opcija da kompajlira datoteku sa izvornim kodom i izvrši program koji se dobije kompajliranjem tog koda.

Prijava na sistem podrazumijeva unos korisničkog imena i lozinke, kao i putanje do sertifikata korisnika koji se prijavljuje na sistem. Na proizvoljan način realizovati čuvanje korisničkih naloga, kao i veze između korisničkog naloga i sertifikata. Procedura kreiranja korisničkih naloga ne mora biti realizovana kroz aplikaciju.

Aplikacija podrazumijeva postojanje infrastrukture javnog ključa. Svi sertifikati treba da budu izdati od strane CA tijela koje je uspostavljeno prije početka rada aplikacije. Sertifikati se generišu nekim eksternim sistemom. 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). Validaciju sertifikata je potrebno vršiti u trenutku njegove upotrebe. Potrebno je ograničiti korisničke sertifikate tako da se mogu koristiti samo u svrhe koje zahtijeva aplikacija.

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). Potrebno je podržati barem tri algoritma za enkripciju i dva algoritma za heširanje.

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*).

Studenti su dužni da kontaktiraju predmetnog asistenta najkasnije sedam dana prije ispitnog roka za koji su prijavili ispit kako bi se odredio termin odbrane projektnog zadatka. Potrebno je predati kompletan izvorni kod aplikacije (NetBeans, Eclipse, Visual Studio ili neki drugi projekat), kako bi se aplikacija mogla testirati na laboratorijskoj opremi.

Projektni zadatak važi od prvog termina februarskog ispitnog roka 2019. godine za predmete Kriptografija i računarska zaštita (III godina) i Kriptografija i kompjuterska zaštita (IV godina). Početkom važenja ovog projektnog zadatka prestaju važiti svi raniji projektni zadaci. Studenti koji do februarskog ispitnog roka ne polože kompletan ispit moraju raditi novi projektni zadatak, bez obzira na datum odbrane prethodnog projektnog zadatka.

Odbranjen projektni zadatak važi do objavljivanja teksta sljedećeg projektnog zadatka.