IBClientApp - resenje

IBClientApp je klijentska aplikacija za sigurnu razmenu poruka u:

1. XML formatu (enveloped stil),
2. csv formatu (bez potpisa).

Za obe aplikacije su korisceni keystore-ovi i sertifikati generisani upotrebom alata Portecle koji se nalaze u *data* folderu pod nazivom *usera.jks i userb.jks*. Za oba fajla password je “1234”. U komentarima u kodu se nalaze detaljnija objasnjenja procesa enkriptovanja i dekriptovanja poruka u oba formata i transformacija kroz koje te poruke prolaze.

Aplikaciju za razmenu poruka u xml formatu sa potpisom bilo je potrebno odraditi kao glavni deo projekta. Kako bi se ova aplikacija pokrenula i poslala i potpisala poruka u xml formatu, potrebno je prvo pokrenuti klasu WriteMailClient.java. U konzoli je potrebno uneti primaoca poruke, subjekat, kao i telo poruke. Prvo se kreira xml fajl sa sadrzajem poruke - ovaj xml fajl se cuva u folderu *data* pod nazivom *mailsent.xml*. Nakon toga, ona se potpisuje u enveloped stilu, i takva se cuva u xml fajl pod nazivom *mailsent_signed.xml*. Potpisana poruka se enkriptuje i cuva u fajl *mailsent_signed_encrypted.xml*, pre slanja se pretvara u String i takva se salje korisniku u telu poruke. Ukoliko je poruka uspesno poslata, korisnik ce o tome biti obavesten u konzoli.

Kako bi se poruka dekriptovala, potrebno je pokrenuti klasu ReadMailClient.java. Iz liste mejlova sada korisniku prikazane u konzoli, potrebno je odabrati i uneti broj poruke koju zelimo da dekriptujemo (poslednja neprocitana poruka je pod brojem 0). Prvo poruku preuzimamo u String formatu, a onda nakon nje kreiramo xml fajl pod nazivom *mail_recieved_encrypted.xml*. Nakon toga se izvrsava dekriptovanje poruke, kao i verifikacija potpisa iz nje. Ukoliko je poruka uspesno dekriptovana, i potpis verifikovan, u konzoli ce se ispisati subjekat i telo poruke.

Takodje je prikazan i slucaj kada je integritet poruke narusen: ukoliko promenimo subjekat poruke, njen integritet ce biti narusen, i potpis u tom slucaju nece biti validan, sto ce biti i ispisano u konzoli.

Napomena: Pravljen je zaseban fajl za svaki stadijum formiranja dokumenta kako bi se lakse pratio proces kroz koji prolazi poruka koja se enkriptuje/dekriptuje.

Aplikaciju za razmenu poruka u csv formatu bilo je potrebno odraditi za kontrolnu tacku. Kako bi se ova aplikacija pokrenula i poslao enkriptovan mejl, potrebno je zakomentarisati kod od linije 93 do linije 113 (zakljucno sa tom linijom), a otkomentarisati kod od linije 120, do linije 179 (zakljucno sa tom linijom) u WriteMailClient.java fajlu, paket app. Nakon pokretanja aplikacije, u konzoli je potrebno upisati primaoca poruke, subjekat, kao i telo poruke. Poruka se tada enkriptuje, i salje primaocu. Ukoliko je poruka uspesno poslata, korisnik ce o tome biti obavesten u konzoli.

Kako bi se poruka uspesno dekriptovala, potrebno je u ReadMailClient.java fajlu zakomentarisati kod od linije 129 do 159 (zakljucno sa tom linijom), a otkomentarisati kod od linije 167 do 221 (zakljucno sa tom linijom). Nakon toga, potrebno je pokrenuti projekat, ulogovati se na mejl na koji je prethodno poslata enkriptovana poruka, naci tu poruku i odabrati broj pod kojim se ona nalazi (uglavnom je poslednja neprocitana poruka pod brojem 0). U konzoli ce biti ispisan Subject, kao i Body poruke u dekriptovanom obliku. Ukoliko je poruka uspesno dekriptovana, njen sadrzaj ce biti ispisan u konzoli.