Projekat IB_Shell i MailClient

Za enkripciju poruke koristimo secretkey koji enkriptujemo uz pomoc javnog kljuca korisnika b i algoritma RSA .
A korisnik B za dekripciju kljuca secretkey kroisti svoj privatni kljuc. I uz pomoc tog secretkey-a koji je upravo dekriptovao moze da dekriptuje poruku koju je dobio.

Napravljeni su fajlovi .jks i .cer, odnosno keystore u alatu portecle.
privatnim i javnim ljucevima oba usera enkriptovali i dekriptovali tajni kljuc i poruke.

Podaci iz keystora su sledeci za klasu MailClient za :
UserA je alias usera, a sifra 1234. I sifra 1234.
UserB je alias userb, a sifra 4567. I sifra keystora je 4567.

U projektu MailClient:

Klasa WriteMailClientSluzi za pisanje poruke i enkripciju poruka.

Dobavljamo javni kljuc od UseraB i njegov sertifikat.
Izgenerisemo tajni kljuc asimetricnim algoritmom.
Kriptovani kljuc je secretkey.
Poruku sifrujem uz pomoc secretkey-a, a secretkey sifrujem uz pomoc javnog kljuca korisnika b.

Klasa ReadMailClient sluzi za citanje enkriptovane poruke i njemu dekripciju.

Privatnim kljucem korisnika B dekriptujemo enkriptovani kljuc i dobijamo secretkey, kojim dekriptujemo dobijenu poruku.
Vertifikacijom (VerifySignatureEnveloped) dokumenta proveravamo da li je dokument/poruka koju smo slali ostala ista, da je neko nije menjao.

obicnaPoruka.xml je poruka koji smo mi poslali na neki mejl.
poslataPoruka.xml je prouka koja je enkriptovana.
potpisanajPoruka je poruka koja sadrzi potpis, tj potpisana je.
dekriptovanaPoruka je poraka koja je dekriptovana i pocitana.

U projektu IB_Shell_Project:

Kada pokrecemo aplikaciju idemo na Chrome i gadjamo adresu https://localhost:8443.

U folder data fajlovi .jks i.cer nam trebaju za protokol https.

Koristim MySQL bazu za cuvanje korisnika.

index.html je glavna stranica, baca na registraciju, osoba ide na login, i baca ga na welcome.html.

U klasi SecurityConfig za sifrovanje password-a sam koristila

bCryptPasswordEncoder.

U klasi User sam stavila da svi korisnici budu aktvini, da se mogu ulogavati kad god, posle registarcije.

U klasi UserInfoSerImplem imamo metodu koja nam po mejlu trazi korisnika.

U paketu src/main/resources register.js sadrzi funkcije za registarciju.

U fajli index.html nam se nalazi izgled register.js.

Fajl import.sql sadrzi koje autoritije imamo, odnosno Admin ili Regular