Емилија Георгиевска 183044

Документација – Домашна задача 2
Протокол Керберос

Note: На последната проверка во main методот, AEC инстанцата не го декриптира Yb – дава null, а добро ги декриптира/енкриптира и Ya и Yab – во што не гледам каде би бил проблемот, да работи за едно, а да не работи за друго исто такво..

Класи и методи:

1. **User**

   Оваа класа претставува апстракција на корисник во целиот овој систем, кој сака да комуницира со други корисници. (пример Алис сака да комуницира со Боб)
   Бидејќи овој корисник мора да биде регистриран во системот, за него чуваме име, уникатно ИД преку кое ке го идентифицираме и клуч потребен за комуникацијата.

   - generateNonce() – генерирање на број кој се користи само еднаш
   - sendRequest() - еден корисник на контролерот(КДЦ) му кажува дека сака да комуницира со друг корисник. (Request : IdAlice, IdBob, NonceAlice)
   - verifyYa()- верификација на ya
   - verifyYbAndYab()-верификација на ya и yab

2. **KDC**

   KDC е системот за утврдување на клучеви – и контролерот за спроведување на целата оваа комуникација.

   - Тој врши регистрирање на корисниците така што им генерира клучеви - со generateKey()
   - Секој еден корисник кој сака да зборува со друг корисник праќа барање до KDC- кое тој го обработува со generateResponse()
   - За секоја комуникација помеѓу 2 корисника KDC генерира сесиски клуч со generateSessionKey(), кој тие два корисника ке го користат за енкрипција на комуникацијата(пораките).

3. **KerberosProtocol**
    a) Најпрво вршиме регистрација на корисниците Алис и Боб
    b) Алис му кажува на КДЦ дека сака да зборува со Боб
    c) Боб генерира одговор на ова барање – ya и yb
    d) Алис го верификува ya и генерира yab
    e) Боб ги верификува yb и yab
    f) Откако се случуваат сите овие проверки, Алис праќа порака енкриптирана со сесискиот клуч, а Боб ја декриптира со истиот тој сесиски клуч.