Емилија Георгиевска 183044

Документација – Домашна задача 3
Протокол STS

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)

За него чуваме :

-име

-приватен и јавен клуч

-рандом вредност што ја генерира

- **getExponential()** – генераторот(според Дифи-Хелман) на степен – бројот што овој корисник рандом го избрал
- **getKey()** – се добива споделениот клуч кој двајцата корисници кои ке комуницираат меѓу себе го користат односно $K = \alpha^{xy}$ - каде што алфа е генераторот.

2. **STS**

Најпрво ги креирам корисниците Алис и Боб , им давам парови клучеви (приватен и јавен клуч) и им генерирам рандом броеви.

Чекор 1:

Алис со генерираниот рандом број – го прави експонентот α^x каде што алфа е генераторот(според Дифи-Хелман).

Чекор 2:

-Со помош на тоа добиено од Чекор1- α^x и со сопствениот α^y - Боб го генерира клучот К.

-Боб ја хешира низата α^y, α^x

-Таквата хеширана вредност Боб ја потпишува со својот приватен клуч

-Потпишаната вредност Боб сега ја енкриптира со клучот К што го доби

-Боб на Алис и ја праќа оваа енкриптирана вредност (последната) и α^y

Чекор 3:

-Алис исто го генерира клучот К на начин на кој го генерираше и Боб

-Алис најпрво ја декриптира целата порака со овој клуч што го доби.

-Потоа од декриптираната порака сака да го верификува потписот на Боб и тоа го прави со неговиот јавен клуч

-Откако овие проверки ќе поминат – истите работи што ги направи Боб – ги прави и Алис – односно таа прави хеширање на α^x α^y, (обратно од Боб) , потоа потпишува со својот приватен клуч...

Во продолжение би следувала иста проверка на добиените податоци од страна на Боб- како што проверката беше кај Алис.

- Дали може да извршиме Man-in-the-Middle напад врз овој протокол? Зошто?

Овој протокол претпоставува дека страните имаат клучеви за потпис(Обезбедени преку сертификати), кои се користат за потпишување пораки, со што се обезбедува безбедност од ваков напад..

- Објаснете ги параметрите што ги има во барањата и одговорите. Зошто ни се потребни?