## Лабораториска вежба 2

Автентицирана размена на клучеви

Рок на изработка: 15.04.2020

Целта на оваа лабораториска вежба, е да се имплементира поедноставената верзија на Kerberos¹ протоколот.

```
Key Establishment Using a Simplified Version of Kerberos
Alice
                                                 KDC
                                                                                         Bob
KEK: kA
                                                 KEK: kA, kB
                                                                                         KEK: kB
generate nonce rA
                                    RQST(ID_A,ID_B,r_A)
                                                 generate random kses
                                                 generate lifetime T
                                                 y_A = e_{k_A}(k_{ses}, r_A, T, ID_B)
                                                 y_B = e_{k_B}(k_{ses}, ID_A, T)
                                           y_A, y_B
k_{ses}, r'_A, T, ID_B = e_{k_A}^{-1}(y_A)
verify r'_A = r_A
verify IDB
verify lifetime T
generate time stamp T_S
y_{AB} = e_{k_{Ses}}(ID_A, T_S)
                                          YAB, YB
                                                                                        k_{ses}, ID_A, T = e_{k_B}^{-1}(y_B)
                                                                                        ID_A', T_S = e_{k_{ses}}^{-1}(y_{AB})
verify ID_A' = ID_A
                                                                                         verify lifetime T
                                                                                         verify time stamp T_S
y = e_{k_{ses}}(x)
                                                                                        x = e_{k_{ses}}^{-1}(y)
```

Според погорната слика, вашата задача е: користејќи го Java Cryptography API-то (од лаб 1), да ги имплементирате сите делови од овој поедноставен протокол.

Поточно, треба да се имплементираат (1) засегнатите страни (Alice, Bob и KDC), (2) барањето до KDC, (3) одговорот од KDC, (4) верификацијата на одговорт, (5) префрлањето на клучот до Bob и (6) праќање на енкриптирани податоци од Alice до Bob.

\_

<sup>&</sup>lt;sup>1</sup> https://en.wikipedia.org/wiki/Kerberos\_(protocol)

## Барања

- (1) Засегнатите страни имплементирајте ги како посебни класи со акциите што ги нудат претставени како методи.
- (2) Барањето моделирајте го како повик на метод.
- (3) Одговорот формулирајте го во соодветен повратен објект што ги содржи соодветните атрибути.
- (4) Верификацијата имплементирајте ја како метод кој што фрла исклучок, доколку одговорот од KDC не е валиден.
- (5) Префрлањето на клучот имплементирајте го како повик кај објектот на Воb, каде што Alice ги праќа параметрите.
- (6) Соодветно дефинирајте метод за енкрипција, декприпција и префрлање на информациите.

Извршете едно целосно сценарио за да проверете дали функционира протоколот како што треба, и дали Воb ќе може да ја прочита пораката на Alice.

**ЗАБЕЛЕШКА**: Претпоставуваме дека KDC веќе ги има клучевите на Alice и Bob. Внимавајте на редоследот во кој ги извршувате операциите, параметрите што ги праќате и својствата што треба да ги задоволите.

Како решение на оваа лабораториска задача, прикачете .zip фајл што го содржи решението (.java), и објаснување на решението (.pdf)