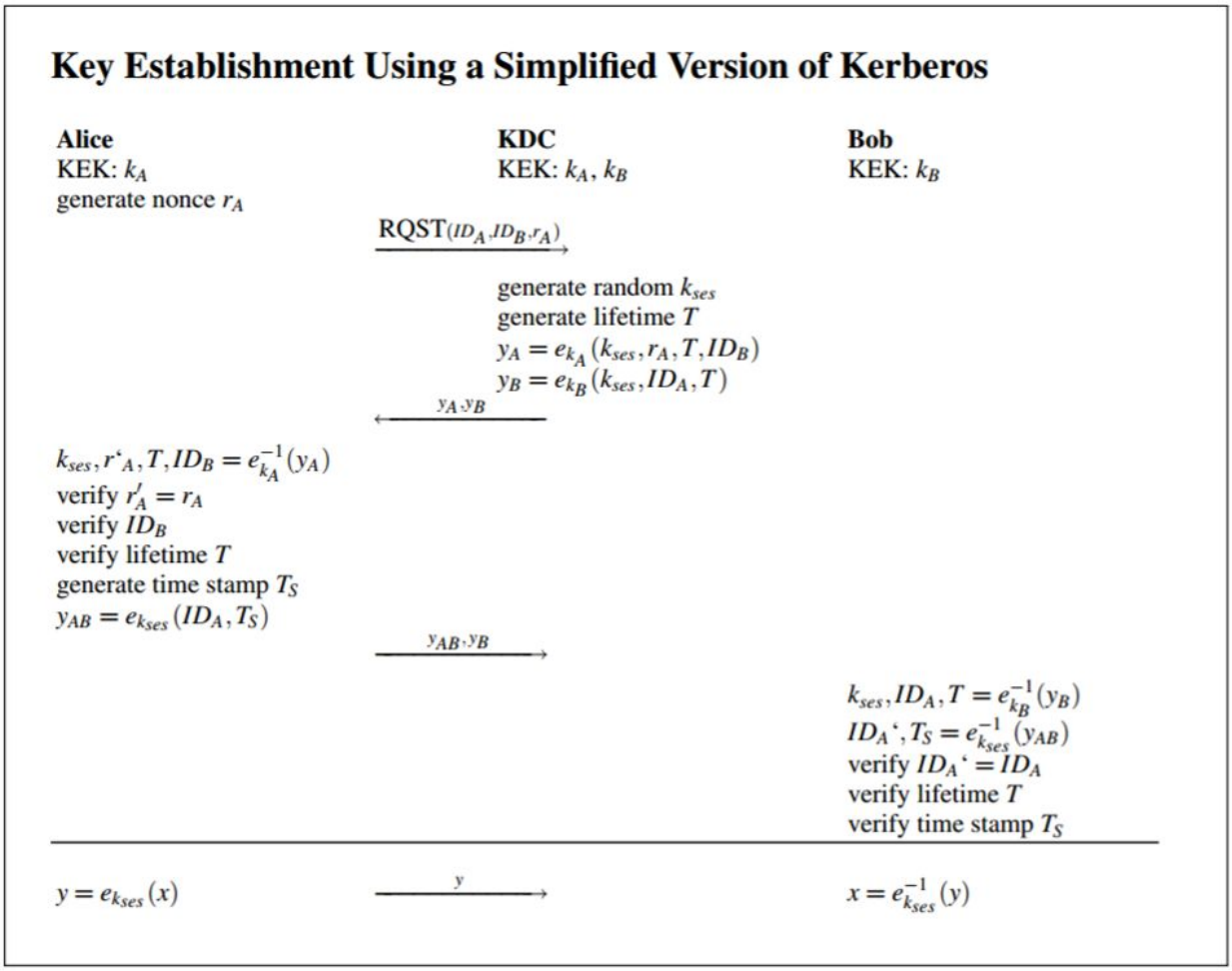
Лабораториска вежба 2

Автентицирана размена на клучеви

Рок на изработка: 15.04.2020

Целта на оваа лабораториска вежба, е да се имплементира поедноставената верзија на Kerberos[1] протоколот.



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.

[1] 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 Bob, 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 Bob 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)