CCMP

За правење на CCMP во Java употребив знаење од предметот Напредно програмирање и работи кои ги слушнав и научив за време на предметот Информациска безбедност.

Проектот се состои од повеќе класи од кои

- Header е класа која содржи MAC (дестинациска и изворна) адреси каде се испраќа пораката
- CleatTextFrame I EncryptedFrame се двете класи за порака каде едната е во чиста форма а другата е во енкриптирана форма со употреба на CCMP
- AES е класата која се користи при енкрипција и декрипција на пораката
- CCMPLogic е главната класа каде се формира целата логика за овој проект
    - encryptFrame() функцијата се користи за енкриптирање на пораката. Во неа прво пораката се дели на блокови од 16 бајти, и се генерира IV, преку тоа се пресметува MIC преку енкриптирање на изворната и дестинациската MAC адреса со тајниот клуч, и потоа со енкриптирање на пораката, и земање на последните 8 бајти.
        - Се врши енкрипција на порака во блокови од 16 блока со помош на counter кој е BigInteger класа од Java
    - decryptFrame() функцијата се користи за дектиптирање на пораката. Тоа започнува со делење на енкриптираната порака во блокови од 16 бајти, и повторно се одвива истиот процес како и кај енкрипција, за секој блок од 16 бајти, се зема counter кој повторно е BigInteger и со помош на него се врши декрипцијата на пораката се додека не заврши циклусот односно целата порака е декриптирана и ја имаме пораката јасно за преглед. Откако порака е декриптирана се пресметува MIC со истата функцијата и ако двете вредности не се исти, тогаш интегритетот на пораката бил компромизиран, но ако се исти тогаш порака е успешно пратена и добиена.