Емилија Георгиевска 183044

Документација – Домашна задача 1
Доверливост и автентичност на пораки

Класи и методи:

1. **Header**

   Кога зборуваме за пакети – односно рамки, заглавјето или Header е почетниот дел на секоја рамка.

   Најважни се изворната и дестинацискатa MAC адреса, но тука се споменати и други важни полиња.

2. **ClearTextFrame**

   Рамката содржи:

   - Header
   - број на пакет(рамка)
   - самите податоци (кои подоцна ќе ги енкриптираме)

3. **EncryptedTextFrame**

   Оваа рамка содржи:

   - Непроменет Header – ист како и почетниот
   - Број на пакет
   - Енкриптирани податоци
   - MiC
   - FCS

4. **Nonce**

   Овој број уште и наречен IV- Иницијализациски вектор, зависи од:

   - Изворната MAC адреса
   - PN- број на пакет(рамка) кој се инкрементира за секој следен испратен пакет, и оттука вредноста на Nonce ќе биде секогаш нова и свежа
   - QoS – Quality of Service

Овие комбинирани заедно даваат 104 бита, кои може соодветно да треба да бидат падирани до 128 бита.

5. CCMP

+Помошна AES готова класа

Најпрво креирам рамка која ќе ја енкриптирам, и клуч KEY од 128 бита кој ќе ми биде потребен за AES функциите

1.Калкулација на MIC за оваа рамка

a) Генерирај Nonce и енкриптирај го со AES = Енкриптиран Nonce
b) Подели ја рамката на делови од 128 бита
c) Енкриптиран Nonce XOR прв 128 битен дел
d) (Резултатот од претходното - c) енкриптирај со AES) XOR следниот 128 битен дел
e) Се додека има делови се прави d), ако последниот дел е <128 бита, AES би требало да го падира, конфигуриран е со PKCS5PADDING
f) Излезот од последниот XOR се енкриптира со AES и се земаат најзначајните 64 бита(јас ги земам сите , го немам имплементирано ова) и на нив правам XOR со иницијалната вредност на COUNTER
g) Излезот од f) е вредноста на MIC

2.Енкрипција на чистите податоци(Без header)

a) Исто како и претходно, податоците ги делам на 128 битни делови.
b) Се прави енкрипција на COUNTER (Иницијалната верзија) = Енкриптиран Counter
c) Енкриптиран Counter XOR 128 битен дел – зачувај резултат
d) За секој следен 128 битен ден Counter го зголемувам за 1, го енкриптирам и правам XOR со него(со делот) – зачувувам резултат
e) Сите зачувани резултати од почеток до крај ги спојувам и тоа се енкриптираните податоци.

Со ова се симулира праќање на енкриптирана рамка и соодветно , MIC.