В рамках данной работы необходимо реализовать протокол sigma, используя в качестве примитивов схемы ECDSA в качестве схемы формирования электронных подписей, ECDH - в качестве схемы формирования общего секрета, AES-CTR - в качестве алгоритма шифрования, HMAC-SHA256 в качестве PRF и MAC.

Пусть ECDSA состоит из тройки алгоритмов - (GEN, SIGN\_X(m), VER\_X(m, s)), где

GEN - функция генерации ключевой пары

SIGN\_X(m) - функция формирования подписи для сообщения m с использованием закрытого ключа пользователя X

VER\_X(m, s) - функция проверки подписи s для сообщения m с использованием открытого ключа пользователя X.

Пусть ECDH состоит из пары алгоритмов - (GEN, GET(X\_SK, Y\_PK)), где

GEN - функция генерации ключевой пары

GET(X\_SK, Y\_PK) - функция выработки общего секрета из открытого ключа Y и закрытого ключа X

#### 0. Предварительный обмен ключами (выполняется вне протокола)

A: (ECDSA\_PK\_A, ECDSA\_SK\_A) <- ECDSA.GEN; ECDSA\_PK\_A -> B  
B: (ECDSA\_PK\_B, ECDSA\_SK\_B) <- ECDSA.GEN; ECDSA\_PK\_B -> A

#### 1. Описание протокола Sigma.

A:   
(DH\_PK\_A, DH\_SK\_A) <- ECDH.GEN;   
r\_A <-^r {0,1}^R;   
(DH\_PK\_A, r\_A) -> B  
  
B:   
(DH\_PK\_B, DH\_SK\_B) <- ECDH.GEN;   
r\_B <-^r {0,1}^R;   
(k\_m, k\_e) <- PRF\_(r\_A||r\_B)(ECDH.GET(DH\_SK\_B, DH\_PK\_A));   
(DH\_PK\_B, r\_B, B, ECDSA.SIGN\_B(DH\_PK\_A, DH\_PK\_B), MAC\_k\_m(B)) -> A  
  
A:   
(k\_m, k\_e) <- PRF\_(r\_A||r\_B)(ECDH.GET(DH\_SK\_A, DH\_PK\_B));   
(A, ECDSA.SIGN\_A(DH\_PK\_B, DH\_PK\_A), MAC\_k\_m(A)) -> B

где <-^r Q - выбор случайного элемента из Q (равномерное распределение);

R - параметр, принять равным 128.

**ВАЖНО - Неявно предполагается проверка всех полученных подписей и кодов аутентичности. Процедуры проверки опущены в описании для простоты. При реализации необходимо реализовать все проверки, и в случае нарушения аутентичности выдавать соответствующее исключение.**

#### 2. Отправка зашифрованных данных

A: c <- AES\_k\_e(m); (c, MAC\_k\_m(c)) -> B

#### Описание лабораторной работы

1. Реализовать протокол Sigma, используя встроенные средства языка, получив общие ключи для аутентификации и шифрования.
2. Использовать полученные ключи для аутентифицированного шифрования AES-CRT-Then-Hmac для обеспечения аутентичности и секретности данных.
3. Проверить аутентичность полученных данных на стороне получателя и расшифровать сообщение.

#### Дополнительные ссылки

https://webee.technion.ac.il/~hugo/sigma-pdf.pdf (стр 17-18)