Задача № 2
Реализация протоколов Диффи–Хеллмана и MQV на эллиптической кривой

Эллиптическая кривая

Рекомендуется использовать кривую Curve P-256. Кривая задана уравнением

$$Y^2 = X^3 + aX + b \pmod{p}.$$

Параметры:

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$
$a = -3$
($b = 0$x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b)

Точка $G = (x_G, y_G)$ является генератором множества точек порядка q, причём q – простое число. В принципе любая точка кроме точки в бесконечности может служить генератором. Иными словами, точки образуют циклическую группу простого порядка.

$q = 115792089210356248762697446949407573529996955224135760342422259061068512044369$
$x_G = 0$x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
$y_G = 0$x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

Протокол Диффи–Хеллмана на эллиптической кривой

Протокол совпадает с тем, который реализовывался в циклической подгруппе простого поля, но мы изменим обозначения, чтобы не было пересечения с обозначениями параметров и точек на кривой.

Пользователи C (Cathy) и F (Fred) выбирают секретные ключи соответственно $c, f \in \mathbf{Z}_q$, вычисляют открытые ключи $C = [c]G$, $F = [f]G$ и обмениваются открытыми ключами (по открытому каналу). Общий для C и F ключ вычисляется ими как $S = [c]F = [f]C$. В качестве результирующего ключа K можно взять координату x точки S или (что лучше) значение хеш-функции от точки S.

Протокол MQV на эллиптической кривой

Обозначим через l половину битовой длины числа q: $l = 128$. Пользователи C и F генерируют долговременные пары секретных и открытых ключей соответственно c, C и f, F: $c, f \in \mathbf{Z}_q$, $C = [c]G$, $F = [f]G$. Открытые ключи пересылаются всем пользователям в виде сертифицированного (подписанного удостоверяющим центром) справочника.

Для построения общего сеансового ключа пользователь C генерирует случайное число $u \in \mathbf{Z}_q$ и вычисляет $U = [u]G$. Пользователь F генерирует случайное число $v \in \mathbf{Z}_q$ и вычисляет $V = [v]G$. Затем пользователи обмениваются точками U и V по открытому каналу связи. Обозначим x-координаты точек U и V через x_U и x_V соответственно. Оба

пользователя вычисляют числа $d = 2^l + (x_U \bmod 2^l)$, $e = 2^l + (x_V \bmod 2^l)$. Пользователь C вычисляет $S_C = [u + dc](V + [e]F)$. Пользователь F вычисляет $S_F = [v + ef](U + [d]C)$ (напомним, что при множители точек приводятся mod q). Должно выполниться равенство $S_C = S_F$. Результирующий ключ получается как координата x точки S или (что лучше) значение хеш-функции от точки S.

Задание

1. Реализовать алгоритмы Диффи–Хеллмана и MQV на эллиптической кривой в аффинном представлении точек.

2. Реализовать алгоритмы Диффи–Хеллмана и MQV на эллиптической кривой в проективном представлении точек.

3. Осуществить замеры времени (в виде числа процессорных циклов) при выполнении основных этапов во всех алгоритмах и провести их сопоставление.