Лабораторная работа 6: «Изучение свойств группы эллиптической кривой» [до 26 мая]

1. О деталях реализации и средствах разработки

- Вывод списка эллиптических кривых, используемых `openssl`:

```
openssl ecparam -list_curves
```

- Генерация файла с параметрами для последующей генерации ключа по протоколу Диффи-Хеллмана на эллиптических кривых (название кривой – любое из списка):

```
openssl ecparam -name prime256v1 -genkey -noout -out params.pem
```

- Просмотр файла с параметрами:

```
openssl ec -in params.pem -text -noout
```

- Генерация закрытого ключа:

```
openssl ecparam -in params.pem -genkey -noout -out privatekey.pem
```

- Для выработки общего ключа[1] по схеме Диффи-Хеллмана на эллиптических кривых сначала следует задать эллиптическую группу точек $E(\mathbb{Z}_p)$, т.е. выбрать параметры эллиптической кривой (a и b) и достаточно большое простое число p. Также нужно выбрать генерирующую точку $G(x_1, y_1)$ подгруппы в группе E, причем наименьшее значение k, при котором $kG = \mathcal{O}$, должно быть очень большим простым числом. Процедура генерации закрытого ключа Алисой и Бобом следующая (значения p, a, b и G не скрываютя):

    1) Алиса выбирает секретное целое число $k_A < p$ и генерирует точку $P_A = k_A \cdot G$.

[1]Ключ K является точкой, т.е. парой чисел. Чтобы использовать его в качестве сеансового ключа для традиционного шифрования, можно, например, просто выбрать из него одну координату (x или y), применив (необязательно) некоторую функцию от этой координаты.

2) Боб выбирает секретное целое число $k_B < p$ и генерирует точку $P_B = k_B \cdot G$.
3) Алиса и Боб обмениваются вычисленными P_A и P_B.
4) Алиса и Боб независимо друг от друга вычисляют значение секретного ключа K:

$$k_A \cdot P_B = k_A \cdot (k_B \cdot G) = k_B \cdot (k_A \cdot G) = k_B \cdot P_A = K.$$

- Этапы выработки ключа по протоколу Диффи-Хеллмана с помощью утилиты `openssl`:

```
openssl genpkey -out alice.pem -algorithm EC -pkeyopt
↪  ec_paramgen_curve:P-256 -pkeyopt ec_param_enc:named_curve

openssl pkey -pubout -in alice.pem -out alice.pub

openssl genpkey -out bob.pem -algorithm EC -pkeyopt
↪  ec_paramgen_curve:P-256 -pkeyopt ec_param_enc:named_curve

openssl pkey -pubout -in bob.pem -out bob.pub

openssl pkeyutl -derive -out alicebob.key -inkey alice.pem -peerkey
↪  bob.pub

openssl pkeyutl -derive -out bobalice.key -inkey bob.pem -peerkey
↪  alice.pub
```

2. Постановка задачи

Напишите программу, генерирующую и визуализирующую все решения уравнения вида $y^2 \equiv x^3 + ax + b \pmod p$, где $a, b \in \mathbb{Z}_p$, где p – простое число (т.е. точки произвольной эллиптической кривой над конечным полем). Реализуйте операции (с наглядным представлением результата): 1) сложения двух точек кривой; 2) удвоения точки кривой.

3. Задания для подготовки к экзамену

1. Распишите (на примере) нахождение точек группы эллиптической кривой. Входные данные: xxx.

2. Реализуйте клиент-серверное приложение, где клиент и сервер совместно вырабатывают закрытый ключ (для дальнейшего взаимо-

действия) на основе эллиптической кривой над конечным полем по протоколу Диффи-Хеллмана.