

Министерство образования Республики Беларусь
Учреждение образования “Белорусский государственный
университет информатики и радиоэлектроники”

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина «Методы защиты информации»

Отчет
к лабораторной работе №7

Выполнил:
студент

г
р
.
6
5
3
5
0
1

Тимофеев К. А.

Проверил:
Артемьев В.С.

Минск, 2019

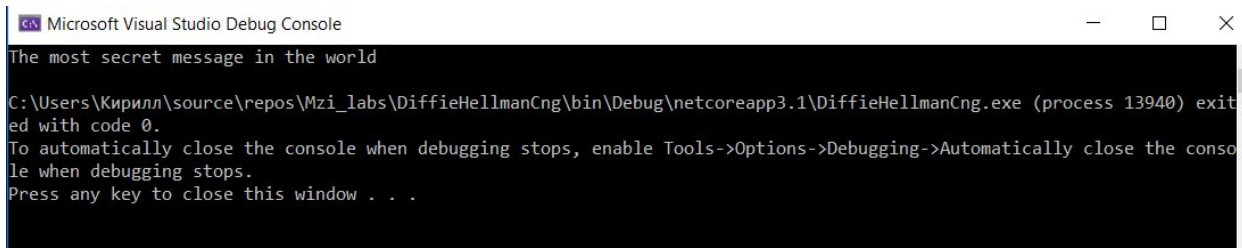
Введение

В лабораторной работе необходимо было реализовать схему шифрования и дешифрования для аналога алгоритма Диффи-Хеллмана на основе эллиптических кривых.

Протокол Диффи-Хеллмана на эллиптических кривых (англ. *Elliptic curve Diffie–Hellman, ECDH*) — криптографический протокол, позволяющий двум сторонам, имеющим пары открытый/закрытый ключ на эллиптических кривых, получить общий секретный ключ, используя незащищённый от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для формирования нового ключа, который затем может использоваться для последующего обмена информацией с помощью алгоритмов симметричного шифрования. Это вариация протокола Диффи-Хеллмана с использованием эллиптической криптографии.

Описание алгоритма

1. Сначала Алиса и Боб генерируют собственные закрытые и открытые ключи. У Алисы есть закрытый ключ d_A и открытый ключ $HA=d_AG$, у Боба есть ключи d_B и $HB=d_BG$. Заметьте, что и Алиса, и Боб используют одинаковые параметры области определения: одну базовую точку G на одной эллиптической кривой в одинаковом конечном поле.
2. Алиса и Боб обмениваются открытыми ключами HA и HB по незащищённому каналу. Посредник (Man In the Middle) перехватывает HA и HB , но не может определить ни d_A , ни d_B , не решив задачу дискретного логарифмирования.
3. Алиса вычисляет $S=d_AHB$ (с помощью собственного закрытого ключа и открытого ключа Боба), а Боб вычисляет $S=d_BHA$ (с помощью собственного закрытого ключа и открытого ключа Алисы). Учтите, что S одинаков и для Алисы, и для Боба.



```
Microsoft Visual Studio Debug Console
The most secret message in the world
C:\Users\Кирилл\source\repos\Mzi_labs\DiffieHellmanCng\bin\Debug\netcoreapp3.1\DiffieHellmanCng.exe (process 13940) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

Рис.1 Результат ввода данных и исполнения программы