Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский Университет ИТМО»
Факультет безопасности информационных технологий

Дисциплина:
«Разработка систем аутентификации и криптографии»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1
«Реализация алгоритма шифрования Эль-Гамаля»

Выполнили:
Магистрант гр. N42514c Э.Р. Кочкаров

Санкт-Петербург
2020 г.

1.Цель работы (задача) – создать программу, которая реализует криптографический алгоритм по схеме Эль-Гамаля.

2.Описание выбранных средств реализации и обоснования выбора

В качестве языка программирования был выбран C# поскольку есть опыт реализации других криптографических алгоритмов на данном языке.

C# является объектно-ориентированным языком программирования, разработанный компанией Microsoft в качестве языка для разработки приложений для платформы Microsoft .NET Framework. В свою очередь, .NET Framework - это программная платформа, т. е. некая "среда выполнения", в которой должен работать код, написанный для данной платформы. Таким образом, чтобы работала программа, написанная на C#, необходима установленная .NET Framework.

В качестве среды разработки будет использована Microsoft Visual Studio 2019. В данном случае можно сказать, что других вариантов просто нет при разработке на Windows. Это официальная, самая "правильная", функциональная среда разработки, в которой есть все что необходимо.

3.Описание алгоритма.

Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

А) Генерация ключей.

1. Генерируется случайное простое число **p**
2. Выбирается целое число **g**— первообразный корень **p**.

3. Выбирается случайное целое число, взаимно простое с **(p-1), x** такое, что **1 < x < p – 1**

4. Вычисляется $\boldsymbol{y = g^x mod\ p}$

5. Открытым ключом является **y**, закрытым ключом — число **x**.

Б) Шифрование

Сообщение **M** должно быть меньше числа **p**. Сообщение шифруется следующим образом:

1. Выбирается сессионный ключ — случайное целое число, взаимно простое с **(p-1), k** такое, что **1 < k < p-1**

2. Вычисляются числа $\boldsymbol{a = g^x\ mod\ p}$ и $\boldsymbol{b = y^k M\ mod\ p}$

3. Пара числе **(a, b)** являются шифротекстом.

В) Расшифрование

Зная закрытый ключ **x**, исходное сообщение можно вычислить из шифротекста **(a, b)** по формуле:

$$\boldsymbol{M = b(a^x)^{-1}\ mod\ p}$$

4.Ссылка на сходный код.

https://github.com/elmurza/crypto/blob/main/task1/Form1.cs

5.Выводы

В результате выполнения лабораторной работы была изучена схема построения криптографических алгоритмов на основе открытых ключей. Изучены проблемы генерации больших простых чисел, рассмотрены плюсы и минусы алгоритмов с открытыми ключами.

Стойкость схемы Эль-Гамаля основана на (гипотетической) сложности задачи дискретного логарифмирования по основанию g. Однако стойкость этой схемы в предположении сложности дискретного логарифмирования по основанию пока не доказана. Очевидно, что это предположение необходимо для стойкости схемы Эль-Гамаля, так как в противном случае противник сможет полностью раскрыть схему, вычислив секретный ключ по известному открытому.