МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Скрытый канал на основе схемы Эль-Гамаля

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Фатеева Сергея Юрьевича

Научный руководитель
доцент к. ф.-м. н. _____ В. Е. Новиков
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

Впервые понятие первообразного корня для простого модуля p вводится великим математиком Эйлером. Спустя время, обобщая наработки таких величайших умов как Ферма, Лагранж, Лежандр и других, Гаусс в своей монографии «Арифметические исследования», опубликованной в сентябре 1801 года и ставшей ключевым этапом в развитии теории чисел, в 3 разделе под названием «О степенных вычетах» доказывает существование первообразных корней для простого модуля p.

В дальнейшем первообразные корни нашли своё применение в такой области как защита информации. Например, в схеме проверки подлинности и подписи Клауса Шнорра, в процедуре открытого распределения ключей Диффи-Хеллмана.

В 1985 году Тахер Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана.

В приложении представлены программная реализация поиска большого простого числа, поиск первых n первообразных корней по модулю этого большого числа, генерации ключей для алгоритмов Эль-Гамаля, соответствующие алгоритмы и скрытый канал передачи информации на основе схемы Эль-Гамаля.

Дипломная работа состоит из введения, 9 разделов (6 подразделов), заключения, списка использованных источников и 4 приложений. Общий объем работы – 48 страниц, из них 37 страниц – основное содержание, включая 26 рисунков, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы «Элементы теории сравнимости» приводится основной теоретический материал, базовые понятия и определения, относящиеся к теории сравнимости.

Второй раздел называется «Первообразные корни» и содержит в себе теоретическую информацию о первообразных корнях и основные теоремы, доказывающие существование первообразных корней по модулю простого числа.

Третий раздел называется «Нахождение первообразных корней по модулю p^a и $2p^a$», в котором рассмотрена основная теорема о первообразных корнях, на которой строится алгоритм, реализованный в приложении А, в функции с названием «primitive_root».

Теорема 4 (О первообразных корнях). Пусть $c = \varphi(m)$ и $q_1, q_2, \dots, q_k$ – различные простые делители числа c. Для того чтобы число g, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^{\frac{c}{q_1}} \equiv 1 (mod\ m), g^{\frac{c}{q_2}} \equiv 1 (mod\ m), \dots, g^{\frac{c}{q_k}} \equiv 1 (mod\ m) \quad (1).$$

Четвертый раздел называется «Генерация большого простого числа. Тест Миллера-Рабина», в котором рассмотрены два алгоритма, позволяющие сгенерировать большое простое число $p = 2^k q - 1$, где q – простое число.

Алгоритм 2. Генерация простого числа

Вход. d – длина в цифрах простого числа.

Выход. p – простое число, в котором количество цифр больше или равно d.

1. Случайным образом выбирается нечётное число a.

2. Запускаем цикл по $k = 1, 2, \dots$:

1) Положим $q \leftarrow 2^k a + 1$.

2) Проверяем q на простоту с помощью теста Миллера-Рабина.

3) Если «Простое», то завершаем цикл.

3. Запускаем цикл по $k = 1, 2, \ldots$:

1) Положим $p \leftarrow 2^k q + 1$.

2) Проверяем p на простоту с помощью теста Миллера-Рабина.

3) Если «Простое», то завершаем цикл. ■

В пятом разделе, который называется «Процедура Диффи-Хеллмана» рассмотрена процедура открытого распределения ключей Диффи-Хеллмана.

Процедура Диффи-Хеллмана (алгоритм генерации и обмена сеансового секретного ключа):

1) абонент A выбирает случайно число x (его закрытый ключ) и вычисляет $X = g^x \bmod p$ (его открытый ключ);

$$A \rightarrow B: \{X\};$$

2) абонент B выбирает случайное число y (его закрытый ключ) и вычисляет $Y = g^y \bmod p$ (его открытый ключ);

$$B \rightarrow A: \{Y\};$$

3) абоненты A и B вычисляют секретный сеансовый ключ:

$$A: k = Y^x \bmod p;$$

$$B: k = X^y \bmod p.$$

Таким образом, после выполнения описанной процедуры у абонентов A и B есть общее число k (секретный ключ), которое используется для шифрования сообщений.

В шестом разделе, под названием «Схема Эль-Гамаль» рассмотрены два алгоритма, которые в сочетании представляют схему Эль-Гамаль.

В первом подразделе шестого раздела рассмотрена шифрсистема Эль-Гамаля.

Ключ $k = (p, g, \beta, a)$ представляется в виде открытого ключа $k_o = (p, g, \beta)$ и секретного ключа $k_c = a$.

Правило шифрования на ключе k_oопределяется формулой

$$E_{k_o}(M) = (C_1, C_2),$$

где

$$C_1 \equiv g^r (\mathrm{mod}\, p),\ C_2 \equiv M * \beta^r (mod\, p),$$

а r – случайное выбираемое число (рандомизатор) из интервала $0 \le r \le p-2$.

Правило расшифровывания на ключе k определяется формулой

$$D_k(C_1, C_2) = C_2 * (C_1^a)^{-1} (\mathrm{mod}\, p).$$

Во втором подразделе рассмотрен алгоритм цифровой подписи Эль-Гамаля.

Подпись для сообщения M вычисляется с помощью следующего алгоритма:

1) Выбрать случайное целое число r, $1 \le r \le p-2$, взаимно простое с $p-1$.

2) Вычислить $\gamma = g^r (mod\, p)$.

3) Для $x = M$ вычислить $\delta = (x - a\gamma) r^{-1} (mod\ (p-1))$.

4) Подписью для сообщения M положить пару (γ, δ).

Алгоритм проверки подписи заключается в проверке сравнения $\beta^\gamma \gamma^\delta \equiv g^x (mod\, p)$. Если оно верно, то подпись принимается, если нет, то отвергается.

В седьмом разделе, который называется «Скрытый канал», вводится определение скрытого канала и схема протокола скрытого канала.

Скрытый канал – тайный канал связи, по которому передаются сообщения, сами по себе не содержащие секретной информации.

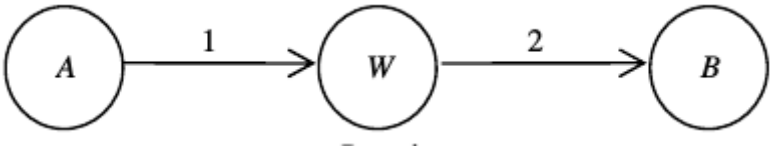

Рисунок 1 – Схема протокола

1.1. Алиса генерирует открытое (безобидное) сообщение;

1.2. Алиса подписывает невинное сообщение, используя секретный ключ, общий с Бобом, и пряча в подписи скрытое сообщение. (Это – ядро протокола скрытого канала);

1.3. Алиса отправляет с Уолтером подписанное сообщение Бобу;

2.1. Уолтер читает невинное сообщение и проверяет подпись;

2.2. Не встретив ничего подозрительного, Уолтер передает Бобу подписанное сообщение;

3.1. Боб проверяет подлинность подписи под невинным сообщением, убеждаясь, что сообщение поступило от Алисы, и не было изменено;

3.2. Боб игнорирует невинное сообщение и, используя секретный ключ, общий с Алисой, извлекает скрытое сообщение.

Восьмой раздел называется «Скрытый канал на основе схемы Эль-Гамаль» и является основным разделом дипломной работы. В этом разделе описана реализация скрытого канала на основе схемы Эль-Гамаль.

Генерация подписи абонентом A для открытого сообщения m:

1. Абонент A формирует t – скрываемое сообщение, $(k, p-1) = 1$, $1 < t < p-1$;

2. Абонент A вычисляет $\gamma = g^t (mod\ p)$;

3. Абонент A вычисляет $\delta = t^{-1}(m - a\gamma)(mod\ p-1)$, подписью являются γ и δ, который удовлетворяют уравнению $m = (a\gamma + t\delta)(mod\ p-1)$. Для скрытого канала должно выполняться дополнительное условие, числа $(m - a\gamma)$ и $(p-1)$ должны быть взаимнопростыми. Это условие выполнить несложно, поскольку m (безобидное сообщение) при необходимости всегда можно немного подправить;

$$A \to W(B): \{m, \gamma, \delta\}.$$

Проверка подписи:

1. Абонент W проверяет, что $\beta^\gamma \gamma^\delta (mod\ p) = g^m (mod\ p)$;

$$W \to B: \{m, \gamma, \delta\};$$

2. Абонент B проверяет, что $\beta^{\gamma}\gamma^{\delta}(mod\ p) = g^{m}(mod\ p)$.

Получение секретного сообщения:

Абонент B извлекает секретное сообщение, $t = \delta^{-1}(m - a\gamma)(mod\ p - 1)$.

В девятом разделе, который называется «Программная реализация» представлены примеры работы программ, реализованных по описанным алгоритмам.

В первом подразделе девятого раздела показаны сгенерированные ключи. На рисунках 5 и 6 представлены закрытый и открытый ключи, соответственно.

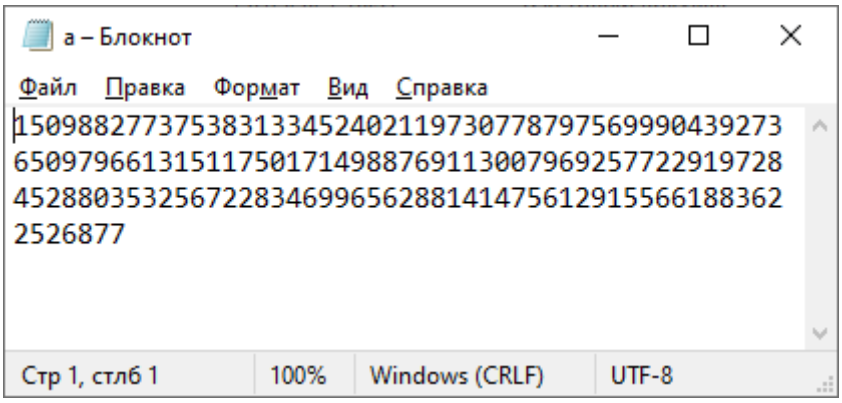

Рисунок 5 – Закрытый ключ

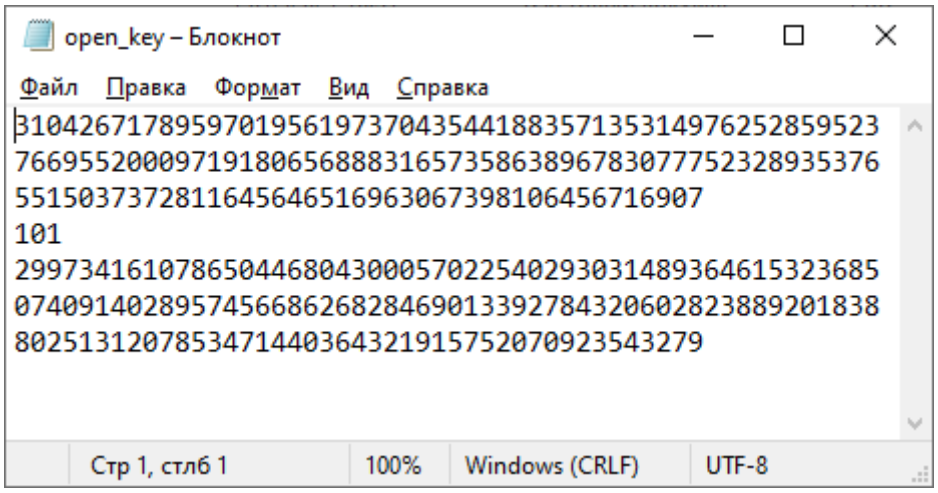

Рисунок 6 – Открытый ключ

Во втором подразделе девятого раздела показано шифрование, на основе схемы Эль-Гамаль. На рисунках 8 и 9 представлено сообщение в открытом и зашифрованном виде, соответственно.

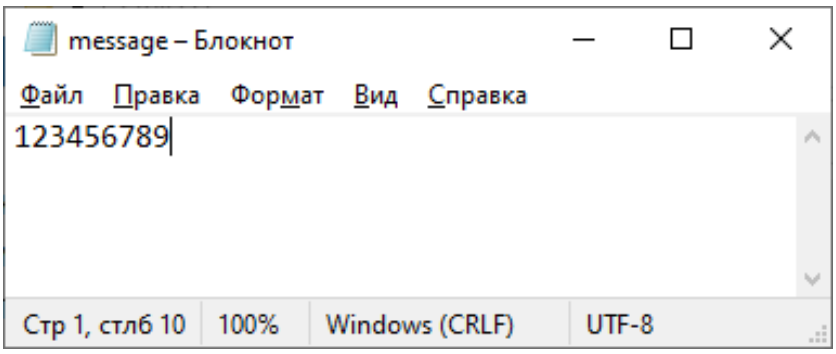

Рисунок 8 – Шифруемое сообщение

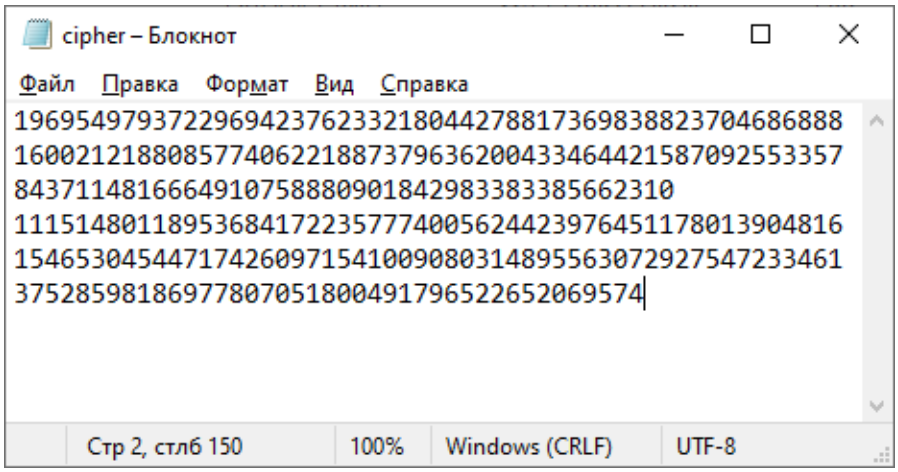

Рисунок 9 – Зашифрованное сообщение

В третьем подразделе девятого раздела показана сгенерированная цифровая подпись, на основе схемы Эль-Гамаль. На рисунке 17 представлено сообщение с подписью.

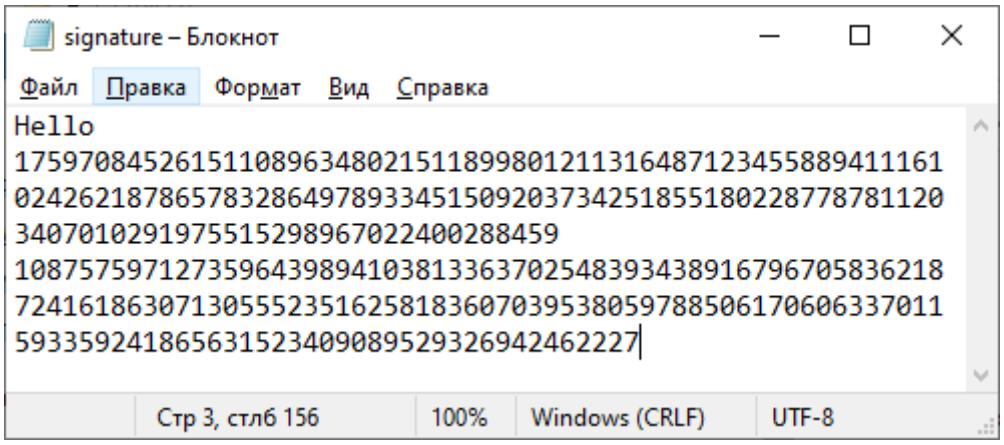

Рисунок 17 – Подписанное сообщение

В четвертом подразделе девятого раздела показана реализация скрытого канала на основе схемы Эль-Гамаль. На рисунке 24 представлено сообщение с подписью.

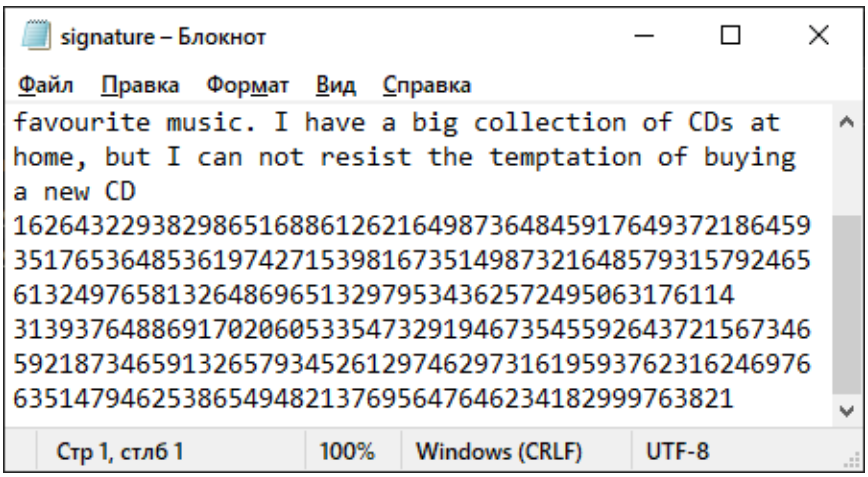

Рисунок 24 – Подписанное сообщение

При обычной проверке сообщения на подлинность, пользователь запускает программу, в окне выбора действия выбирает «0», после чего на экране появится соответствующее сообщение. На рисунке 25 представлено сообщение о подлинности подписи.

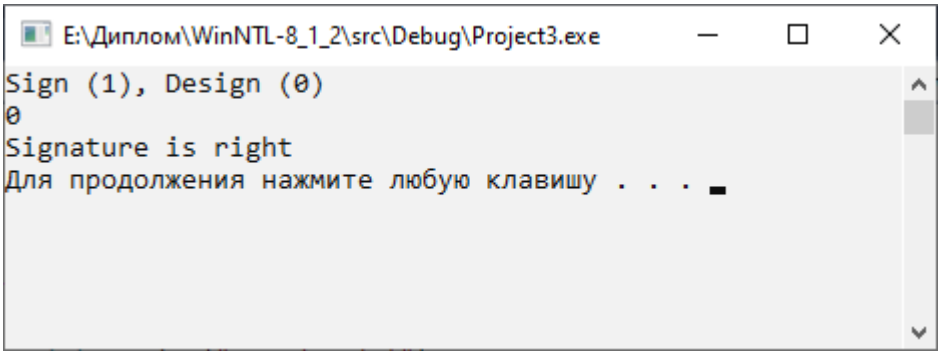

Рисунок 25 – Проверка подписи

Для того, что бы получить секретное сообщение, скрываемое в подписи, пользователь запускает программу, предоставляет закрытый ключ a и в окне выбора действия выбирает «0». На рисунке 26 представлено полученное секретное сообщение.

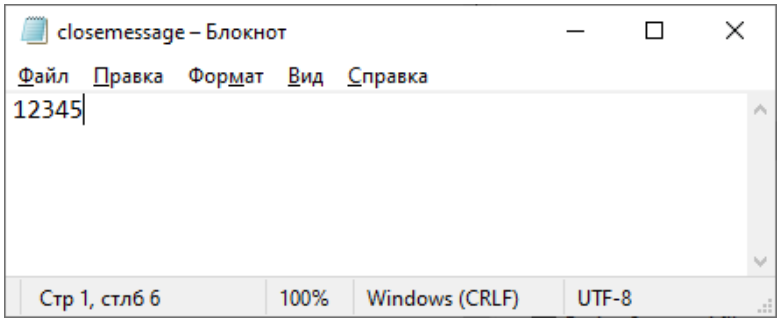

Рисунок 26 – Расшифрованное секретное сообщение

ЗАКЛЮЧЕНИЕ

Схема цифровой подписи Эль-Гамаля послужила образцом для построения большого семейства во многом сходных по своим свойствам схем подписи. В их основе лежит проверка сравнения вида

$$g^A \beta^B \equiv \gamma^C \pmod{p},$$

в котором тройка (A, B, C) совпадает с одной из перестановок $\pm x$, $\pm \delta$ и $\pm \gamma$ при некотором выборе знаков. Например, исходная схема получается при $A = x$, $B = -\gamma$ и $C = \delta$.

На базе схем подписи их этого семейства построены и стандарты цифровой подписи США и России. Так, в американском стандарте DSS (*Digital Signature Standart*) используются значения $A = x$, $B = \gamma$ и $C = \delta$, а в российском стандарте – значения $A = -x$, $B = \gamma$ и $C = \delta$.

В результате проделанной работы был разработан программный продукт по реализации скрытого канала на основе схемы Эль-Гамаль и программное обеспечение для реализации данной схемы.

В данной работе все поставленные цели были достигнуты и все поставленные задачи выполнены.