

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №51

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ _____

ПРЕПОДАВАТЕЛЬ

К.Т.Н., доцент

должность, уч. степень, звание

подпись, дата

Овчинников А.А.

инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №5

Алгоритмы с открытым ключом

по дисциплине: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ
ИНФОРМАЦИИ

СТУДЕНТ ГР. №

5912

номер группы

подпись, дата

Калташов В.А.

инициалы, фамилия

Санкт-Петербург, 2022

Цель работы

Реализовать криптосистему Эль-Гамала. При постановке подписи использовать хеш-функцию MD4.

Работа алгоритма

Схема Эль-Гамала является криптосистемой с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи.

Функции алгоритма

1. Генерация ключей

- Генерируется случайное простое число p
- Выбирается целое число g – первообразный корень p
- Выбирается случайное целое число x такое, что $(1 < x < p-1)$
- Вычисляется $y = g^x \bmod p$.
- Открытым ключом является (y, g, p) , закрытым ключом – число x .

2. Работа в режиме шифрования

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 $a = g^k \bmod p$ и $b = y^k M \bmod p$.

3. Пара чисел (a,b) является шифротекстом.

3. Работа в режиме расшифрования

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

$$M = b(a^x)^{-1} \bmod p.$$

При этом нетрудно проверить, что

$$(a^x)^{-1} = g^{-kx} \bmod p$$

4. Подпись сообщений

Для подписи сообщения M выполняются следующие операции:

- 1) Вычисляется $m = h(M)$. (В нашем случае хеш-функция MD4).
- 2) Выбирается случайное число $1 < k < p - 1$ взаимно простое с $p - 1$ и вычисляется $r = g^k \bmod p$.
- 3) Вычисляется число $s = (m - xr)k^{-1} \pmod{p - 1}$
- 4) Подписью сообщения M является пара (r,s) .

5. Проверка подписи

Зная открытый ключ (p, g, y) , подпись (r,s) сообщения M проверяется следующим образом:

- 1) Проверяется выполнимость условий $0 < r < p$ и $0 < s < p-1$.
- 2) Если хотя бы одно из них не выполняется, то подпись считается неверной.
- 3) Вычисляется $m = h(M)$.
- 4) Подпись считается верной, если выполняется сравнение:

$$y^r r^s = g^m \bmod p.$$

Пример работы программы.

```
M = 5, p = 11, g = 2, k = 9
e => d => 3
9
d => 3
r => 6
5
Result: -1
17 20 21
10 10
```

Рисунок 1. Работа программы

Вывод

Была реализована криптосистема Эль-Гамала. При постановке подписи использовали хеш-функцию MD4. Научились работать с алгоритмами с рабочим ключом.