

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

ассистент

М.Н.Исаева

должность, уч. степень,
звание

подпись, дата

инициалы,
фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №6

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Студент гр. №

5912

И.К. Лобач

номер
группы

подпись,
дата

инициалы,
фамилия

Санкт-Петербург 2022

Цель работы: реализация протокола идентификации Клауса Шнора.

1 Описание протокола

Протокол Шнора является одним из наиболее эффективным практическим протоколом аутентификации. В протоколе два участника – Алиса и Боб. Алиса должна доказать свою личность, а Боб, соответственно проверяет личность Алисы. У Алисы есть два ключа – общедоступный K_1 и секретный K_2 .

Для генерации ключей выбирается простое число p . Выбирается простое число q такое, что оно является делителем числа $p - 1$, т.е. $p - 1 = 0 \bmod q$. Затем выбирается число g , отличное от 1 и такое, что $g^q = 1 \bmod p$.

Алиса выбирает случайное целое число $w < q$ и вычисляет $y = g^{q-w} \bmod p$. Открытым ключом Алисы будет (p, q, g, y) , а секретным w .

2 Особенности реализации

- 1) Алиса выбирает случайное число $r < q$ и вычисляет $x = g^r \bmod p$.
- 2) Алиса посылает Бобу x
- 3) Боб выбирает случайное число e из диапазона $0 \dots 2^t - 1$ и отправляет его Алисе
- 4) Алиса вычисляет $s = r + we \bmod q$ и посылает s Бобу
- 5) Боб проверяет, что $x = g^s y^e \bmod p$

3 Пример работы программы

```
Генерация ключей:
p = 9967
q = 151
g = 117
w (private key) = 102
y (public key) = 5183

Реализция протокола идентификации:
r = 102
Алиса x = 2498

t = 652322890
e = 12635
s = 87
Боб x: 2498
```

Рисунок 1 - Пример работы программы

4 Выводы

Безопасность алгоритма зависит от параметра t . Сложность вскрытия алгоритма примерно равна 2^t . Рекомендуется использовать t около 72 бит, для $p \geq 2^{512}$ и $q \geq 2^{140}$. При таких значениях сложность будет около 2^{72} .

Список используемых источников:

- 1) Яценко В.В. Введение в криптографию. Под общей ред. В. В. Яценко — СПб.: Питер, 2001. - 288 с.