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. $p-1=0\ mod\ q$. Затем выбирается число g, отличное от 1 и такое, что $g^q=1\ mod\ p$.

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

2 Особенности реализации

1) Алиса выбирает случайное число $r<q$ и вычисляет $x=g^r mod\ p$.

2) Алиса посылает Бобу x

3) Боб выбирает случайное число e из диапазона $0\ldots 2^t-1$ и отправляет его Алисе

4) Алиса вычисляет $s=r+we\ mod\ q$ и посылает s Бобу

5) Боб проверяет, что $x=g^s y^e\ mod\ p$

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