1. **Задание:** реализация протокола аутентификации без разглашения Фиата-Шамира

2. **Аннотация:**

Протокол Фиата — Шамира — это один из наиболее известных протоколов идентификации с нулевым разглашением (Zero-knowledge protocol). Протокол был предложен Амосом Фиатом (англ.Amos Fiat) и Ади Шамиром (англ.Adi Shamir).

Пусть **A** знает некоторый секрет **s**. Необходимо доказать знание этого секрета некоторой стороне **B** без разглашения какой-либо секретной информации. Стойкость протокола основывается на сложности извлечения квадратного корня по модулю достаточно большого составного числа **n**, факторизация которого неизвестна.

Описание протокола

A доказывает **B** знание **s** в течение **t** раундов. Раунд называют также аккредитацией. Каждая аккредитация состоит из 3х этапов.

Предварительные действия

Доверенный центр **T** выбирает и публикует модуль $n=p*q$, где **p**, **q** — простые и держатся в секрете.

Каждый претендент **A** выбирает **s** взаимно-простое с **n**, где $s \in [1, n-1]$. Затем вычисляется $v = s^2 (mod\ n)$. **V** регистрируется **T** в качестве открытого ключа **A**.

Передаваемые сообщения (этапы каждой аккредитации)

$$A \Rightarrow\!\!\!\gg B: \; x = r^2 (mod\ n)$$

$$A \ll\!\!= B: \; e \in 0{,}1$$

$$A \Rightarrow\!\!\!\gg B: \; y = r * s^e (mod\ n)$$

Основные действия

Следующие действия последовательно и независимо выполняются **t** раз. **B** считает знание доказанным, если все t раундов прошли успешно.

- **A** выбирает случайное **r**, такое, что $r \in [1, n-1]$ и отсылает $x^2 = r$ стороне **B** (доказательство)

- **B** случайно выбирает бит **e** (**e**=0 или **e**=1) и отсылает его **A** (вызов)
- **A** вычисляет **y** и отправляет его обратно к **B**. Если ***e***=*0*, то $y = r$, иначе $y = r * s$ (ответ)
- Если ***y***=*0*, то **B** отвергает доказательство или, другими словами, **A** не удалось доказать знание **s**. В противном случае, сторона **B** проверяет, действительно ли $y^2 = x * v^e$ и, если это так, то происходит переход к следующему раунду протокола.

Выбор **e** из множества {0,1} предполагает, что если сторона А действительно знает секрет, то она всегда сможет правильно ответить, вне зависимости от выбранного e.

Достоинством многораундового протокола Фиата−Шамира является его сравнительно низкая вычислительная сложность − каждая из сторон участвующих в протоколе выполняет не более 2*z* модульных умножений, где *z* – заданное число раундов. Однако, существенным недостатком всех многораундовых протоколов является необходимость выполнения очень большого числа чередующихся пересылок сообщений от доказывающего к проверяющему и обратно.

3. Ход работы

Рассмотрим выполнение алгоритма на примере одного раунда:

Выбираем простое число p = 751 и простое число q = 317. Тогда произведение чисел n = p * q = 238067.

Вычисляем s и v такие, что s = 160915 – случайное число в диапазоне от 0 до n-1, взаимно простое с n. Тогда v = s^2 mod n = 41903. Далее А отсылает доказательство В: x = 41903. В выбирает случайное e = 1 и отсылает его А (вызов). А вычисляет y = 41903 и отправляет его В. Выполняется проверка условия: y^2 = 117284 и x * v^e = 117284.

Так как y^2= x*v^e – раунд 1-ый пройден успешно.

4. Контрольный пример

Количество раундов вводится пользователем в консоль:

Просто число p = 701

Простое число q = 389

Произведение чисел n = p * q = 272689

Введите количество **t - раундов**: 12

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 1-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 1 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 53173

x * v^e = 53173

Раунд 2-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 3-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 4-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 5-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 6-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 7-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

В выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 8-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 9-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 10-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 11-ый пройден успешно

s: 65812

v: 99957

A отсылает доказательство B: x = 99957

B выбирает e = 0 и отсылает его A (вызов)

A вычисляет y = 65812 и отправляет его B

y^2 = 99957

x * v^e = 99957

Раунд 12-ый пройден успешно

Таким образом, можно заметить, что все двенадцать раундов пройдены успешно. B удостоверяется в знании A.

5. Вывод:

В ходе выполнения лабораторной работы смоделирован протокол аутентификации взаимодействия при использовании схемы Фиата – Шамира с нулевым разглашением.