Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

ИДЕНТИФИКАЦИЯ С ПОМОЩЬЮ ПРОТОКОЛА ФЕЙГА – ФИАТА – ШАМИРА

Аннотация*: в данной статье рассматривается проверка подлинности с помощью с схемы Фейга – Фиата – Шамира.*

Ключевые слова*: идентификация, криптография, протокол, арбитр, закрытый ключ, открытый ключ.*

Введение

В современном мире часто необходимо удостовериться, что одна из сторон владеет информацией, но не раскрывая её содержания. Для решения данной задачи рассмотрим протокол Фейга, Фиата и Шамира для идентификации сторон, являющийся одним из наиболее известных доказательств с нулевым разглашением.

Основные определения

Введем некоторые определения, которые будут использованы в работе.

1. Протокол – это порядок действий, предпринимаемых двумя или более сторонами, предназначенный для решения определенной задачи.

2. Простое число – натуральное число, большее единицы, имеющее ровно два натуральных делителя: 1 и само себя.

3. Доказательство с нулевым разглашением знания – интерактивный криптографический протокол, позволяющий одной из интерактивных сторон убедиться в достоверности какого-либо утверждения, не имея при этом никакой другой информации от второй стороны

Генерация ключей

1. На первоначальном этапе *арбитр,* которому доверяют обе стороны, выбирает случайный модуль n, который является произведением двух больших простых чисел $n = p \cdot q$, где числа p,q простые. Число n является открытым, а числа p, q – секретными.

2. Для генерации открытого и закрытого ключа *Алиса* выбирает последовательность из k случайных целых чисел $v_1, v_2, ..., v_k$, $1 \le v_i \le n-1$ и каждое v_i – квадратичный остаток по модулю n, то есть необходимо чтобы $x^2 \equiv v_i (\mathrm{mod}\, n)$ имело решение, и существовало $v_i^{-1} \bmod n$. Последовательность $v_1, v_2, ..., v_k$ называется открытым ключом.

3. Вычисляется последовательность $s_1, s_2, ..., s_k$, в которой $s_i \equiv sqrt(v_i^{-1}) (\mathrm{mod}\, n)$ Данная последовательность называется закрытым ключом.

Работа протокола

1. *Алиса*: Выбирает случайное целое число r, $1 \le \kappa \le n-1$ и вычисляет $x = -r^2 (\mathrm{mod}\, n)$ и отправляет x *Бобу*

2. *Боб*: Посылает *Алисе* набор k случайных битов: $b_1, b_2, ..., b_k$

3. *Алиса*: Вычисляет $y = r \cdot \prod_{i=1}^{k} s_i^{b_i} (\mathrm{mod}\, n)$. Таким образом, если случайный бит $b_i = 1$, то s_i войдет в произведение, иначе $b_i = 0$ и s_i не войдет в произведение.

4. *Боб*: Проверяет, что $x = y^2 \cdot \prod_{i=1}^{k} v_i^{b_i}$

Протокол повторяется несколько раундов до тех пор пока *Боб* не убедится в том, что *Алиса* действительно знает последовательность $s_1, s_2, ..., s_k$. Вероятность успешной атаки на протокол путем подбора значений b_i из последовательности $b_1, b_2, ..., b_k$ составляет $\left(\frac{1}{2}\right)^{kt}$. Для того, чтобы снизить вероятность успешной рекомендуется использовать параметры k = 5 и t =4, таким образом вероятность успешной атаки на протокол равна $\left(\frac{1}{2}\right)^{20}$.

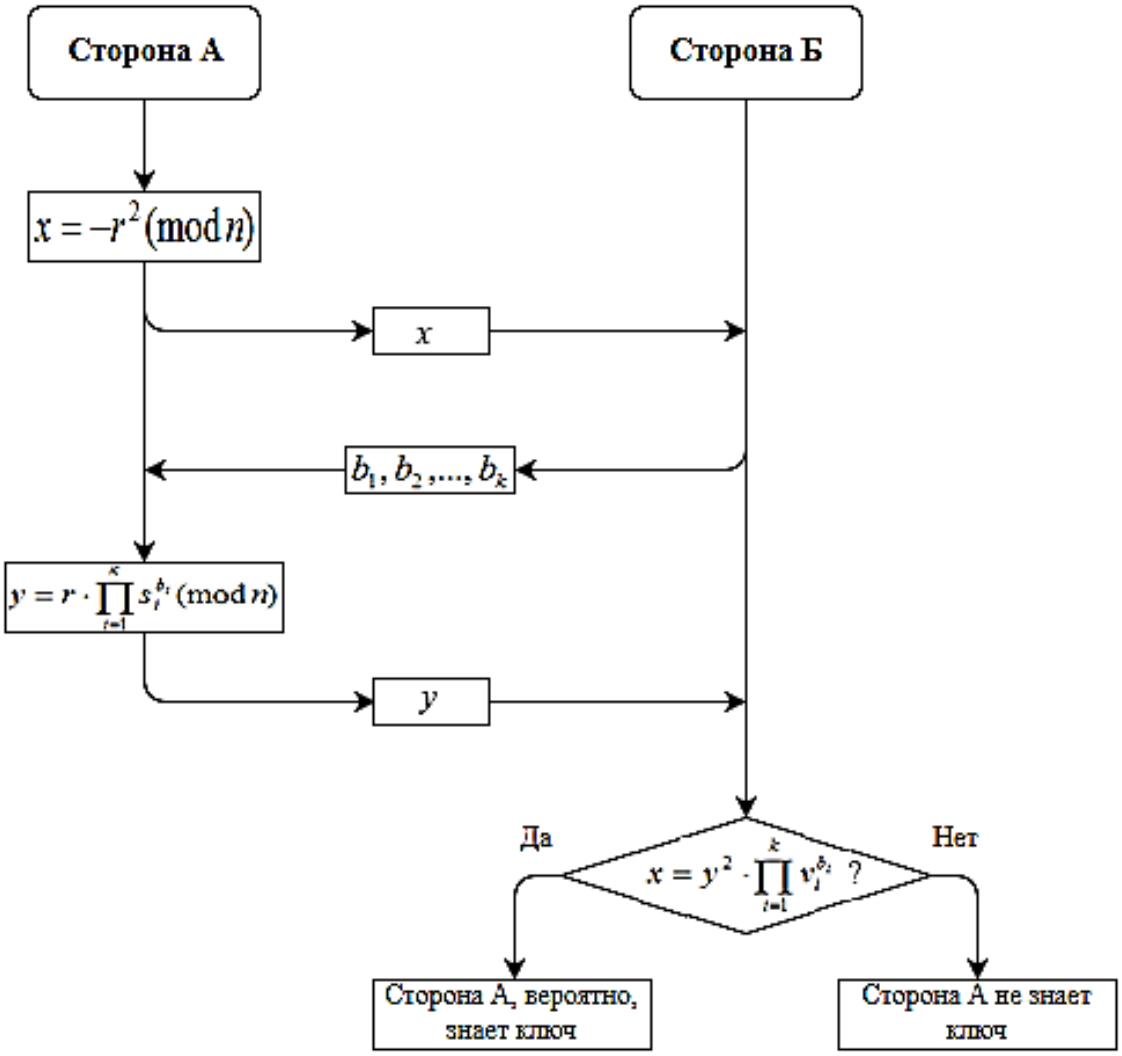

Рис. 1. Схема работы протокола

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.