МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ компьютерной безопасности и криптографии

**Схема аутентификации Фейге – Фиата – Шамира**

ОТЧЁТ

ПО ДИСЦИПЛИНЕ

«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

студента 5 курса 531 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

|  |  |  |
| --- | --- | --- |
| Преподаватель, доцент | \_\_\_\_\_\_\_\_\_\_ | В.E. Новиков |
|  | подпись, дата |  |

Саратов 2024

**Алгоритм аутентификации Фейге – Фиата – Шамира**

Протокол Фейга — Фиата — Шамира — протокол аутентификации с нулевым разглашением, обобщение более раннего протокола Фиата — Шамира, разработанный Уриэлем Фейге, Амосом Фиатом и Ади Шамиром в 1986 году.

Протокол позволяет одному участнику (доказывающему A) доказать другому участнику (проверяющему B), что он обладает секретной информацией, не раскрывая ни единого бита этой информации.

Безопасность протокола основана на сложности извлечения квадратного корня по модулю достаточно большого составного числа n, факторизация которого неизвестна.

**Выбор параметров системы**

Доверенный центр публикует большое число , где и простые числа, которые держаться в секрете. Также выбираются параметры безопасности и (– это количество раундов, но в нашей реализации он не имеет значения, так как мы выполняем шаги последовательно в итеративном режиме).

**Генерация секретов для участников**

Каждый участник выбирает случайных целых чисел и случайных бит

Затем вычисляет

Участник идентифицирует себя окружающим с помощью значений , которые выступают в качестве его открытого ключа, в то время как секретный ключ известен только самому участнику (в нашем случае в качестве участника будет выступать Алиса).

**Действия протокола в рамках одного раунда**

1. Алиса выбирает случайное целое число вычисляет: и отправляет Бобу.
2. Боб отправляет Алисе случайный битный вектор , где или .
3. Алиса вычисляет и отправляет Бобу: .
4. Боб вычисляет: и проверяет, что и . (Если это условие выполняется то, то Алиса смогла доказать Бобу тот факт, что она что-то знает).