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 Гиллу – Кискате**

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

**Описание протокола:**

Схема аутентификации Guillou-Quisquater Пегги – это интеллектуальная карточка, которая собирается доказать свою подлинность Виктору. Идентификация Пегги проводится по ряду атрибутов, представляющих собой строку данных, содержащих название карточки, период действия, номер банковского счета и другие, подтверждаемые ее применимость, данные. Эта битовая строка называется 𝐽. (В реальности строка атрибутов может быть очень длинной, и в качестве 𝐽 используется ее хэш-значение. Это усложнение никак не влияет на протокол).

Сторона отправляет стороне свои атрибуты . Стороне необходимо убедить сторону , что это именно её атрибуты. Для этого сторона доказывает своё знание секрета стороне , не раскрывая при этом ни одного бита самого секрета

**Алгоритм создания открытого и закрытого ключей**

1. Центр доверия выбирает два различных случайных простых чисел и , после чего вычисляет их произведение .
2. выбирает целое число (), взаимно простое со значением функции Функция является функцией Эйлера.
3. вычисляет и секрет
4. вычисляет
5. Тройка публикуется в качестве открытого ключа.
6. играет роль закрытого ключа, и передается стороне .

**Обмен сообщениями (аутентификация пользователя)**

1. выбирает случайное целое находящееся в диапазоне от 1 до вычисляет и отправляет его .
2. выбирает случайное целое , находящееся в диапазоне от 0 до посылает стороне .
3. вычисляет и посылает его .
4. проверяет: если то подлинность доказана.

Математика не слишком сложна: