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

**Аутентификация по программе SKEY**

**(на основе однонаправленных функций)**

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 S/Key, основанный на одноразовых паролях и описанный в RFC 1760, представляет собой надежную схему аутентификации для удаленных пользователей. Основные этапы его работы включают инициализацию списка одноразовых паролей с использованием односторонней хеш-функции (обычно MD4 или MD5), передачу одноразового пароля по сети в открытом виде и проверку на сервере. Преимущество этой схемы в том, что каждый пароль используется только один раз, что делает перехват пароля бесполезным для злоумышленника.

**Описание протокола**

1. **Инициализация:**
   1. Сервер генерирует случайный ключ для пользователя.

1.2 Сервер генерирует список заданной длины одноразовых паролей (количество паролей для каждого пользователя определяется на сервере), применяя хеш-функцию к этому ключу многократно. Например, для одноразовых паролей выполняются итерация хеш-функции:

1.3 Секретный ключ , а также начальные параметры и (номер текущего одноразового пароля) хранятся на сервере. Предварительно также необходимо передать ключ пользователю.

**2. Создание хэш значения пользователем при заданном и**

2.1 При каждом сеансе аутентификации сервер отправляет пользователю значение .

2.2 Пользователь вычисляет пароль путём  многократного применения хеш-функции к своему ключу и значению :

2.3 Пользователь отправляет на сервер

**3. Аутентификация**

3.1 Сервер проверяет его, применяя хеш-функцию один раз: и сравнивает с сохранённым ​. Если значения совпадают, аутентификация успешна.

3.2 После успешной аутентификации заменяется на, а уменьшается на единицу.