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 подписи 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

Схему аутентификацииГиллу – Кискате можно превратить в схему подписи. Открытый и закрытый ключи не меняются и генерируются следующим образом:

**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 .

**Подпись сообщения**

Пусть хочет подписать сообщение .

1. выбирает случайное целое , находящееся в диапазоне от 1 до вычисляет
2. вычисляет где подписываемое сообщение, a однонаправленная хэш-функция. Значение , полученное с помощью хэш-функции, должно быть в диапазоне от 0 до Если выход хэш-функции выходит за этот диапазон, он должен быть приведен по модулю .
3. вычисляет Подпись состоит из сообщения двух вычисленных значений , и ее атрибутов . посылает подпись

**Проверка подписи**

Пусть хочет проверить подпись.

1. вычисляет Затем он вычисляет Если то знает и ее подпись действительна.