МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		М.Н. Исаева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912		В.И.Исаева
	подпись, дата	инициалы, фамилия

Санкт-Петербург
2022

Задача

Вариант 2.

Реализовать протокол идентификации Guillou-Quisquater.

Требования к работе:

- Разработка двух независимых модулей-участников протокола.
- Реализация должна позволять попытки ложной аутентификации.
- Количество раундов протокола должно быть параметром схемы.

Тестируемый алгоритм

Guillou-Quisquater представляет собой интерактивный протокол, который позволяет доказать, что доказываемое утверждение верно, и доказывающий знает это доказательство, в то же время не предоставляя никакой информации о самом доказательстве данного утверждения. Данный криптографический протокол обладает тремя свойствами:

1. *Полнота*: если утверждение действительно верно, то доказывающий убедит в этом проверяющего с любой наперед заданной точностью.
2. *Корректность*: если утверждение неверно, то любой, даже «нечестный», доказывающий не сможет убедить проверяющего.
3. *Нулевое разглашение*: если утверждение верно, то любой, даже «нечестный», проверяющий не узнает ничего кроме самого факта, что утверждение верно.

Описание алгоритма

Протокол Guillou-Quisquater требует только один раунд обмена сообщениями и состоит из трёх этапов. Схематично их можно изобразить следующим образом:

A=>B: доказательство
A<=B: вызов
A=>B: ответ

Сначала A выбирает из заранее определённого непустого множества некоторый элемент, который становится её секретом — закрытым ключом. По этому элементу вычисляется, а затем публикуется открытый ключ. Знание секрета определяет множество вопросов, на которые A всегда сможет дать правильные ответы. Затем A выбирает случайный элемент из множества, по определённым правилам вычисляет доказательство и затем отсылает его B. После этого B выбирает из всего множества вопросов один и просит A ответить на него (вызов). В зависимости от вопроса, A посылает B ответ. Полученной информации B достаточно, чтобы проверить

действительно ли A владеет секретом.

Схема идентификации:
Сторона A отправляет стороне B свои атрибуты J. Стороне A необходимо убедить сторону B, что это именно ее атрибуты. Для этого сторона A доказывает свое знание секрета x стороне B, не раскрывая при этом ни одного бита самого секрета x. Для этого сторонам потребуется всего 1 раунд.

Алгоритм создания открытого и закрытого ключей:

1. Центр доверия T выбирает два различных случайных простых числа p и q, после чего вычисляет их произведение n = p * q
2. T выбирает целое число e (1 < e < φ(n)), взаимно простое со значением функции φ(n).
3. T вычисляет $s = e^{-1} \ mod \ \varphi(n)$ и секрет $x = J^{-s} \ mod \ n$
4. T вычисляет $y = x^e \ mod \ n$
5. Тройка {n, e, y} публикуется в качестве открытого ключа.
6. *x* играет роль закрытого ключа и передается стороне A

Обмен сообщениями:

1. A выбирает случайное целое r, находящееся в диапазоне от 1 до n-1. A вычисляет $a = r^e \ mod \ n$ и отправляет его B.
2. B выбирает случайное целое c, находящееся в диапазоне от 0 до e-1. B посылает c стороне A.
3. A вычисляет $z = rx^c \ mod \ n$ и отправляет его B.
4. B проверяет: если $z^e = ay^c \ mod \ n$, то подлинность доказана.

Обмен сообщениями можно повторять заданное количество раундов, чтобы избежать случайного попадания в секретный ключ.

Пример использования алгоритма

Атрибуты J: «sign»

Количество раундов: 3

```
n = 729372856524577593533940741287815244069170049818090486522364612496518262635 29
e = 996688033963263973292988266840726052948577230249411484734327635764587658416078004491357204106499889994045437323569944947585137151516371677630785330657670 3
x = 652946780528333349009657746260722314924165749287362078387819674834704693844 80
y = 388567331318383524536843210160896550406959728009106040035504275502366882085 97
B -> True
A <- good true
B -> True
A <- good true
B -> True
A <- good true
A <- very good true
```

Изменим секретный ключ x и проверим:

```
n = 729372856524577593533940741287815244069170049818090486522364612496518262635 29
e = 996688033963263973292988266840726052948577230249411484734327635764587658416078004491357204106499889994045437323569944947585137151516371677630785330657670 3
x = 652946780528333349009657746260722314924165749287362078387819674834704693843 80
y = 388567331318383524536843210160896550406959728009106040035504275502366882085 97
B -> False
A <- bad false
```

Вывод

В данной лабораторной работе был реализован протокол идентификации Guillou-Quisquater, который позволяет доказать подлинность сообщения без передачи секретного ключа. Ключ зависит от атрибутов, задаваемых пользователем (данные банковской карты, паспорт), которые потом обрабатываются хеш-функцией. Поэтому при попытке взлома протокол достаточно быстро и просто вычислит попытку атаки, а дополнительные раунды помогут избежать случайных прохождений теста.