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 О ЛАБОРАТОРНОЙ РАБОТЕ №6

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

по курсу: Криптографические методы защиты информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №	5912		Ю.Г. Иванова
		подпись, дата	инициалы, фамилия

Санкт-Петербург 2022

ЦЕЛЬ РАБОТЫ: реализовать схему разделения секрета Шамира.

Разработка двух независимых модулей:

- первый должен принимать на вход секрет и возвращать его проекции,
- второй должен брать проекции и возвращать секрет.

1. Описание криптографической системы.

Схема разделения секрета Шамира (схема интерполяционных полиномов Лагранжа) — схема разделения секрета, широко используемая в криптографии. Схема Шамира позволяет реализовать (k, n) — пороговое разделение секретного сообщения (секрета) между n сторонами так, чтобы только любые k и более сторон ($k \leq n$) могли восстановить секрет. При этом любые k-1 и менее сторон не смогут восстановить секрет.

1.1. Подготовительная фаза.

Пусть нужно разделить секрет M между n сторонами таким образом, чтобы любые k участников могли бы восстановить секрет (то есть нужно реализовать (k, n)-пороговую схему).

Выберем некоторое простое число $p > M$. Это число можно открыто сообщать всем участникам. Оно задаёт конечное поле размера p. Над этим полем построим многочлен степени k-1 (то есть случайно выберем все коэффициенты многочлена, кроме M):

$$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1x + M) \bmod p$$

В этом многочлене M — это разделяемый секрет, а остальные коэффициенты $a_{k-1}x^{k-1}$, $a_{k-2}x^{k-2}$, … , a_1x — некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

1.2. Генерация долей секрета.

Теперь вычисляем «доли» — значения построенного выше многочлена, в n различных точках, причём ($x \neq 0$):

$$k_1 = F(1) = (a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \ldots + a_1 \cdot 1 + M) \bmod p$$

$$k_2 = F(2) = (a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + \ldots + a_1 \cdot 2 + M) \bmod p$$

…

$$k_i = F(i) = (a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + \ldots + a_1 \cdot i + M) \bmod p$$

…

$k_n = F(n) = (a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \ldots + a_1 \cdot n + M) \bmod p$

Аргументы многочлена (номера секретов) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдаётся доля секрета k_i вместе с номером i.

Помимо этого, всем сторонам сообщается степень многочлена k-1 и размер поля p. Случайные коэффициенты a_{k-1}, a_{k-2}, … , a_1 и сам секрет M «забываются».

1.3. Восстановление секрета.

Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет.

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных k-1 долей оценивается как p^{-1}. То есть в результате интерполяции по k-1 точке секретом может быть любой элемент поля с равной вероятностью. При этом попытка полного перебора всех возможных теней не позволит злоумышленникам получить дополнительную информацию о секрете.

Прямолинейное восстановление коэффициентов многочлена через решение системы уравнений можно заменить на вычисление интерполяционного многочлена Лагранжа (отсюда одно из названий метода). Формула многочлена будет выглядеть следующим образом:

$$F(x) = \sum_i l_i(x) y_i \mod p$$

$$l(x) = \prod_{i \neq j} \frac{x - x_i}{x_i - x_j} \mod p$$

где (x_i, y_i) — координаты точек многочлена. Все операции выполняются также в конечном поле p.

2. Пример работы программы.

2.1. Тест 1.

```
P = 95881
K = 4
Секрет: 18121

Многочлен: 22641*x^3 + 7575*x^2 + 17715*x^1 + 18121*x^0

Пользователь 1: 66052
Пользователь 2: 73217
Пользователь 3: 79581
Пользователь 4: 29228
Пользователь 5: 58004

2 --> 73217
3 --> 79581
1 --> 66052
4 --> 29228

18121
Секрет найден!
```

2.2. Тест 2.

```
P = 48259
K = 4
Секрет: 18284

Многочлен: 13391*x^3 + 16048*x^2 + 30847*x^1 + 18284*x^0

Пользователь 1: 30311
Пользователь 2: 10003
Пользователь 3: 37706
Пользователь 4: 730
Пользователь 5: 27680
Пользователь 6: 5866
Пользователь 7: 15634
Пользователь 8: 40812
Пользователь 9: 16969
Пользователь 10: 24451

1 --> 30311
7 --> 15634
6 --> 5866
4 --> 730

18284
Секрет найден!
```

2.3.Тест 3.

```
P = 11273
K = 4
Секрет: 6554

Многочлен: 8358*x^3 + 5432*x^2 + 630*x^1 + 6554*x^0

Пользователь 1: 9701
Пользователь 2: 6222
Пользователь 3: 1173

2 --> 6222
3 --> 1173
1 --> 9701
2 --> 6222

Секрет не найден!!!!!!
```

ВЫВОД.

В результате выполнения лабораторной работы была реализована схема разделения секрета Шамира, состоящая из двух модулей:

- первый принимает на вход секрет и возвращать его проекции,
- второй берет проекции и возвращать секрет.

Данная схема нашла применение в аппаратных криптографических модулях, где она используется для многопользовательской авторизации в инфраструктуре открытых ключей.

Также схема используется в цифровой стеганографии для скрытой передачи информации в цифровых изображениях, для противодействия атакам по сторонним каналам при реализации алгоритма AES.

Помимо этого, с помощью схемы Шамира может осуществляться нанесение цифрового водяного знака при передаче цифрового видео и генерация персонального криптографического ключа, используемого в биометрических системах аутентификации.