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 разделения секрета Карнина-Грина-Хеллмана**

ОТЧЁТ

ПО ДИСЦИПЛИНЕ

«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

студента 5 курса 531 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Норикова Павла Сергеевича

|  |  |  |
| --- | --- | --- |
| Преподаватель  аспирант | \_\_\_\_\_\_\_\_\_\_ | Р. А. Фарахутдинов |
|  | подпись, дата |  |

Саратов 2023

**ВВЕДЕНИЕ**

Цель работы – изучение и реализация схемы разделения секрета Карнина-Грина-Хеллмана.

**1 Теория**

Разделение секрета — термин в криптографии, под которым понимают любой из способов распределения секрета среди группы участников, каждому из которых достаётся своя некая доля. Секрет может воссоздать только коалиция участников из первоначальной группы, причём входить в коалицию должно не менее некоторого изначально известного их числа.

* 1. **Описание алгоритма**

Выбирается таких -мерных векторов , что ранг любой матрицы размером , образованной из этих векторов, равен . Вектор – это вектор размерности .

Секрет –это матричное произведение . Долями секрета являются произведения , где меняется от до .

Любые долей можно использовать для решения системы линейных уравнений размерности , неизвестными являются коэффициенты . известно всем, остальные известны -м участникам.

Восстановление секрета происходит с помощью решения СЛУ из уравнений и неизвестных относительно компонент вектора :

Получив решение , нужно вычислить . Это значение и будет секретом .

**2 Практическая реализация**

**2.1 Описание программы**

Функция *gen\_v* при помощи функции *gram\_schmidt* генерирует ЛНЗ векторы.

На вход программе подается количество участников *n* и минимальное количество участников для раскрытия секрета *m*.

**2.2 Тестирование программы**

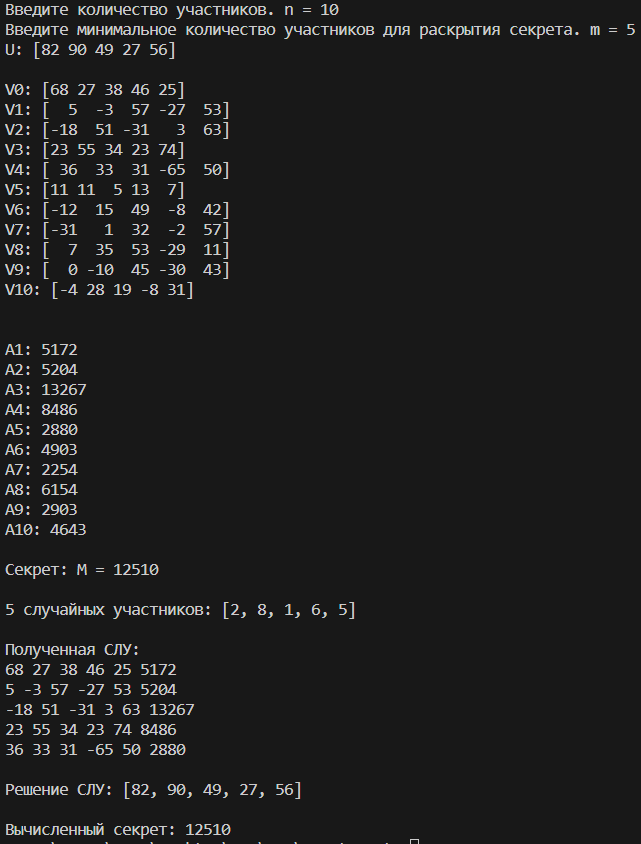


Рисунок 1 - Работа протокола

**ПРИЛОЖЕНИЕ А**

**Листинг программы**

import numpy as np

import random as rand

def gram\_schmidt(vectors):

basis = []

for vector in vectors:

for existing\_vector in basis:

vector -= np.dot(vector, existing\_vector) // np.dot(existing\_vector, existing\_vector) \* existing\_vector

basis.append(vector)

return basis

def gen\_v(n, t, integer\_range=(1, 100)):

random\_vectors = []

while len(random\_vectors) < n + 2:

random\_vector = np.random.randint(integer\_range[0], integer\_range[1] + 1, size=t)

random\_vectors.append(random\_vector)

random\_vectors = gram\_schmidt(random\_vectors)

return random\_vectors

def main():

n = int(input('Введите количество участников. n = '))

m = int(input('Введите минимальное количество участников для раскрытия секрета. m = '))

V = gen\_v(n, m)

U = V[0]

V = V[1:]

print('U:', U, '\n')

for i, vector in enumerate(V):

print(f"V{i}: {vector}")

print('\n')

A\_i = []

for i in range(1, len(V)):

A\_i.append(np.dot(U, V[i]))

print(f"A{i}: {A\_i[i-1]}")

M = np.matmul(U, V[0])

print('\nСекрет: M =', M, '\n')

all\_members = list(range(1, n))

members = []

matrix = []

vector = []

for \_ in range(m):

x = rand.choice(all\_members)

matrix.append(V[x])

vector.append(A\_i[x-1])

members.append(x)

all\_members.remove(x)

print(m, 'случайных участников:', members, '\n')

print('Полученная СЛУ:')

for i in range(m):

for j in range(m):

print(V[i][j], end = ' ')

print(A\_i[i])

res = np.linalg.solve(matrix, vector)

#print(res)

res = [round(x) for x in res]

print('\nРешение СЛУ:', res)

UV0 = round(np.matmul(res, V[0]))

print('\nВычисленный секрет:', UV0)

main()