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

к.т.н., доцент		Овчинников А.А.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №6

Криптографичекие протоколы

по дисциплине: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАШИТЫ ИНФОРМАЦИИ

СТУДЕНТ ГР. №	5912		Калташов В.А.
	номер группы	подпись, дата	инициалы, фамилия

Санкт-Петербург, 2022

Цель работы

Реализовать схему разделения секрета на китайской теореме об остатках.

Описание:

Реализуем схему разделения секрета по схеме Асмута – Блума.
Совместное использование секрета состоит в восстановлении секрета S из набора общих ресурсов, каждый из которых содержит частичную информацию о секрете. Китайская теорема об остатках (CRT) утверждает, чтодля данной системы уравнений решение уникально в некотором **Z**/n**Z**, при n>0. Таким образом, совместное использование секретов может использовать китайскую теорему об остатках для получения общих ресурсов, представленных в уравнениях, и секрет может быть восстановлен путем решения системы сравнений, чтобы получить уникальное решение, которое будет секретом для восстановления.

Генерируем последовательность попарно взаимно простых чисел $m_0<...<m_n$ таких что $m_0 * m_{n-k+2} ... m_n<m_1 ... m_k$.

```
m[0]                    =
generate_prime(bitsize)
m[1]                    =
generate_prime(bitsize)
m[2]                    =
generate_prime(bitsize)
m[3]                    =
generate_prime(bitsize)
m[4]                    =
generate_prime(bitsize)


m = sorted(m)


while (m[1] * m[2] * m[3] < m[0] * m[3] * m[4]) and m[4] <
    m[3]:m[4] = generate_prime(bitsize)
```

Затем генерируется случайное целое α такое что $S + \alpha * m_0<m_1 ... m_k$. $S + \alpha * m_0$это выражение вычисляется по модулю m_i, где i от 1 до n. Полученные доли используются для китайской теоремы об остатках.

```
alpha = randint(1, M)


share[0] = (secret + alpha * m[0]) %
m[1]share[1] = (secret + alpha *
m[0]) % m[2]share[2] = (secret +
alpha * m[0]) % m[3] share[3] =
(secret + alpha * m[0]) % m[4]
```

Решив эту систему, получаем секрет.

Пример работы:

Secret: 17

Alpha: 704601010767810484922871477241115907

Prime0: 783899930018202523

Prime1: 859188296676368179

Prime2: 993940184354624107

Prime3: 1002040666611397913

Prime4: 1065236065983982441

Share 1 (s1,m1): 87172455285473130 859188296676368179

Share 2 (s2,m2): 822509133021010391 993940184354624107

Share 3 (s3,m3): 617288263902291362 1002040666611397913

Share 4 (s4,m4): 540875680731115707 1065236065983982441

Public part (m0): 783899930018202523

Now using the first three shares and

solve CRTSecret: 17

Вывод:

Поскольку китайская теорема об остатках предоставляет нам метод однозначного определения чисел по модулю относительно простых целых чисел, идея состоит в том, чтобы построить схему, которая определит секрет S с учетом любых k долей (в данном случае остаток от S по модулю каждого из чисел m_i), но не раскроет секрет S, которому дано менее k долей.