1. Министерство высшего образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 1**

«**МАТЕМАТИЧЕСКИЕ ПРИМИТИВЫ КРИПТОГРАФИИ**»

1. по дисциплине «Основы Информационной Безопасности»
2. Выполнил
3. студент гр. Белоконь Д. А.
4. <*подпись*>

Проверил Пахомов М. А.

1. <*подпись*>

1. Санкт-Петербург
2. 2023
3. **Цель работы**

Приобретение базовых знаний в области криптографии.

Формулировка задания

Необходимо вручную посчитать несколько примеров на алгоритм Евклида, зашифровать и расшифровать текст по алгоритму RSA и смоделировать «на бумаге» установление сеансового ключа. После этого нужно разработать утилиту для алгоритма Меркля-Хеллмана.

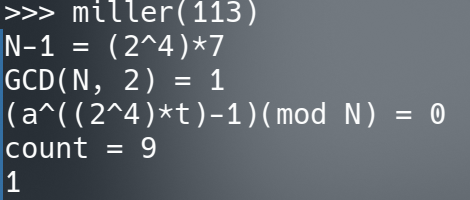
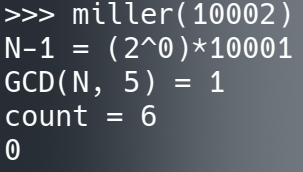
Результаты

Пойдём по инструкции. ((2+1)11+13)(mod 11) = (31 + 13)(mod 11) + 2 = ((27 mod 11)3 \* 9 + 13)(mod 11) = (53 \* 9 + 13)(mod 11) = (125 \* 9 + 13)(mod 11) = (4 \* 9 + 2)(mod 11) = 38 mod 11 = 5.

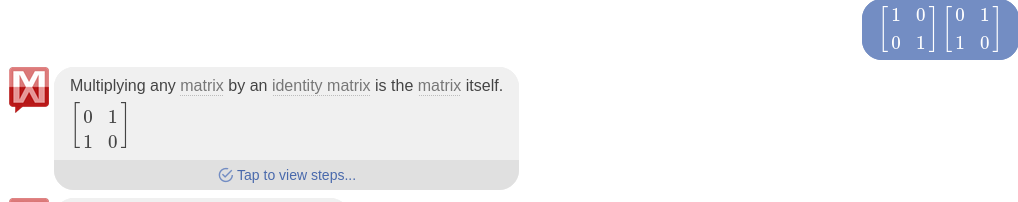
Цезарь: Курицов Сыр Салатович при k = 1, m = 33. Получается Лфсйчпг Тьс Тбмбупгйш — шифр греческий (с сыром и оливками).

A = (2 (8 + 1 (mod 7)))2 = (2 \* 9)2 = 4 \* 81 = 4 + 320 = 324. B = 10082004 = 10082004… НОД(А, B(mod 95) + 900), НОД(А, (В + 50)(mod 97) + 700), НОД(А, (B+20)(mod 101) + 1500, (B — 40)(mod 103) + 2500). Всё это в приложении.

Миллер: N = 10002, N1 = 113.

Штюрлиц: p = 101, q = 103. n = 10403, ф(n) = 10200. e = 13.

a = 13, b = 10200 => q = 0, r = 13.

a = 10200, b = 13 => q = 784, r = 8.

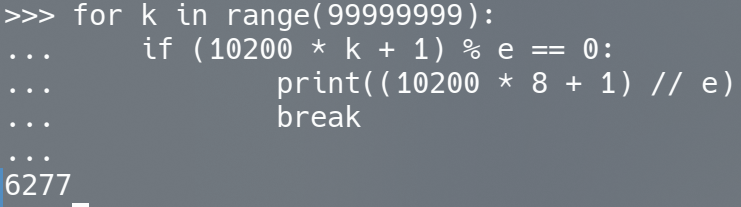
a = 13, b = 8 => q = 1, r = 5.

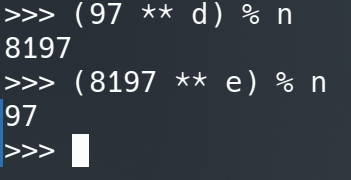
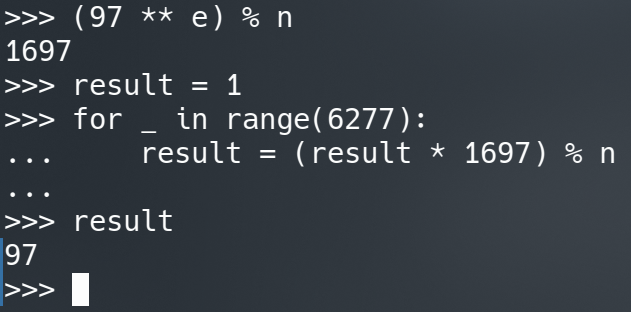
 a = 8, b = 5 => q = 1, r = 3.

a = 5, b = 3 => q = 1, r = 2.

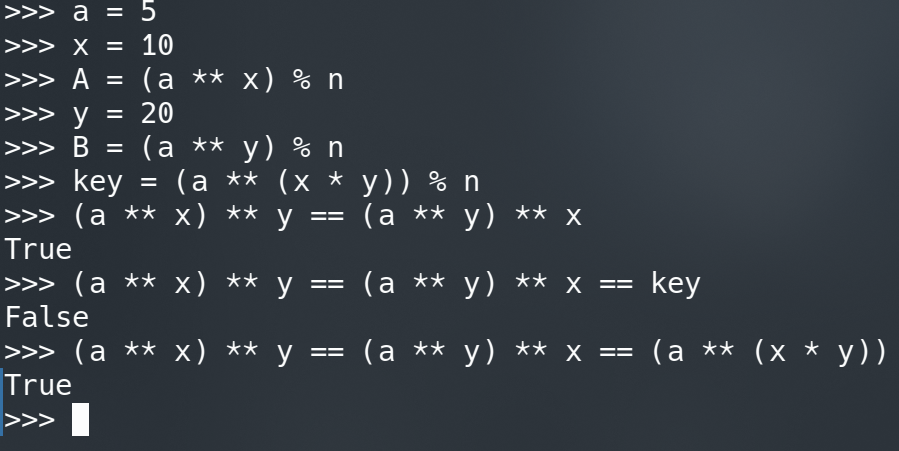
a = 3, b = 2 => q = 1, r = 1.

a = 2, b = 1 => q = 2, r = 0 => e \* (-3923) + ф(n) \* 5 = 1 => d = -3923. Это верно, но такой результат не удовлетворителен. Поэтому пойдём нормальным путём:

Проверяем:



А теперь сеансовые ключи:



Вывод

Это было очень забавным погружением в базовые алгоритмы шифрования. В ходе него было получено много информации об отсутствии каких-либо нормальный объяснений в Интернете.

**Приложение**

