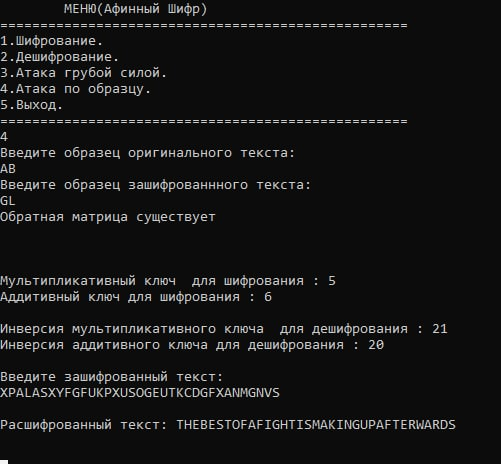
## Билет №16

(Шифр Афинный стр. 85)

Аффинный шифр. При заданном тексте и модуле выполнить шифрование/дешифрование, атаку грубой силы и/или по образцу.

* Описать алгоритмы шифрования, дешифрования, уязвимости и возможные атаки.
* Написать программу и расшифровать текст «XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS», если известны n = 26 и образцы - ab ⇔ GL.



Файл: afinnyi.cpp

## Билет №18

(Шифр Хилла стр. 96)

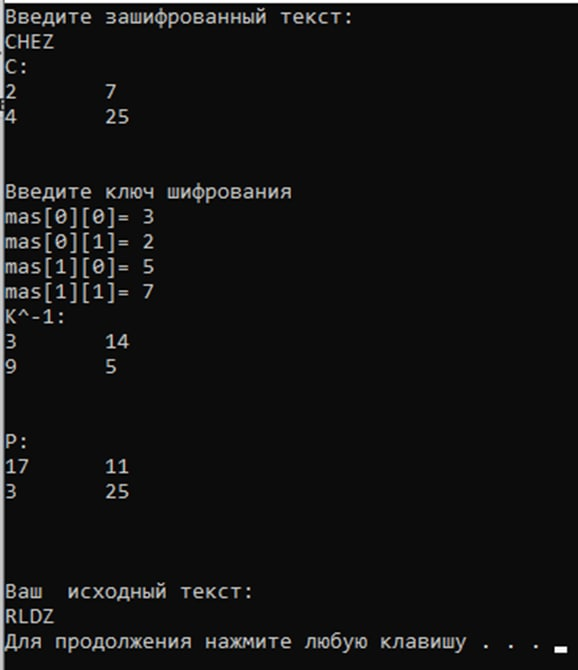
Шифр Хилла. При заданном тексте, модуле и ключе выполнить шифрование/дешифрование, а также атаку грубой силы и/или по образцу (при известной длине ключа).

* Описать алгоритмы шифрования, дешифрования, уязвимости и возможные атаки.
* Написать программу и расшифровать текст

«IUVAFSLDNNLDWMCOTKGMCHEZ», полученный шифром Хилла с ключом

|  |  |
| --- | --- |
| **3** | **2** |
| **5** | **7** |

К = n = 26.



**В данном билете нужно 6 раз сделать блок 2х2 и получить исходный текст:**

**WE LIVE IN AN INSECURE WORLD Z**

Файл: hilla\_decrypt.cpp

## Билет №19

*Страница 104*

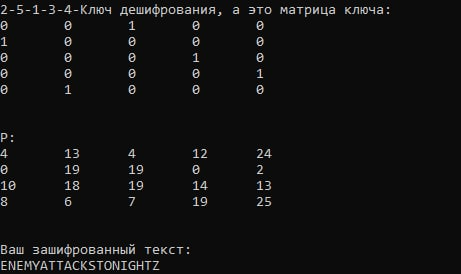
Перестановка по ключу. При заданном тексте и ключе выполнить шифрование/дешифрование, а также атаку грубой силы и/или по образцу.

Описать алгоритмы шифрования, дешифрования, уязвимости и возможные атаки.

Написать программу и реализовать атаку грубой силы по отысканию ключевой матрицы и взлому шифротекста

«EEMYNTAACTTKONSHITZG»





Ключ дешифрования – 2-5-1-3-4

Ключ шифрования – 3 1 4 5 2

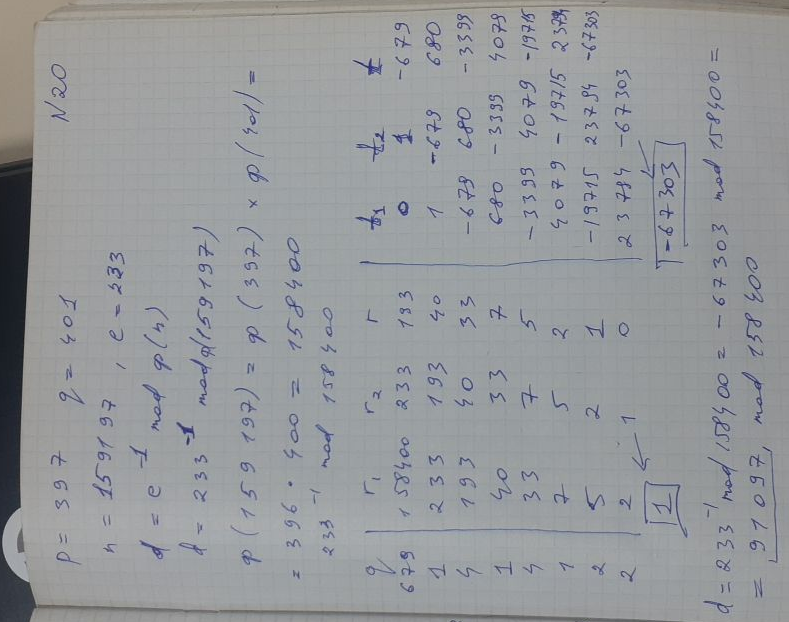
## Билет №20

Криптосистема RSA, моделирование (для небольших чисел и текста) шифрования/дешифрования, а также атака разложения на множители.

* Описать алгоритмы шифрования, дешифрования, атаку разложения на множители.
* Написать программу шифрования и атаки разложения на множители для задачи:

Выбирая p = 397 и q = 401, Дженифер создает для себя пару ключей (e, d). Она передает Тэду открытый ключ n = 159197, е = 233. Тэд шифрует сообщение «**No**» → C1. Ева перехватывает C1 и проводит успешную атаку. Как?

*Страница 327*



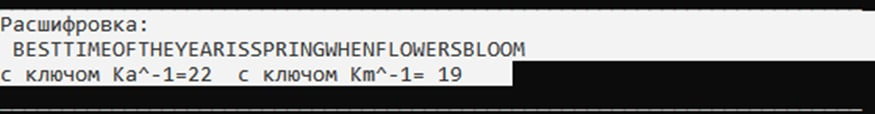
## Билет №24

Алиса перехватила зашифрованное сообщение от Евы к Бобу: PWUFFOGWCHFDWIWEJOUUNJORSMDWRHVCMWJUPVCCG. Она предполагает, что сообщение зашифровано аффинным шифром. Помогите Алисе написать программу, которая расшифрует данное сообщение, опишите алгоритм атаки.

(Шифр Афинный стр. 85)

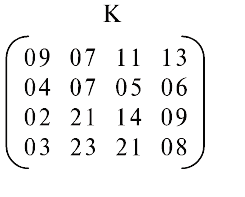
Атака грубой силы.

**Best time of the year is spring when flower bloom** - ответ

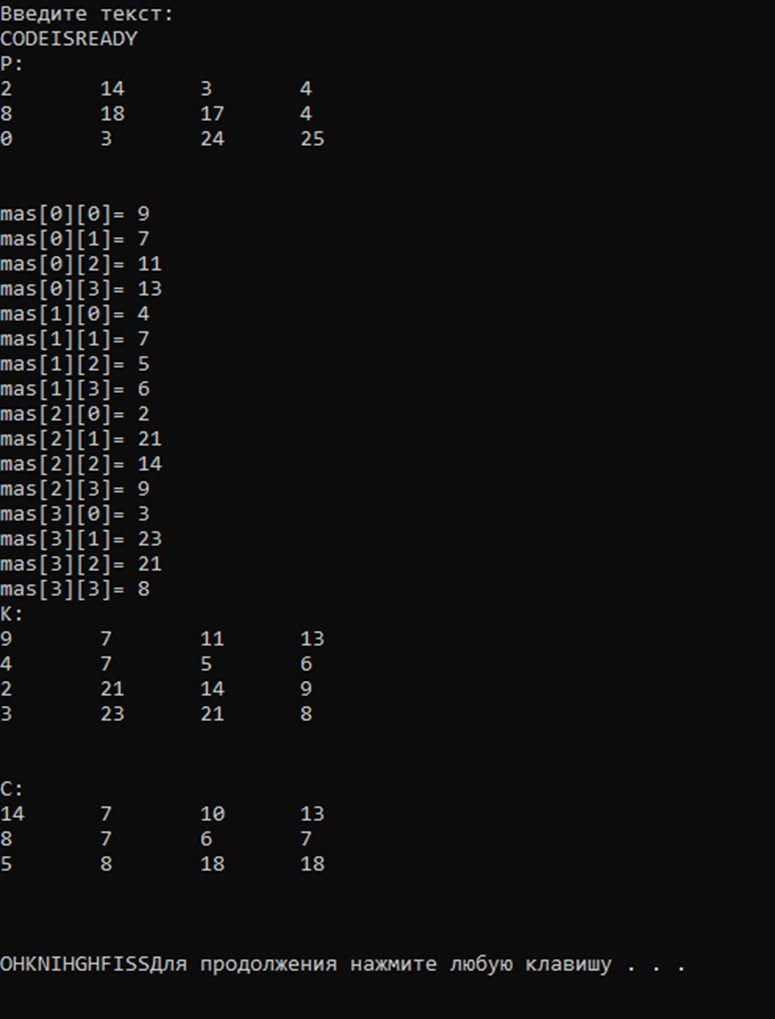


## Билет №25

Боб хотел узнать у Алисы о состоянии ее программного кода. Но Боб не хотел, чтобы про это кто-нибудь узнал. Он отправил ей ключ шифрования в виде матрицы чтобы она зашифровала и сообщила ему. Помогите Алисе написать программу, которая сможет зашифровать сообщение «CODEISREADY» с ключом -



(Шифр Хилла стр. 96)



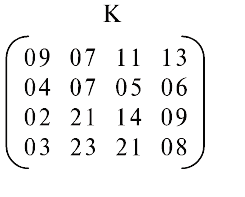
## Билет №26

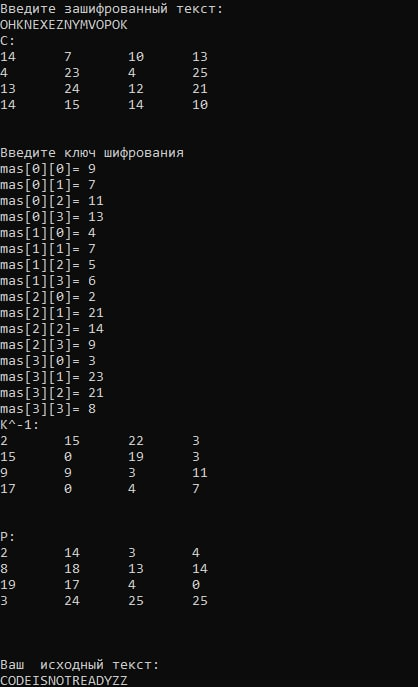
(Шифр Хилла стр. 96)

Боб получил сообщение от Алисы в зашифрованном виде

OHKNEXEZNYMVOPOK.

Боб знает ключ шифрование

но ему нужен ключ дешифрование чтобы он мог расшифровать данное сообщение. Напишите программу, которая расшифрует сообщение Алисы, опишите алгоритм атаки.



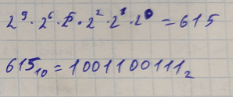
## Билет №27

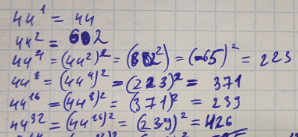
(Теорема Эйлера стр. 281) (Возведение в степень стр. 282-283)

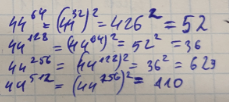
Опишите/реализуйте программу, которая вычисляеет инверсию заданного числа при составном модуле на основе теоремы Эйлера и алгоритма возведения в квадрат и умножения. Вычислите 44-1 mod 667= ? и проверьте ответ. (Отв.: 379)

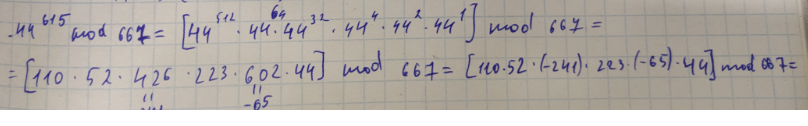
 =  

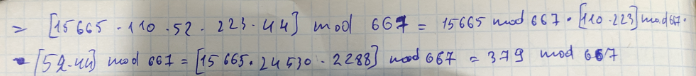




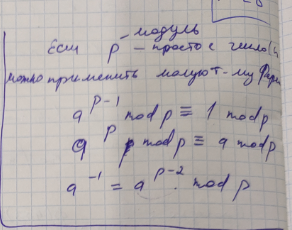


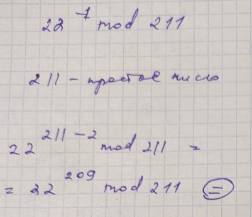


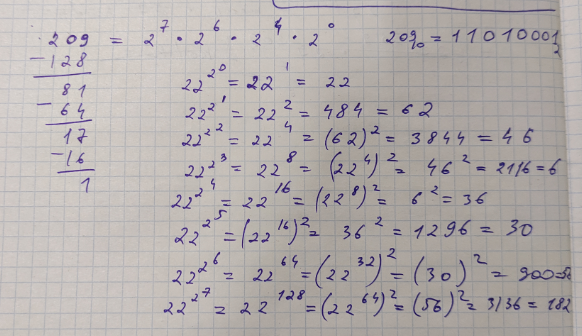


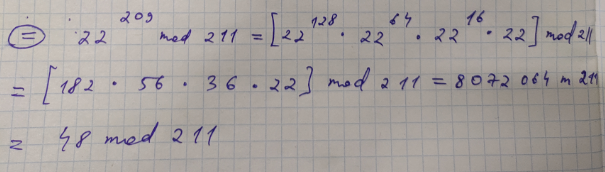
## Билет №28

Опишите/реализуйте программу, которая вычисляеет инверсию заданного числа при простом модуле с использованием малой теоремы Ферма и алгоритма возведения в квадрат и умножения. Вычислите 22-1 mod 211 = ?. (Отв.: 48)







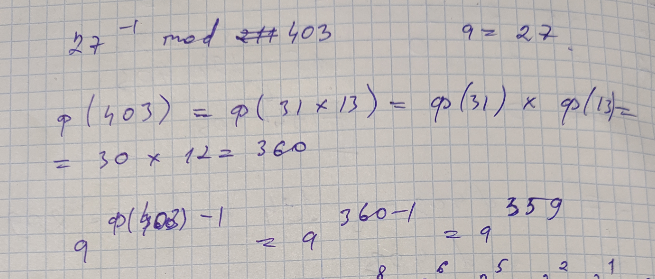


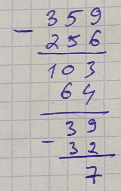
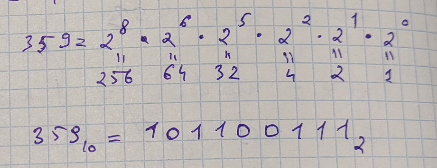
## Билет №30

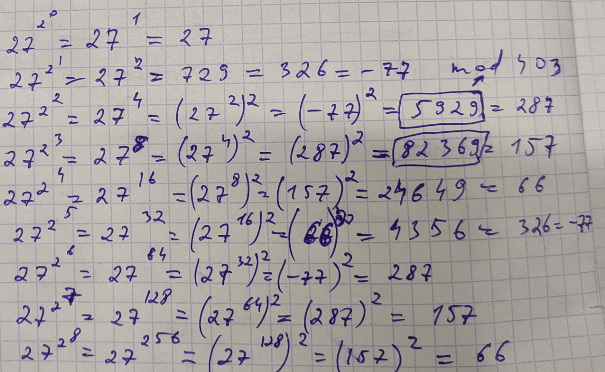
(Теорема Эйлера стр. 281) (Возведение в степень стр. 282-283)

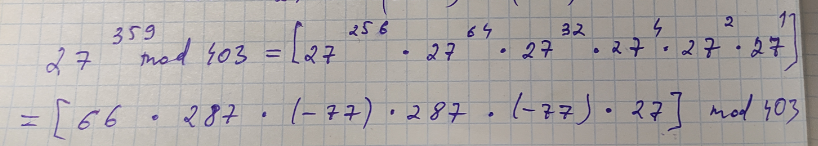
Опишите/реализуйте программу, которая вычисляеет инверсию заданного числа при составном модуле при помощи теоремы Эйлера и алгоритма возведения в квадрат и умножения. Вычислите 27-1 mod 403 = ? и проверьте ответ.

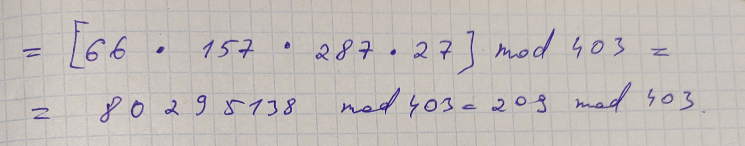
Теорема Эйлера Вена: (формула) a-1 mod n = aФ(n)-1  mod n









## Билет №31

(Алгоритм Евкалида стр. 42/Мультипликативная инверсия 57 стр.)

Опишите суть и реализуйте программу, которая, используяалгоритмы Евклида, вычисляет мультипликативную инверсию заданного числа при известном модуле. Найдите 27-1 mod 403 = ? (Отв.: 209)

Решение:

27-1 mod 403

a \* x ≡ 1 mod (n)

НОД (n, a) = 1, а и n взаимно простые, имеет мультипликативную инверсию Zn

НОД (403, 27) = НОД (27, 25) = НОД (25, 2) = НОД (2, 1) = НОД (1, 0) = 1

У 27 есть мультипликативная Z403

Таблица (Алгоритм Евкалида)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | r1 | r2 | r | t1 | t2 | t |
| 14 | 403 | 27 | 25 | 0 | 1 | -14 |
| 1 | 27 | 25 | 2 | 1 | -14 | 15 |
| 12 | 25 | 2 | 1 | -14 | 15 | -194 |
| 2 | 2 | 1 | 0 | 15 | -194 | 403 |
|  | 1 | 0 |  | -194 | 403 |  |

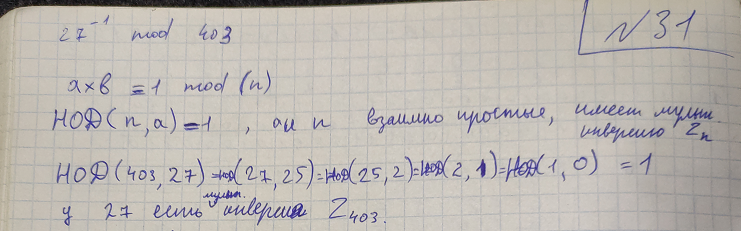
Проверка:

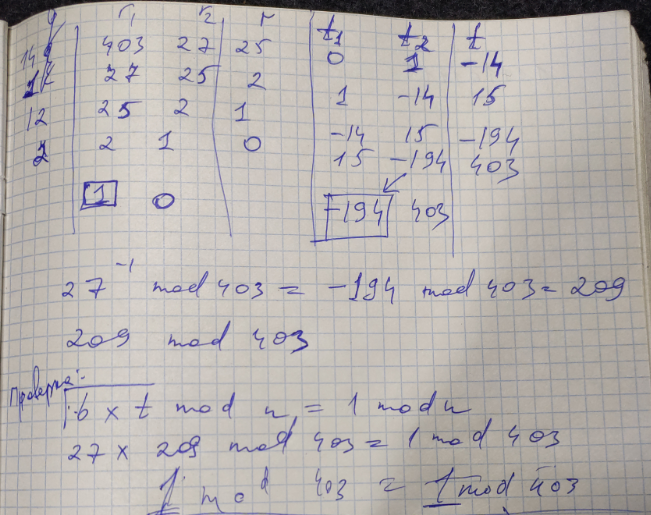
mod 403 = - 194 mod 403 = 209

209 mod 403

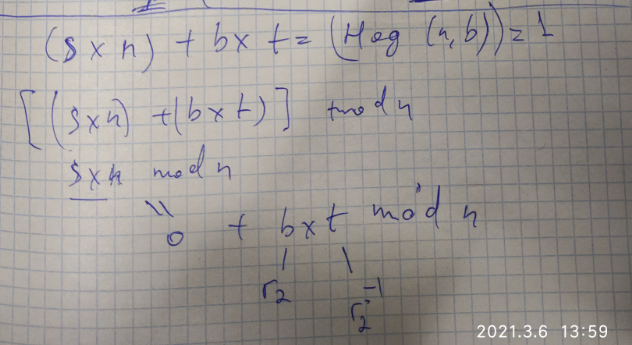
b \* t mod n = 1 mod n

27 \* 209 mod 403 = 1 mod 403

1 mod 403 = 1 mod 403



(Для тех кто шарит)



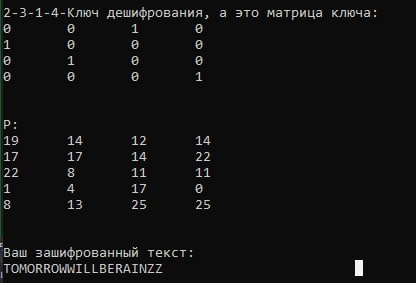
## Билет №32

Ева перехватывает сообщение Алисы “MTOOORRWLWILRBEAZINZ” и предполагает, что Алиса использует шифр перестановки. Напишите программу, которая реализует атаку Евы для получения исходного текста.

1.Каков размер ключа перестановки?

2.Какую атаку предпримет Ева?

*Страница 102*



Ключ шифрования 3 1 2 4

Ключ дешифрования 2 3 1 4

## Билет №33

Страница 80+

Используйте атаку грубой силы, чтобы расшифровать следующее сообщение, зашифрованное Алисой, применяя аддитивный шифр. Предположим, что Алиса всегда использует ключ, связанный с её днем рождения, который приходится на 13-е число каждого месяца.

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTYJ(аддитивный)



## Билет №35

Криптосистема RSA, моделирование (для небольших чисел и текста) шифрования/дешифрования.

* Описать алгоритмы шифрования, дешифрования.
* Написать программу шифрования и атаки разложения на множители для задачи:

Дженифер по открытому ключу n = 403, е = 29 передает день и месяц предстоящего важного мероприятия С = 220. Ева перехватывает это сообщениеи проводит успешную атаку. Описать и реализовать тип ее атаки. (При решении задачи использовать алгоритм быстрого возведения в степень). (Отв.: 207)

