# Письменное задание 1

Вариант 13

## Задача 1

Дано слово на русском языке и ключ. Зашифруйте данное слово с данным

ключом при помощи шифра Цезаря. Считайте, что в алфавите присутствуют

все 33 буквы (ё, й и т.д.).

Слово=баскетболист, Ключ=15.

Ответ: поащубпэъчаб

## Задача 2

Дана криптограмма, полученная при помощи шифра Цезаря после зашифрования

слова на русском языке, и ключ. Расшифруйте данную криптограмму с данным

ключом. Считайте, что в алфавите присутствуют все 33 буквы (ё, й и т.д.).

Криптограмма=ихтлрзхтпшщ, Ключ=7.

Ответ: волейболист

## Задача 3

Дано слово на русском языке и соответствующая ему криптограмма.

Проведите атаку по известному открытому тексту. Считайте, что в

алфавите присутствуют все 33 буквы (ё, й и т.д.).

Слово=подписка, Криптограмма=чцлчрщтз.

Ответ: Ключ =8

## Задача 4

Дана криптограмма, полученная после зашифрования русского слова шифром Цезаря.

Методом полного перебора ключей (методом грубой силы) найдите исходный открытый текст и ключ, который был использован при зашифровании. Считайте, что в алфавите присутствуют все 33 буквы (ё, й и т.д.).

Криптограмма=жщжйёжъшёбэ.

Ответ: слово- обоснование, ключ 25

# Письменное задание 3

## Задача 1

Даны числа a и b. Найдите их наибольший общий делитель, используя

алгоритм Евклида.

a=33012525, b=31045875.

33012525/31045875 = 1 (остаток 1966650)

31045875/1966650 = 15 (остаток 1546125)

1966650/1546125 = 1 (остаток 420525)

1546125/420525 = 3 (остаток 284550)

420525/284550 = 1 (остаток 135975)

284550/135975 = 2 (остаток 12600)

135975/12600 = 10 (остаток 9975)

12600/9975 = 1 (остаток 2625)

9975/2625 = 3 (остаток 2100)

2625/2100 = 1 (остаток 525)

2100/525 = 4 (остаток 0)

Ответ: НОД = 525

## Задача 2

Даны числа a и b. Найдите их наименьшее общее кратное.

a=3498, b=3744.

3498 = 2\*3\*11\*53

3744 = 2\*2\*2\*2\*2\*3\*3\*13

2\*2\*2\*2\*2\*3\*3\*13\*11\*53 = 2182752

Ответ: НОК = 2182752

## Задача 3

Даны три пары чисел: (x1,y1), (x2,y2) и (x3,y3). Определите, какие

из них являются взаимно простыми, а какие - нет.

x1=10, y1=31, x2=11, y2=18, x3=15, y3=94.

НОД(10,31)=1

НОД(11,18)=1

НОД(15,94)=1

Ответ: Взаимно простые- x1 y1, x2 y2, x3 y3

## Задача 4

Даны целые числа a и b. Используя обобщенный алгоритм Евклида,

решить диофантово уравнение ax+by = НОД(a,b).

a=260, b=270.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | U | | | V | | | T | | |
| u1 | u2 | u3 | v1 | v2 | v3 | t1 | t2 | t3 |
| 270/260 = 1 | 270 | 1 | 0 | 260 | 0 | 1 | 270 mod 260 = 10 | 1-1\*0=1 | 0-1\*1=-1 |
| 260/10 = 6 | 260 | 0 | 1 | 10 | 1 | -1 | 260 mod 10 = 0 | 0 – 6\*1 = -6 | 1-6\*-1=7 |
|  | 10 | 1 | -1 | 0 | -6 | 7 |  |  |  |

Ответ: НОД = 10, x=-1, y=1

## Задача 5

Даны взаимно простые числа c и m. Найдите инверсию числа c

по модулю m, используя обобщенный алгоритм Евклида.

c=22, m=123.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | U | | | V | | | T | | |
| u1 | u2 | u3 | v1 | v2 | v3 | t1 | t2 | t3 |
| 123/22 = 5 | 123 | 1 | 0 | 22 | 0 | 1 | 123 mod 22 = 13 | 1-5\*0=1 | 0-5\*1=-5 |
| 22/13 = 1 | 22 | 0 | 1 | 13 | 1 | -5 | 22 mod 13 = 9 | 0-1\*1=-1 | 1-1\*-5=6 |
| 13/9=1 | 13 | 1 | -5 | 9 | -1 | 6 | 13 mod 9 = 4 | 1-1\*-1=2 | -5-1\*6=-11 |
| 9/4=2 | 9 | -1 | 6 | 4 | 2 | -11 | 9 mod 4 = 1 | -1-2\*2=-5 | 6-2\*-11=28 |
| 4/1=4 | 4 | 2 | -11 | 1 | -5 | 28 | 4 mod 1 = 0 | 2-4\*-5=22 | -11-4\*28=-123 |
|  | 1 | -5 | 28 | 0 | 22 | -132 |  |  |  |

Ответ: 28

# Письменное задание 4

## Задача 1

Даны некоторые из параметров шифра Шамира и передаваемое сообщение m.

Вычислите недостающие параметры и выполните все шаги работы данного

шифра. Убедитесь, что отправленное сообщение равно полученному.

p=13, Ca=5, Cb=5, m=11.

A:

B:

A:

B:

Отправленное сообщение совпадает с полученным

## Задача 2

Даны некоторые из параметров шифра Эль-Гамаля, а также два сообщения Mab

и Mba, первое из которых передается от абонента A абоненту B, а второе -

от абонента B абоненту A. Параметр Kab - это случайное число, выбираемое

абонентом A, а Kba - это случайное число, выбираемое абонентом B.

Вычислите недостающие параметры шифра и выполните все шаги работы данного

шифра по передаче обоих сообщений. Убедитесь, что отправленные сообщения

совпадают с полученными.

p=23, g=21, Ca=11, Cb=18, Mab=14, Mba=14, Kab=21, Kba=3.

Генерация ключей:

Передача от А к B:

Абонент A:

Абонент B:

Передача от B к A:

Абонент B:

Абонент A:

Отправленные сообщения совпадают с полученными

## Задача 3

Даны некоторые из параметров шифра RSA для двух абонентов, а также два

сообщения Mab и Mba, передаваемые соответственно от абонента A абоненту B

и от абонента B абоненту A. Вычислите недостающие параметры и выполните

необходимые шаги по передаче обоих сообщений. Убедитесь, что отправленные

сообщения совпадают с полученными.

Pa=5, Pb=11, Qa=7, Qb=2, Da=11, Db=7, Mab=15, Mba=24.

Генерация ключей:

Передача от А к B:

Абонент A:

Абонент B:

Передача от B к A:

Абонент B:

Абонент A:

Отправленные сообщения совпадают с полученными

## Задача 4

Даны некоторые из параметров цифровой подписи RSA, а также сообщение m,

которое нужно подписать. Вычислите недостающие параметры и цифровую

подпись данного сообщения. Выполните также проверку подлинности

сообщения. Для простоты в качестве используемой хеш-функции используйте

тождественную функцию h(m)=m.

P=5, Q=7, d=17, m=30.

Генерация ключей:

A:

B:

Сообщение подлинно.

## Задача 5

Даны некоторые из параметров цифровой подписи Эль-Гамаля, а также

сообщение m, предназначенное для подписи. Параметр k - это случайное

число, выбираемое при генерации подписи. Вычислите недостающие параметры

данного протокола, подпишите сообщение и затем проверьте его подлинность.

p=47, g=31, x=11, m=32, k=35.

A:

15

B:

(mod 46)

Сообщение подлинно.

# Письменное задание 6

## Задача 1

Даны параметры a, x и p. Вычислите значение функции a^x mod p, используя алгоритм быстрого возведения в степень. Подробно распишите все промежуточные действия.

a=9, x=827, p=11.

Y=9^827 mod 11

82710=11001110112

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 91 | 92 | 94 | 98 | 916 | 932 | 964 | 9128 | 9256 | 9512 |
| 9 | 81 | 16 | 25 | 9 | 81 | 16 | 25 | 9 | 81 |
| 9 | 4 | 5 | 3 | 9 | 4 | 5 | 3 | 9 | 4 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
|  | 36 |  | 9 | 81 | 16 |  |  | 45 | 4 |
| 9 | 3 |  | 9 | 4 | 5 |  |  | 1 | **4** |

Ответ: 4

## Задача 2

Дано значение параметра p. Оцените сложность (число операций умножения)

вычисления прямой (при помощи алгоритма быстрого возведения в степень по

модулю) и обратной функции (методами полного перебора и “Шаг младенца - Шаг

великана”) a^x mod p при таком значении p. Считайте, что параметры a и x могут быть

произвольными из диапазона от 2 до p-1.

p=71059000000.

Количество умножений для алгоритма быстрого возведения в степень: 37

Количество умножений для метода полного перебора:

Количество умножений для метода “Шаг младенца – Шаг великана”:

## Задача 3

Дано число абонентов сети (N). Найдите количество секретных ключей, необходимых для того, чтобы все абоненты могли общаться друг с другом попарно безопасно.

N=14106.

Ответ: 99 482 565

## Задача 4

Даны некоторые из параметров системы Диффи-Хеллмана для трех абонентов.Вычислите недостающие параметры и сформируйте ключи для каждой пары абонентов.

p=23, g=10, Xa=9, Xb=8, Xc=11.

|  |  |  |
| --- | --- | --- |
| Абонент | Закрытый ключ | Открытый ключ |
| A | 9 | 20 |
| B | 8 | 2 |
| C | 11 | 22 |

## Задача 5

Дано число p. Найдите все подходящие значения параметра g для системы Диффи-Хеллмана. Если p>11, то найдите не все, а только два значения.

p=23.

Два подходящих значений g: 9, 11