**Индивидуальные домашние задания №1**

**Задание №1. Шифр Цезаря**. Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.

Исходный текст:

**«**КОЩАВЦЕВ ДАНИИЛ ВАСИЛЬЕВИЧ**»**

Используем алфавит, содержащий 33 буквы и пробел, стоящий после буквы Я:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ*пробел*

Ключом в шифре Цезаря является число 3. Каждая буква в исходном тексте сдвигается по алфавиту на 3 позиции. Таким образом, получаем:

|  |  |
| --- | --- |
| Исходный текст | КОЩАВЦЕВ ДАНИИЛ ВАСИЛЬЕВИЧ |
| Зашифрованный текст | НСЬГЕЩЗЕВЖГРЛЛОВЕГФЛОЯЗЕЛЪВ |

**Задание №2. Алгоритм шифрования ГОСТ 28147-89.** Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены (см. Приложение А). Для получения 64 бит исходного текста *используйте 8 первых символов из своих данных*: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. *Первый подключ содержит первые 4 буквы.*

Исходные данные для зашифрования из 32 букв: КОЩАВЦЕВ ДАНиил Васильевич и криптография.

В качестве первого блока используем 8 первых символов: КОЩАВЦЕВ Для первого подключа Х используем первые 4 буквы ключа: ДАН.

Переводим исходный текст и первый подключ в двоичную последовательность (см. Приложение Б):

К – 11001010

О – 11001110

Щ – 11011001

А – 11000000

В – 11000010

Ц – 11010110

Е – 11000101

В – 11000010

первый подключ X0

Пробел – 00100000

Д – 11000100

А – 11000000

Н – 11001101

Таким образом, первые 64 бита определяют входную последовательность

L0: 11001010 11001110 11011001 11000000

R0: 11000010 11010110 11000101 11000010

следующие 32 бита определяют первый подключ

Х0: 00100000 11000100 11000000 11001101

I. Найдем значение функции преобразования f(R0,X0) (см. Приложение А)

1). Вычисление суммы R0 и X0 по mod 232

R0: 1100 0010 1101 0110 1100 0101 1100 0010

Х0: 0010 0000 1100 0100 1100 0000 1100 1101

1110 0011 1001 1011 1000 0110 1000 1111

2). Преобразование в блоке подстановки

Результат суммирования R0+X0 по mod 232

1110 0011 1001 1011 1000 0110 1000 1111

преобразуем в блоке подстановки (см. Приложение В). Для каждого 4-битного блока вычислим его адрес в таблице подстановки. Номер блока соответствует номеру столбца, десятичное значение блока соответствует номеру строки в таблице.

номера блоков

8 7 6 5 4 3 2 1

1110 0011 1001 1011 1000 0110 1000 1111

соответствующие номера строк в таблице подстановки

8 7 6 5 4 3 2 1

14 3 9 11 8 6 8 15

1000 0001 0110 1110 1110 0100 0010 0011

3). Циклический сдвиг результата п.2 на 11 бит влево

0111 0111 0010 0001 0001 1100 0000 1011

Таким образом, нашли значение функции f (R0,X0):

0111 0111 0010 0001 0001 1100 0000 1011

II. Вычисляем R1= f(R0,X0) L0.

Результат преобразования функции f(R0,X0) складываем с L0 по mod2:

L0: 1100 1010 1100 1110 1101 1001 1100 0000

f(R0,X0): 0111 0111 0010 0001 0001 1100 0000 1011

R1: 0011 0001 1110 1111 1110 0101 1100 1011

**Задание №3. Алгоритм шифрования RSA.** Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

I. Генерация ключей (см. Приложение Г).

Выберем два простых числа *р* = 13 и *q* = 31 (см. Приложение Д). Тогда модуль *n* = *pq*=13\*31 = 403 и функция Эйлера

*(n)* = *(p-1)(q-1)* = 12\*30= 360.

Закрытый ключ *d* выбираем из условий *d* < *(n)* и *d* взаимно просто с *(n)*, т.е. *d* и *(n)* не имеют общих делителей. Пусть *d* = 107.

Открытый ключ *e* выбираем из условий *e*<*(n)* и *de*=1*(mod* *(n)):* *e*<360, 107*e*=1(mod 360).

Последнее условие означает, что число 107*e*-1 должно делиться на 360 без остатка. Таким образом, для определения *e* нужно подобрать такое число *k*, что 107*e*-1 = 360 *k*.

Будем подбирать это число с помощью расширенного алгоритма Евклида: делим с остатком 360 на 107:

делении

𝑃0 = 3, 𝑃1 = 𝑞1, 𝑃𝑖 = 𝑞𝑖 ∙ 𝑃𝑖−1 + 𝑃𝑖−2 для 𝑖 ≥ 2

Контроль: 𝑃𝑠 = 𝑛

Тогда 𝑎−1 ≡ (−1)𝑠−1𝑃𝑠−1(𝑚𝑜𝑑 𝑛)

****

s = 6. Контроль: 𝑃𝑠 = 𝑛, то есть 𝑃6 = 360 − верно. Значит, 107−1 ≡ (−1)𝑠−1𝑃𝑠−1 = (−1)537 ≡ 323 (𝑚𝑜𝑑 216).

Таким образом, (323, 403) – открытый ключ, (107, 403) – секретный ключ.

Замечание. После формирования ключа промежуточные числа (*p*, *q*, (*n*)) рекомендуется уничтожить.

1. Зашифрование.

Представим шифруемое сообщение «КДВ» как последовательность целых чисел.

Пусть буква «К» соответствует числу 12, буква «Д» - числу 5 и буква «В» - числу 3. Зашифруем сообщение, используя открытый ключ (323, 403):

𝐶1 = (12323) 𝑚𝑜𝑑 403 = 363

𝐶2 = (5323) 𝑚𝑜𝑑 403 = 242

𝐶3 = (3323) 𝑚𝑜𝑑 403 = 321

Таким образом, исходному сообщению (12, 5, 3) соответствует криптограмма (363, 242, 321).

1. Расшифрование

Расшифруем сообщение (363, 242, 321), пользуясь секретным ключом (107,403):

𝑀1 = (363107) 𝑚𝑜𝑑 403 = 12

𝑀2 = (242107) 𝑚𝑜𝑑 403 = 5

𝑀3 = (321107) 𝑚𝑜𝑑 403 = 3

В результате расшифрования было получено исходное сообщение (12, 5, 3), то есть "КДВ".

**Задание №4. Функция хеширования.** Найти хеш–образ своей Фамилии, используя хеш–функцию Hi =(Hi 1− +M modni )2 , где *n = pq*. Числа p, q взять из задания №3.

Хешируемое сообщение «КОЩАВЦЕВ». Возьмем два простых числа *p*=13, *q*=31 (см. Приложение Е). Определим *n*=*pq*=13\*19=247. Вектор инициализации H0 выберем равным

23 (выбираем случайным образом). Слово «САВИН» можно представить

последовательностью чисел (19, 1, 3, 10, 15) по номерам букв в алфавите. Таким образом, n=403, H0=38, M1=12, M2=16, M3=27, M4=1, M5=3, M6=24, M7=6, M8=3.

Используя формулу

Hi =(Hi 1− +M modni )2 ,

получим хеш-образ сообщения «КОЩАВЦЕВ»:

H1 = mod 403 = 82

H2 = mod 403 = 335

H3 = mod 403 = 69

H4 = mod 403 = 64

H5 = mod 403 = 56

H6 = mod 403 = 355

H7 = mod 403 = 152

H8 = mod 403 = 248

итоге получаем хеш-образ сообщения «КОЩАВЦЕВ», равный 248.

**Задание №5. Электронная цифровая подпись.** Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

Пусть хеш-образ Фамилии равен 248, а закрытый ключ алгоритма RSA равен (107, 403). Тогда электронная цифровая подпись сообщения, состоящего из Фамилии, вычисляется по правилу (см. Приложение Ж) *s* = 248 107 mod 403 = 248.

Для проверки ЭЦП, используя открытый ключ (323, 403), найдем H = 248 323 mod 403 = 248.

Поскольку хеш-образ сообщения совпадает с найденным значением H, то подпись признается подлинной.