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

Имя Отчество.

Исходный текст:

«КЛЕХТА ВИКТОР РОМАНОВИЧ»

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

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯпробел

Ключом в шифре Цезаря является число 3. Каждая буква в исходном тексте сдвигается

по алфавиту на 3 позиции. Таким образом, получаем:

|  |  |
| --- | --- |
| Исходный текст | КЛЕХТА ВИКТОР РОМАНОВИЧ |
| Зашифрованный текст | **НОЗШХГВЕЛНХСУВУСПГРСЕЛЪ** |

**Задание №2. Алгоритм шифрования ГОСТ 28147-89.** Алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. 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: КЛЕХТА ВИКТОр Романович и

криптография.

В качестве первого блока используем 8 первых символов: КЛЕХТА В

Для первого подключа Х используем первые 4 буквы ключа: ИКТО.

Переводим исходный текст и первый подключ в двоичную последовательность (см.

Приложение Б):

исходный текст

К 11001010

Л 11001011

Е 11000101

Х 11010101

Т 11010010

А 11000000

пробел 00100000

В 11000010

первый подключ X0

И 11001000

К 11001010

Т 11010010

О 11001110

Таким образом, первые 64 бита определяют входную последовательность

L0: 11001010 11001011 11000101 11010101

R0: 11010010 11000000 00100000 11000010

следующие 32 бита определяют первый подключ

Х0: 11001000 11001010 11010010 11001110

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

1). Вычисление суммы R0 и X0 по

R0: 1101 0010 1100 0000 0010 0000 1100 0010

Х0: 1100 1000 1100 1010 1101 0010 1100 1110

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1001 1011 1000 1010 1111 0011 1001 0000

2). Преобразование в блоке подстановки

Результат суммирования R0+X0 по



Преобразуем в блоке подстановки

Номера блоков

8 7 6 5 4 3 2 1

1001 1011 1000 1010 1111 0011 1001 0000

Соответствующие номера строк в таблице подстановки

9 11 8 10 15 3 9 0

Заполнение

2 7 3 9 3 13 3 4

Результат

0010 0111 0011 1001 0011 1101 0011 0100

Циклический сдвиг результата п.2 на 11 бит влево

1100 1001 1110 1001 1010 0001 0011 1001

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

1100 1001 1110 1001 1010 0001 0011 1001

II. Вычисляем

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

L0: 1100 1010 1100 1011 1100 0101 1101 0101

f(R0,X0): 1100 1001 1110 1001 1010 0001 0011 1001

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

R1: **0000 0011 0010 0010 0010 0100 1110 1100**

**Задание №3. Алгоритм шифрования RSA.** Сгенерируем 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 .

Выберем два простых числа р = 11 и q = 17 .

Тогда модуль

n = pq=11\*17 = 187

и функция Эйлера

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 = 23.

Открытый ключ e выбираем из условий e< (n) и de=1(mod (n)): e<160,

23e=1(mod 160).

Последнее условие означает, что число 23e-1 должно делиться на 160 без остатка.

Таким образом, для определения e нужно подобрать такое число k, что

23e-1 = 160 k.

Будем подбирать это число с помощью расширенного алгоритма Евклида: делим с

остатком 160 на 23:

Последний ненулевой остаток в схеме Евклида – это НОД этих чисел. Выражаем теперь последовательно НОД, начиная с конца:

1 = 23 − 1 ∙ 22 = 23 − 1 ∙ ( 160 − 6 ∙ 23) = −1 ∙ 160 + 7 ∙ 23

По модулю 160 получим 7 ∙ 23 = 1(𝑚𝑜𝑑 160),

значит, 𝑒 = 7 ≡ 7 + 160 = 167 (𝑚𝑜𝑑 160)

Таким образом, (167, 187) – открытый ключ, (23, 187) – секретный ключ.

II. Зашифрование.

Представим шифруемое сообщение «КВР» как последовательность целых чисел.

Пусть буква «К» соответствует числу 12, буква «В» - числу 3 и буква «Р» - числу 18.

Зашифруем сообщение, используя открытый ключ (167, 187):

Таким образом, исходному сообщению (12, 3, 18) соответствует криптограмма **(177, 130, 171)**.

III. Расшифрование

Расшифруем сообщение (177, 130, 171), пользуясь секретным ключом (23,187):

В результате расшифрования было получено исходное сообщение (12, 3, 18), то есть "КВР".

**Задание №4. Функция хеширования.** Найти хеш–образ своей Фамилии, используя

хеш–функцию

Хешируемое сообщение «КЛЕХТА». Возьмем два простых числа p=11, q=17 . Определим n=pq=11\*17=187. Вектор инициализации H0 выберем равным 23 (выбираем случайным образом). Слово «КЛЕХТА» можно представить последовательностью чисел (12, 13, 6, 23, 20, 1) по номерам букв в алфавите. Таким образом,

n=187, H0=23, M1=12, M2=13, M3=6, M4=23, M5=20, M6=1.

,

получим хеш-образ сообщения «КЛЕХТА»:

H1=(H0+M1)2 mod n = (23 + 12)2 mod 187 = 103

H2=(H1+M2)2 mod n = (103 + 13)2 mod 187 = 179

H3=(H2+M3)2 mod n = (179 + 6)2 mod 187 = 4

H4=(H3+M4)2 mod n = (4 + 23)2 mod 187 = 168

H5=(H4+M5)2 mod n = (168 + 20)2 mod 187 = 1

H6=(H5+M6)2 mod n = (1 + 1)2 mod 187 = 4

В итоге получаем хеш-образ сообщения «КЛЕХТА», равный 4.

**Задание №5. Электронная цифровая подпись.** Используя хеш-образ своей

Фамилии, вычислите электронную цифровую подпись по схеме RSA.

Хеш-образ Фамилии равен 4, а закрытый ключ алгоритма RSA равен (23, 187).

Тогда электронная цифровая подпись сообщения, состоящего из Фамилии, вычисляется по

правилу

Для проверки ЭЦП, используя открытый ключ (167, 187), найдем

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

признается подлинной.

Ответ. 1) НОЗШХГВЕЛНХСУВУСПГРСЕЛЪ

2) R1= 0000 0011 0010 0010 0010 0100 1110 1100

3) (177, 130, 171)

4) 4

5) 4