# Задание №1. Шифр Цезаря.

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 | ШПОНАРСКИЙ БОГДАН ВЛАДИСЛАВОВИЧ |
| Зашифрованный текст | ЫТСРГУФНЛМВДСЁЖГРВЕОГЖЛФОГЕСЕЛЪ |

# Задание №2. Алгоритм шифрования ГОСТ 28147-89.

В качестве первого блока используем 8 первых символов: ШПОНАРСК

Для первого подключа Х используем первые 4 буквы ключа: ИЙ Б

исходный текст

|  |  |
| --- | --- |
| Ш | 11011000 |
| П | 11001111 |
| О | 11001110 |
| Н | 11001101 |
| А | 11000000 |
| Р | 11010000 |
| С | 11010001 |
| К | 11001010 |

первый подключ X0

|  |  |
| --- | --- |
| И | 11001000 |
| Й | 11001001 |
| пробел | 00100000 |
| Б | 11000001 |
|  |  |

L0 = 11011000 11001111 11001110 11001101

R0 = 11000000 11010000 11010001 11001010

X0 = 11001000 11001001 00100000 11000001

Вычисление суммы R0 и X0 по mod 232

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R0: | 1100 0000 | 1101 0000 | 1101 0001 | 1100 1010 |
| Х0: | 1100 1000 | 1100 1001 | 0010 0000 | 1100 0001 |
|  | 1000 1001 | 1001 1001 | 1111 0010 | 1000 1011 |

Номера блоков

8 7 6 5 4 3 2 1

1000 1001 1001 1001 1111 0010 1000 1011

Соответствующие номера строк в таблице подстановки

8 9 9 9 15 2 8 11

Заполнение

9 10 6 10 3 1 2 12

Результат

1001 1010 0110 1010 0011 0001 0010 1100

Циклический сдвиг результата п.2 на 11 бит влево

0101 0001 1000 1001 0110 0100 1101 0011

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

0101 0001 1000 1001 0110 0100 1101 0011

Результат преобразования функции f (R0, X0) складываем с L0 по mod 2:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L0: | 1101 | 1000 | 1100 | 1111 | 1100 | 1110 | 1100 | 1101 |
| f(R0,X0): | 0101 | 0001 | 1000 | 1001 | 0110 | 0100 | 1101 | 0011 |
| R1: | 1000 | 1001 | 0100 | 0110 | 1010 | 1010 | 0001 | 1110 |

# Задание №3. Алгоритм шифрования RSA.

* 1. Генерация ключей

# Выберем два простых числа *р* = 11 и *q* = 53.

# Тогда модуль n = 583.

*(n)* = *(p-1)\*(q-1)* = 10\*52 = 520.

# Пусть d = 33 – закрытый ключ.

# Будем подбирать открытый ключ с помощью расширенного алгоритма Евклида: делим с остатком 520 на 33:

# 520 = 15\*33 + 25, 33 = 1\*25 + 8, 25 = 3\*8 + 1, 8 = 8\*1

# 1 = 25 – 3\*8 = 25 – 3\*(33 – 1\*25) = 4\*25 – 3\*33 = 4\*(520 – 15\*33) – 3\*33 = 4\*520 – 63\*33.

# Получаем e = 520 – 63 = 457 (*mod* 520)

Таким образом, (457, 583) – открытый ключ, (33, 583) – секретный ключ.

1. Зашифрование.

Представим шифруемое сообщение «ШБВ» как последовательность целых чисел.

Пусть букве «Ш» соответствует числу 26, буква «Б» - числу 2 и буква «В» - числу 3.

# Зашифруем сообщение, используя открытый ключ (457, 583):

𝐶1 = (26457) 𝑚𝑜𝑑 583 = 390

𝐶2 = (2457) 𝑚𝑜𝑑 583 = 304

𝐶3 = (3457) 𝑚𝑜𝑑 583 = 207

Вычисления для C1, C2, C3:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | *ak* | *i* | *s* | *p* |
| 1 | 26 | 457 | 1 | 26 |
| 2 | 26∙26=676=93 | 228 | 0 | 26 |
| 3 | 93∙93=8649=487 | 114 | 0 | 26 |
| 4 | 487∙487=237169=471 | 57 | 1 | 26∙471=12246=3 |
| 5 | 471∙471=221841=301 | 28 | 0 | 3 |
| 6 | 301∙301=90601=236 | 14 | 0 | 3 |
| 7 | 236∙236=55696=311 | 7 | 1 | 3∙311=933=350 |
| 8 | 311∙311=96721=526 | 3 | 1 | 350∙526=184100=455 |
| 9 | 526∙526=276676=334 | 1 | 1 | 455∙334=151970=**390** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | *ak* | *i* | *s* | *p* |
| 1 | 2 | 457 | 1 | 2 |
| 2 | 2∙2=4 | 228 | 0 | 2 |
| 3 | 4∙4=16 | 114 | 0 | 2 |
| 4 | 16∙16=256 | 57 | 1 | 2∙256=512 |
| 5 | 256∙256=65536=240 | 28 | 0 | 512 |
| 6 | 240∙240=57600=466 | 14 | 0 | 512 |
| 7 | 466∙466=217156=280 | 7 | 1 | 280∙512=143360=525 |
| 8 | 280∙280=78400=278 | 3 | 1 | 278∙525=145950=200 |
| 9 | 278∙278=77284=328 | 1 | 1 | 200∙328=65600=**304** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| K | *ak* | *i* | *s* | *p* |
| 1 | 3 | 457 | 1 | 3 |
| 2 | 3∙3=9 | 228 | 0 | 3 |
| 3 | 9∙9=81 | 114 | 0 | 3 |
| 4 | 81∙81=6561=148 | 57 | 1 | 3∙148=444 |
| 5 | 148∙148=21904=333 | 28 | 0 | 444 |
| 6 | 333∙333=110889=119 | 14 | 0 | 444 |
| 7 | 119∙119=14161=169 | 7 | 1 | 169∙444=75036=412 |
| 8 | 169∙169=28561=577 | 3 | 1 | 577∙412=237724=443 |
| 9 | 577∙577=332929=36 | 1 | 1 | 36∙443=15948=**207** |

# Таким образом, исходному сообщению (26, 2, 3) соответствует криптограмма (390, 304, 207).

1. Расшифрование

# Расшифруем сообщение (390, 304, 207), пользуясь секретным ключом (33, 583):

𝑀1 = (39033) 𝑚𝑜𝑑 583 = 26

𝑀2 = (30433) 𝑚𝑜𝑑 583 = 2

𝑀3 = (20733) 𝑚𝑜𝑑 583 = 3

# В результате расшифрования было получено исходное сообщение (26, 2, 3), то есть «ШБВ».

# Задание №4. Функция хеширования.

# Хешируемое сообщение «ШПОНАРСКИЙ». Возьмем два простых числа p = 11, q = 53. Определим n = 583. Вектор инициализации H0 выберем равным 17. Слово «ШПОНАРСКИЙ» можно представить последовательностью чисел (26, 17, 16, 15, 1, 18, 19, 12, 10, 11) по номерам букв в алфавите. Таким образом, n = 583, H0 = 17, M1 = 26, M2 = 17, M3 = 16, M4 = 15, M5 = 1, M6 = 18, M7 = 19, M8 = 12, M9 = 10, M10 = 11.

H1=(H0+M1)2 mod n = (17 + 26)2 mod 583 = 1849 mod 583 = 100

H2=(H1+M2)2 mod n = (100 + 17)2 mod 583 = 13689 mod 583 = 280

H3=(H2+M3)2 mod n = (280 + 16)2 mod 583 = 87616 mod 583 = 166

H4=(H3+M4)2 mod n = (166 + 15)2 mod 583 = 32761 mod 583 = 113

H5=(H4+M5)2 mod n = (113 + 1)2 mod 583 = 12996 mod 583 = 170

H6=(H5+M6)2 mod n = (170 + 18)2 mod 583 = 35344 mod 583 = 364

H7=(H6+M7)2 mod n = (364 + 19)2 mod 583 = 146689 mod 583 = 356

H8=(H7+M8)2 mod n = (356 + 12)2 mod 583 = 135424 mod 583 = 168

H9=(H8+M9)2 mod n = (168 + 10)2 mod 583 = 31684 mod 583 = 202

H10=(H9+M10)2 mod n = (202 + 11)2 mod 583 = 45369 mod 583 = 478

# В итоге получаем хеш-образ сообщения «ШПОНАРСКИЙ», равный 478.

# Задание №5. Электронная цифровая подпись.

# Пусть хеш-образ «ШПОНАРСКИЙ» равен 478, а закрытый ключ алгоритма RSA равен (33, 583). Тогда электронная цифровая подпись сообщения, состоящего из «ШПОНАРСКИЙ» вычисляется следующим образом:

# s = 47833 mod 583 = 213

# Для проверки электронной цифровой подписи, используя открытый ключ (457, 583), найдем:

# H = 213457 mod 583 = 478

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