**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО**

Факультет автоматизированных и информационных систем

Кафедра «Информатика»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

по дисциплине **«Основы защиты информации»**

на тему: **«**Простейшие алгоритмы шифрования**»**

Выполнила: студентка гр. ИП-32

Суховенко Э.С.

Принял: преподаватель Кудин В.П.

Гомель 2022

Цель работы: Изучить простейшие алгоритмы шифрования.

**Ход выполнения:**

* 1. **Простейшие перестановочные шифры:**

Удаление пробелов и написание слов только большими буквами:

СУХОВЕНКОЭДУАРДСЕРГЕЕВИЧ

Разбиение зашифрованного текста на блоки:

СУХО ВЕНК ОЭДУ АРДС ЕРГЕ ЕВИЧ

Запись слов в обратном порядке:

ОХУС КНЕВ УДЭО СДРА ЕГРЕ ЧИВЕ

Геометрическая фигура:

М: суховенкоэдуардсергеевич

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | c | y | x | о | в |
| 2 | е | н | к | о | э |
| 3 | д | у | а | р | д |
| 4 | с | е | р | г | е |
| 5 | е | в | и | ч |  |

Матрица 5 строк, 5 столбцов. Запись построчная. Чтение по столбцам сверху вниз 1, 2, 3, 4, 5

С: седсеунуевхкариооргчвэде

* 1. **Шифр типа «Железнодорожная изгородь»**

Пусть имеется правило записи текста следующим образом:

1 7 13 19 25

2 6 8 12 14 18 20 24 26

3 5 9 11 15 17 21 23 27

4 10 16 22 28

С Н А Г

У Е К У Р Р Е Ч

Х В О Д Д Е Е И

О Э С В

Исходный текст “СУХОВЕНКОЭДУАРДСЕРГЕЕВИЧ” будет записан в виде: ‘СНАГЧУЕКУРРЕЧХВОДДЕЕИОЭСВ’

**1.3 Ключевое слово или ключевая фраза**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К**  **5** | **Р**  **8** | **И**  **3** | **П**  **7** | **Т**  **10** | **О**  **6** | **Г**  **2** | **Р**  **9** | **А**  **1** | **Ф**  **11** | **И**  **4** | **Я**  **12** |
| **с** | **у** | **х** | **о** | **в** | **е** | **н** | **к** | **о** | **э** | **д** | **у** |
| **а** | **р** | **д** | **с** | **е** | **р** | **г** | **е** | **е** | **в** | **и** | **ч** |

М: КРИПТОГРАФИЯ

С: ОЕНГХДДИСАЕРОСУРКЕВЕЭВУЧ

**1.4 Метод поворачивающейся решетки**

Суть метода: исходный текст записывается через отверстия в решетке, которая по мере заполнения поворачивается на 90º. Предварительно текст разбивается на блоки (в данном случае блок равен 16 символам).

– строится матрица (NхN);

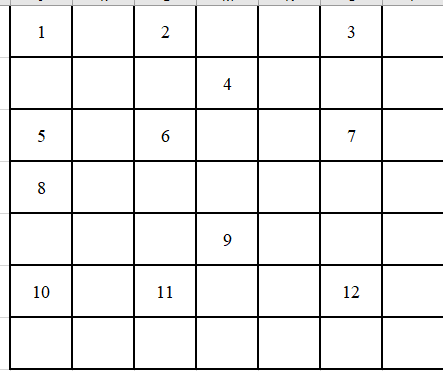
– ячейки матрицы, которые при повороте матрицы на 90 градусов занимают одинаковое положение нумеруются одинаково. Для этого можно нумеровать ячейки закручивая значения во внутрь одновременно со всех сторон;

– Если длина стороны матрицы нечетно – центральная ячейка не участвует в шифровании;

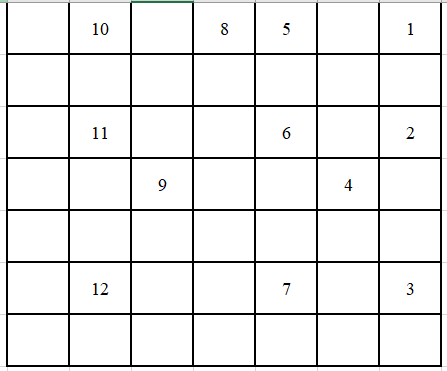
– вырезается один из квадратов с одинаковым номером.

М: СУХОВЕНКОЭДУАРДСЕРГЕЕВИЧ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 |  | 12 |  |  | 7 |  |
|  |  |  | 9 |  |  |  |
| 11 |  | 2 |  |  | 3 |  |
| 8 |  |  |  |  |  |  |
|  |  |  | 4 |  |  |  |
| 5 |  | 10 |  |  | 6 |  |
|  |  |  |  |  |  |  |



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| с |  | у |  |  | х |  |
|  |  |  | о |  |  |  |
| в |  | е |  |  | н |  |
| к |  |  |  |  |  |  |
|  |  |  | о |  |  |  |
| э |  | д |  |  | у |  |
|  |  |  |  |  |  |  |



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | а |  | р | д |  | с |
|  |  |  |  |  |  |  |
|  | е |  |  | р |  | г |
|  |  | е |  |  | е |  |
|  |  |  |  |  |  |  |
|  | в |  |  | и |  | ч |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| с | а | у | р | д | х | с |
| ф | а | п | о | ы | и | к |
| в | е | е | г | р | н | г |
| к | у | е | о | в | е | е |
| ф | ш | ф | о | о | н | з |
| э | в | д | п | и | у | ч |
| ш | й | с | т | м | с | д |

М: СУХОВЕНКОЭДУАРДСЕРГЕЕВИЧ

С: САУРДХСФАПОЫИКВЕЕГРНГКУЕОВЕЕФШФООНЗЭВДПИУЧ ШЙСТМСД

**Подстановочные шифры. Аффинное преобразование**

символ шифротекста вычисляется по математическому выражению:  
ci = (k1×a+ k2) mod n  
где ai – символ исходного текста;  
k1 – ключ = 13

k2 - вторая часть ключа = 7

числа 3 и 13 взаимно простые, то есть (33, 13) = 1  
n – мощность алфавита = 33

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| к | л | м | н | о | п | р | с | т | у | ф |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

М: ЙГЬДАЁЧСДБЩГЖЭЩЙЁЭМЁЁАШХ

Сi = (13 \* аi + 7) mod 33

С = (13 \* 18 + 7) mod 33 = 10 = Й

**Вывод:** в ходе выполнения данной лабораторной работы были изучены простейшие алгоритмы шифрования.