**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**»**

Выполнил: студент гр. ИП-32

Коваленко А.И.

Принял: преподаватель Кудин В.П.

Гомель 2023

Цель работы: изучить простейшие алгоритмы шифрования

**Ход выполнения:**

* 1. **Простейшие перестановочные шифры:**

Удаление пробелов и написание слов только большими буквами:

КОВАЛЕНКОАНАСТАСИЯИГОРЕВНА

Разбиение зашифрованного текста на блоки:

КОВА ЛЕНК ОАНА СТАС ИЯИГ ОРЕВ НА

Запись слов в обратном порядке:

АВОК КНЕЛ АНАО САТС ГИЯИ ВЕРО АН

Геометрическая фигура:

М: коваленкоанастасияигоревна

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | к | о | в | а | л | е |
| 2 | н | к | о | а | н | а |
| 3 | с | т | а | с | и | я |
| 4 | и | г | о | р | е | в |
| 5 | н | а |  |  |  |  |

Матрица 5 строк, 6 столбцов. Запись построчная. Чтение по столбцам сверху вниз 1, 2, 3, 4, 5

С: кнсиноктгавоаоаасрлниееаяв

* 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

К Н С И Н

О Е К А Т Я Г В А

В Л О Н А И О Е

А А С Р

Исходный текст “ КОВАЛЕНКОАНАСТАСИЯИГОРЕВНА” будет записан в виде: ‘КНСИНОЕКАТЯГВАВЛОНАИОЕААСР

**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** |
| **к** | **о** | **в** | **а** | **л** | **е** | **н** | **к** | **о** | **а** | **н** | **а** |
| **с** | **т** | **а** | **с** | **и** | **я** | **и** | **г** | **о** | **р** | **е** | **в** |
| **н** | **а** |  |  |  |  |  |  |  |  |  |  |

М: КРИПТОГРАФИЯ

С: оониванексиеяасотакглиарав

**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);

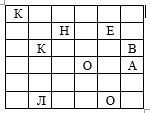
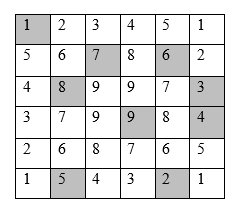
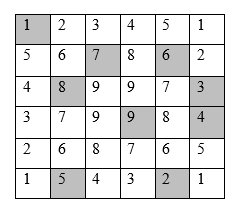
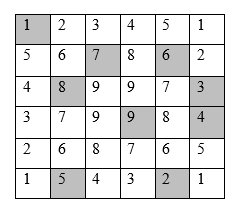
– ячейки матрицы, которые при повороте матрицы на 90 градусов занимают одинаковое положение нумеруются одинаково. Для этого можно нумеровать ячейки закручивая значения во внутрь одновременно со всех сторон;

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

– вырезается один из квадратов с одинаковым номером.

М: КОВАЛЕНКОАНАСТАСИЯИГОРЕВНА

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 1 |
| 5 | 6 | 7 | 8 | 6 | 2 |
| 4 | 8 | 9 | 9 | 7 | 3 |
| 3 | 7 | 9 | 9 | 8 | 4 |
| 2 | 6 | 8 | 7 | 6 | 5 |
| 1 | 5 | 4 | 3 | 2 | 1 |

****

М: КОВАЛЕНКОАНАСТАСИЯИГОРЕВНА

С: КГГДЕАТЖНИЕВРКАЙСВОЗЯОААНВИНАЕБЛСАОИ

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