**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

Кирпиченко Д.Д.

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:

КИРПИЧЕНКОДМИТРИЙДЕНИСОВИЧ

Разбиение зашифрованного текста на блоки:

КИРП ИЧЕН КОДМ ИТРИ ЙДЕН ИСОВ ИЧ

Запись слов в обратном порядке:

ЧИ ВОСИ НЕДЙ ИРТИ МДОК НЕЧИ ПРИК

Геометрическая фигура:

М: кирпиченкодмитрийденисович

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | к | и | р | п | и |
| 2 | ч | е | н | к | о |
| 3 | д | м | и | т | р |
| 4 | и | й | д | е | н |
| 5 | и | с | о | в | и |
| 6 | ч |  |  |  |  |

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

С: пктевкчдиичиемйсиорнирнидо

* 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 Е И Е И

И Ч Н М Т Д Н В Ч

Р И К Д Р Й И О

П О И С

Исходный текст “ КИРПИЧЕНКОДМИТРИЙДЕНИСОВИЧ ” будет записан в виде: КЕИЕИИЧНМТДНВЧРИКДРЙИОПОИС

**1.3 Ключевое слово или ключевая фраза**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **З**  **5** | **А**  **1** | **К**  **7** | **О**  **8** | **Д**  **4** | **И**  **6** | **Р**  **10** | **О**  **9** | **В**  **3** | **А**  **2** | **Т**  **11** | **Ь**  **12** |
| **к** | **и** | **р** | **п** | **и** | **ч** | **е** | **н** | **к** | **о** | **д** | **м** |
| **и** | **т** | **р** | **и** | **й** | **д** | **е** | **н** | **и** | **с** | **о** | **в** |
| **и** | **ч** |  |  |  |  |  |  |  |  |  |  |

М: КИРПИЧЕНКОДМИТРИЙДЕНИСОВИЧ

С: итчоскиийкиичдррпиннеедомв

**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 49 символам).

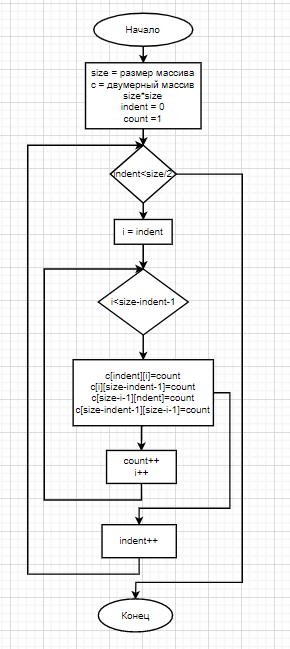
– строится матрица (NхN);

– 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: МИСТЕРКИРПИЧЕНКОДМИТРИЙДЕНИСОВИЧУЧИТКРИПТОГРАФИЮ



Алгоритм создание решетки

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| М |  |  |  | И |  |  |
|  |  | С |  |  |  | Т |
|  | Е |  |  | Р |  |  |
| К |  |  |  |  | И |  |
|  |  |  | Р |  |  |  |
|  | П |  |  |  |  | И |
|  |  |  |  | Ч |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Е |  |  | Н |
|  | К |  |  | О |  |  |
|  |  |  |  |  | Д |  |
|  |  | М |  |  |  |  |
| И |  |  |  | Т |  | Р |
|  |  |  | И |  |  |  |
|  | Й |  |  |  | Д |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Е |  |  |  |  |
| Н |  |  |  |  | И |  |
|  |  |  | С |  |  |  |
|  | О |  |  |  |  | В |
|  |  | И |  |  | Ч |  |
| У |  |  |  | Ч |  |  |
|  |  | И |  |  |  | Т |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | К |  |  |  | Р |  |
|  |  |  | И |  |  |  |
| П |  | Т |  |  |  | О |
|  |  |  |  | Г |  |  |
|  | Р |  |  |  |  |  |
|  |  | А |  |  | Ф |  |
| И |  |  | Ю |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| М | К | Е | Е | И | Р | Н |
| Н | К | С | И | О | И | Т |
| П | Е | Т | С | Р | Д | О |
| К | О | М |  | Г | И | В |
| И | Р | И | Р | Т | Ч | Р |
| У | П | А | И | Ч | Ф | И |
| И | Й | И | Ю | Ч | Д | Т |

М:МИСТЕРКИРПИЧЕНКОДМИТРИЙДЕНИСОВИЧУЧИТКРИПТОГРАФИЮ

С: МКЕЕИРННКСИОИТПЕТСРДОКОМГИВИРИРТЧРУПАИЧФИИЙИЮЧДТ

**Подстановочные шифры. Аффинное преобразование**

символ шифротекста вычисляется по математическому выражению:  
ci = (k1×a+ k2) mod n  
где ai – символ исходного текста;  
k1 – ключ = 2

k2 - вторая часть ключа = 7

числа 3 и 13 взаимно простые, то есть (33, 2) = 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: кирпиченкодмитрийденисович

Сi = (2\*аi+7) mod 33

ЬШЗЁШХРВЬДОАШЛЗШЪОРВШЙДКШХ

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