БГУИР

Кафедра ЗИ

Отчет

по практическому занятию №6

по теме:

«ШИФРОВАНИЕ И РАСШИФРОВАНИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ЦЕЗАРЯ»

Выполнили: Проверил:

Студенты гр.150503 Столер Д.В.

Ходосевич М.А.  
Семков А.Д.  
Шарай П.Ю.  
Гайчук В.Н.

Минск 2023

**Цель занятия:** изучение способов криптографического преобразования информации и получения базовых практических навыков шифрования сообщений, а также криптоанализа шифротекста на примере шифра Цезаря.

Условия заданий для 4 варианта:

1. **Задание для шифрования:**

Спасибо за утро такое,

За чудные эти часы

Лесного – не сна, а покоя,

Безмолвной морозной красы.

1. **Задание для расшифровки:**

Цсанх ъычщчци цн йчлиыи, И хцн ьпн ынх ючщчби,

Аыч ыих циьмиаь учлми-ыч Хчз цищчмсфиъе мьби.

Результат выполнения шифрования в задании 1: «Шцжшпзх ож ъщчх щжсхл, Ож юъкфвл дщп южшв Тлшфхйх – фл шфж, ж цхсхё, Злоухтифхр ухчхофхр счжшв.».

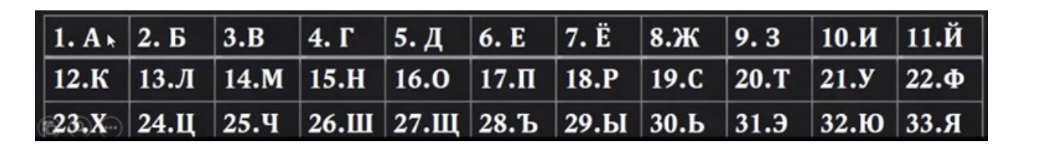


Рисунок 1

Таблица 1 – Алгоритм шифрования

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ  шифрования | Итоговый шифротекст | |
| утро | | ъщчх | |
| Буква шифруемого сообщения | Порядковый номер буквы по алфавиту | Порядковый номер буквы после сдвига | Буква шифротекста |
| У | 21 | 7 | 28 | Ъ |
| Т | 20 | 27 | Щ |
| Р | 18 | 25 | Ч |
| О | 16 | 23 | Х |
|  |  |  |  |

Результат выполнения расшифровки в задании 2: «Ничем сторона не богата, А мне уже тем хороша, Что там наудачу когда-то Моя народилась душа.».

Таблица 2 – алгоритм расшифровки

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифротекста | | Ключ  шифрования | Расшифрованный фрагмент сообщения | |
| Цсанх | | Ничем | |
| Буква шифротекста | Порядковый номер буквы по алфавиту | Порядковый номер буквы после обратного сдвига | Буква расшифрованного сообщения |
| Ц | 24 | 9 | 15 | Н |
| С | 19 | 10 | И |
| А | 1 | 25 | Ч |
| Н | 15 | 6 | Е |
| Х | 23 | 14 | М |

Процесс подбора криптографического ключа. Возьмем слово из шифротекста “ Цсанх”:

Ключ 1 – Хрямф

Ключ 2 – Фпюлу

Ключ 3 – Уоэкт

Ключ 4 – Тньйс

Ключ 5 – Смыир

Ключ 6 – Рлъзп

Ключ 7 – Пкщжо

Ключ 8 – Ойшён

Ключ 9 - Ничем

Следовательно, ключ расшифрования – 9 со смещением влево.