Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

Кафедра защиты информации

ОТЧЕТ

Практическое занятие №6

«Шифрование и расшифрование информации

с использованием шифра Цезаря»

Выполнили:

студенты гр. №250502

Бекетова М.А.

Шершнева Е.С.

Проверил:

Столер Д.В.

Минск 2024

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

Результаты выполнения практических заданий.

Таблица 1 – Исходные условия для выполнения заданий

|  |  |  |
| --- | --- | --- |
| Номер  варианта | Номер  задания | Условие задания |
| 3 | 1 | Ничем сторона не богата,  А мне уже тем хороша,  Что там наудачу когда-то  Моя народилась душа. |
| 2 | Зэ, фмъмуд ъзтзж, чшцщъц ямшъ йцпдфр! Пзирйзмъ  тшгаы имугфр кйцплдфр. Ъцудтц фхм хм щъшзахц, р  й фцмс щылдим Хмчыъмйгф щмшлюмф ж чшриръ т  ъмим. |

Таблица 2 – Криптографический ключ для выполнения первого задания

|  |  |
| --- | --- |
| Номер варианта | Ключ шифрования |
| 1 | 7 |
| 2 | 8 |
| 3 | 9 |
| 4 | 7 |
| 5 | 8 |
| 6 | 9 |
| 7 | 7 |
| 8 | 8 |
| 9 | 9 |
| 10 | 7 |

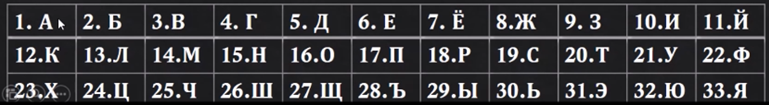


Рисунок 1 – Алфавит для шифрования и расшифрования сообщений

Описание процедуры шифрования сообщения в шифре Цезаря заключается в том, что каждая буква исходного сообщения сдвигается на фиксированное количество позиций в алфавите. Это количество позиций определяется ключом шифрования, который представляет собой целое число.

Таблица 3 – Алгоритм шифрования фрагмента сообщения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ шифрования | Итоговый шифротекст | |
|  | |  | |
| Буква шифруемого сообщения | Порядковый номер буквы по алфавиту | Порядковый номер буквы после сдвига | Буква шифротекста |
| *с* | 19 | 9,  Сдвиг вправо по алфавиту | 28 | ъ |
| *т* | 20 | 29 | ы |
| *о* | 16 | 25 | ч |
| *р* | 18 | 27 | щ |
| *о* | 16 | 25 | ч |
| *н* | 15 | 24 | ц |
| *а* | 1 | 10 | и |

Результат шифрования всего сообщения:

«Цсанх ъычщчци цн йчлиыи,

И хцн ьпн ынх ючщчби,

Аыч ыих циьмиаь учлми-ыч

Хчз цищчмсфиъе мьби.»

Описание процесса поиска криптографического ключа заключается в том, что идет процесс переборки вариантов ключа.

Таблица 4 – Алгоритм расшифрования фрагмента шифротекста

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифротекста | | Ключ расшифро-вания | Расшифрованный фрагмент сообщения | |
|  | |  | |
| Буква шифротекста | Порядковый номер буквы по алфавиту | Порядковый номер буквы после обратного сдвига | Буква расшифрованного сообщения |
| *ф* | 22 | 8, Сдвиг влево по алфавиту | 14 | м |
| *м* | 14 | 6 | е |
| *ъ* | 28 | 20 | т |
| *м* | 14 | 6 | е |
| *у* | 21 | 13 | л |
| *д* | 5 | 30 | ь |

Результат расшифрования всего шифротекста:

«Ах, метель такая, просто черт возьми!

Забивает крышу белыми гвоздьми.

Только мне не страшно, и в моей судьбе

Непутевым сердцем я прибит к тебе.»