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. № 251003

Габрусь С. П.

Панкратьев Е. С.

Кухоцковолец А. М.

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 |
| 8 | 1 | Касаясь трех великих океанов,  Она лежит, раскинув города,  Покрыта сеткою меридианов,  Непобедима, широка, горда. |
| 2 | Рёчёечв шцкы зксороы фркёуфз,  Фуё скмош, цёчроущз  ифцфйё, Хфрцбшё чкшрфд ткцойоёуфз,  Укхфжкйотё, юоцфрё, ифцйё. |

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 |

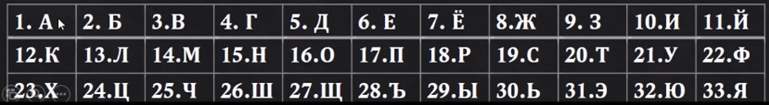


Рисунок 1 – Алфавит для шифрования и расшифрования сообщений

Описание процедуры шифрования сообщения заключается в том, что к порядковому номеру буквы алфавита прибавляется ключ и получается порядковый номер зашифрованной буквы. В случае превышения результатом количества букв в алфавите, производится операция взятия остатка полученного значения от количества букв в алфавите.

Таблица 3 – Алгоритм шифрования фрагмента сообщения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ шифрования | Итоговый шифротекст | |
| Касаясь | |  | |
| Буква шифруемого сообщения | Порядковый номер буквы по алфавиту | Порядковый номер буквы после сдвига | Буква шифротекста |
| К | 12 | 8 | 20 | Т |
| А | 1 | 9 | З |
| С | 19 | 27 | Щ |
| А | 1 | 9 | З |
| Я | 33 | 8 | Ж |
| С | 19 | 27 | Щ |
| Ь | 30 | 5 | Д |

Результат шифрования всего сообщения:

*Тзщзжщд ъшмэ ймуртрэ цтмзхцй,*

*Цхз уморъ, шзщтрхый кцшцлз,*

*Чцтшгъз щмътцё фмшрлрзхцй,*

*Хмчцимлрфз, аршцтз, кцшлз.*

Описание процесса поиска криптографического ключа заключается в том, что берется одно слово, и методом подбора просматривается каждая возможная вариация сдвига (от 1 до 32). В случае если получается осмысленное слово, то найден ключ и по этому ключу расшифровывается всё сообщение.

Таблица 4 – Алгоритм расшифрования фрагмента шифротекста

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифротекста | | Ключ расшифро-вания | Расшифрованный фрагмент сообщения | |
| Рёчёечв | | Осенний | |
| Буква шифротекста | Порядковый номер буквы по алфавиту | Порядковый номер буквы после обратного сдвига | Буква расшифрованного сообщения |
| Р | 18 | 1 | 19 | С |
| Ё | 7 | 8 | Ж |
| Ч | 25 | 26 | Ш |
| Ё | 7 | 8 | Ж |
| Е | 6 | 7 | Ё |
| Ч | 25 | 26 | Ш |
| В | 3 | 4 | Г |
| Р | 18 | 2 | 20 | Т |
| Ё | 7 | 9 | З |
| Ч | 25 | 27 | Щ |
| Ё | 7 | 9 | З |
| Е | 6 | 8 | Ж |
| Ч | 25 | 27 | Щ |
| В | 3 | 5 | Д |
| … | … | … | … | … |
| Р | 18 | 27 | 12 | К |
| Ё | 7 | 1 | А |
| Ч | 25 | 19 | С |
| Ё | 7 | 1 | А |
| Е | 6 | 33 | Я |
| Ч | 25 | 19 | С |
| В | 3 | 30 | Ь |

Результат расшифрования всего шифротекста:

*Касаясь трех великих океанов,*

*Она лежит, раскинув города,*

*Покрыта сеткою меридианов,*

*Непобедима, широка, горда.*