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

Бригадир А.С.

Горох А.А.

Копылова Е.С.

Цвирко Е.Д.

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 |
| 10 | 1 | То было много лет назад.  Я тоже в первый раз  С толпою сверстников-ребят  Явился в школьный класс. |
| 2 | Ъг хм лцуомх цщъзйужъд Лцфз тхркы р ъмъшзлд!  Чзшъз – еъц хм тшцйзъд. Р хмудпж хз хмс умозъд! |

Таблица 2 – Криптографический ключ для выполнения первого задания

|  |  |
| --- | --- |
| Номер варианта | Ключ шифрования |
| 10 | 7 |

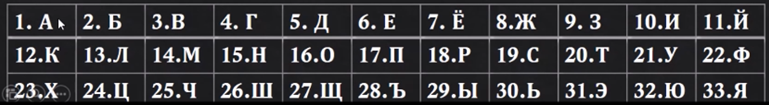


Рисунок 1 – Алфавит для шифрования и расшифрования сообщений

Описание процедуры шифрования сообщения заключается в том, что необходимо к порядковому номеру каждой буквы прибавить ключ шифрования. Результат взять по модулю 33.

Таблица 3 – Алгоритм шифрования фрагмента сообщения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ шифрования | Итоговый шифротекст | |
| Много | | Уфхйх | |
| Буква шифруемого сообщения | Порядковый номер буквы по алфавиту | Порядковый номер буквы после сдвига | Буква шифротекста |
| *М* | 14 | 7 | 21 | У |
| *Н* | 15 | 22 | Ф |
| *О* | 16 | 23 | Х |
| *Г* | 4 | 11 | Й |
| *О* | 16 | 23 | Х |

Результат шифрования всего сообщения:

Щх звтх уфхйх тлщ фжожк.

Ё щхнл и цлчивр чжо

Ш щхтцхе шилчшщфпсхи-члзёщ

Ёиптшё и ясхтгфвр стжшш.

Описание процесса поиска криптографического ключа заключается в том, что необходимо последовательно перебрать все ключи при котором фрагмент шифротекста преобразуется в читабельный текст.

Таблица 4 – Алгоритм расшифрования фрагмента шифротекста

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифротекста | | Ключ расшифро-вания | Расшифрованный фрагмент сообщения | |
| ючщчби | | хороша | |
| Буква шифротекста | Порядковый номер буквы по алфавиту | Порядковый номер буквы после обратного сдвига | Буква расшифрованного сообщения |
| *Л* | 13 | 8 | 5 | Д |
| *Ц* | 24 | 16 | О |
| *У* | 21 | 13 | Л |
| *О* | 16 | 8 | Ж |
| *М* | 14 | 6 | Е |
| *Х* | 23 | 15 | Н |

Результат расшифрования всего шифротекста:

Ты не должен оставлять Дома книгу и тетрадь! Парта – это не кровать. И нельзя на ней лежать!