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. №

ФИО

ФИО

ФИО

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 |
|  | 1 |  |
| 2 |  |

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 |

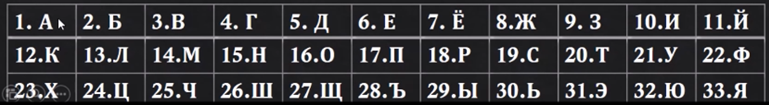


Рисунок 1 – Алфавит для шифрования и расшифрования сообщений

Описание процедуры шифрования сообщения заключается в том, что …

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 |
| *1-ая буква* |  |  |  |  |
| *2-ая буква* |  |  |  |
| *i-буква* |  |  |  |

Результат шифрования всего сообщения:

Описание процесса поиска криптографического ключа заключается в том, что …

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 |
| *1-ая буква* |  |  |  |  |
| *2-ая буква* |  |  |  |
| *i-буква* |  |  |  |

Результат расшифрования всего шифротекста: