БГУИР

Кафедра ЭВМ

Отчет по практическому занятию № 6

Тема: «Шифрование и расшифрование информации с использованием шифра цезаря»

Вариант 10

Выполнили:

студенты гр. №150502

Альхимович Н.Г.

Катковская Е.А.

Скалозуб К.А.

Сацюк Я.И.

Проверил:

Столер Д.В.

Минск

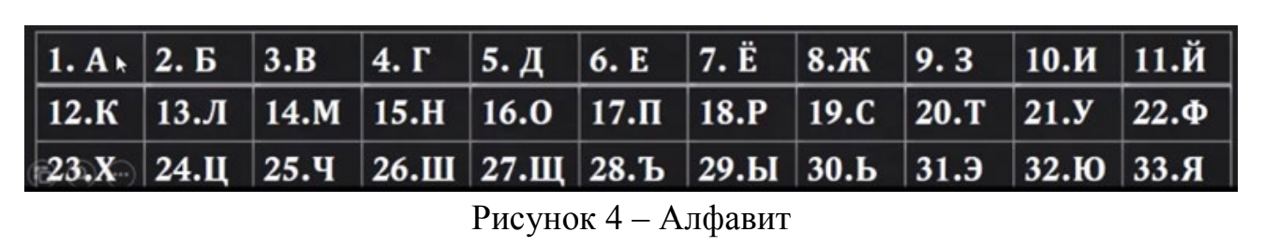
2023

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

**Задание 2.1**

Криптографический ключ шифрования: 7.

Алфавит:



Исходный текст:

То было много лет назад.

Я тоже в первый раз

С толпою сверстников-ребят

Явился в школьный класс.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ шифруемого сообщения | Итоговый шифротекст | |
| ребят | | члзёщ | |
| Буква  шифруемого  сообщения | Порядковый  номер буквы по  алфавиту | Порядковый  номер буквы  после сдвига | Буква  шифротекста |
| *р* | 18 | 7 | 25 | ч |
| *е* | 6 | 13 | л |
| *б* | 2 | 9 | з |
| *я* | 33 | 7 | ё |
| *т* | 20 | 27 | щ |

Зашифрованный текст:

Щх звтх уфхйх тлщ фжожк.

Ё щхнл и цлчивр чжо

Ш щхтцхе шилчшщфпсхи-члзёщ

Ёиптшё и ясхтгфвр стжшш.

**Задание 2.2**

Зашифрованный текст:

Ъг хм лцуомх цщъзйужъд Лцфз тхркы р ъмъшзлд!

Чзшъз – еъц хм тшцйзъд. Р хмудпж хз хмс умозъд!

Поиск ключа шифрования:

Ключ 1 – сфпйъ;

Ключ 2 – руойщ;

Ключ 3 – птнзш;

Ключ 4 – осмжч;

Ключ 5 – нрлёц;

Ключ 6 – мпкех;

Ключ 7 – лойдф;

**Ключ 8 – книгу.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фрагмент шифруемого сообщения | | Ключ шифруемого сообщения | Итоговый шифротекст | |
| тхркы | | книгу | |
| Буква  шифруемого  сообщения | Порядковый  номер буквы по  алфавиту | Порядковый  номер буквы  после сдвига | Буква  шифротекста |
| *т* | 20 | 8 | 12 | к |
| *х* | 23 | 15 | н |
| *р* | 18 | 10 | и |
| *к* | 12 | 4 | г |
| *ы* | 29 | 21 | у |

Исходный текст:

Ты не должен оставлять

Дома книгу и тетрадь!

Парта – это не кровать.

И нельзя на ней лежать!

Вывод: в ходе выполнения данной работы были изучены способов криптографического преобразования информации, а также были получены практические навыки шифрования сообщений, криптоанализа шифротекста на примере шифра Цезаря.