Учреждение образования “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

Практическое занятие №5

«Криптографическая защита информации»

Выполнил:

студент 2 курса, 7 группы

Бобрович Глеб Сергеевич

Проверил:

Барковский Евгений Валерьевич

Минск 2022ПроТТеоре

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

1. Шифр Цезаря

Алфавит:



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | **Б** | **о** | **б** | **р** | **о** | **в** | **и** | **ч** | **Г** | **л** | **е** | **б** | **С** | **е** | **р** | **г** | **е** | **е** | **в** | **и** | **ч** |
| Номер 1 | 2 | 16 | 2 | 18 | 16 | 3 | 10 | 25 | 4 | 13 | 6 | 2 | 19 | 6 | 18 | 4 | 6 | 6 | 3 | 10 | 25 |
| Номер 1 +5 | 7 | 21 | 7 | 23 | 21 | 8 | 15 | 30 | 9 | 18 | 11 | 7 | 24 | 11 | 23 | 9 | 11 | 11 | 8 | 15 | 30 |
| Шифр | **Ё** | **У** | **Ё** | **Х** | **У** | **Ж** | **Н** | **Ъ** | **З** | **Р** | **Й** | **Ё** | **Ц** | **Й** | **Х** | **З** | **Й** | **Й** | **Ж** | **Н** | **Ъ** |

1. Шифр Трисемуса

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |  | , | . |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

Исходный текст: БобровичГлебСергеевич

Ключ: ЗащитаЗащитаЗащитаЗащ

Зашифрованный текст: ЙПЫЬВГСШЭХШВЬЁКМШЁКЁС

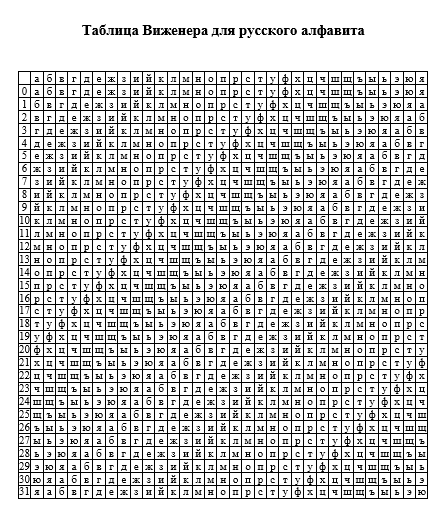
1. Шифр Плейфейра

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Z | A | S | H | I |
| T | B | C | D | E |
| F | G | K | L | M |
| N | O | P | Q | R |
| U | V | W | X | Y |

BobrovichGlebSergeevich = GV EO VA SE AL MD CA MY MB BY SE DH

Zashita

1. Шифр Вижинера



Исходный текст: БобровичГлебСергеевич

Ключ: ЗащитаЗащитаЗащитаЗащ

Зашифрованный текст: 6 0 24 24 4 30 31 9 22 29 13 31 22 27 9 5 13 27 5 24 30

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. | **тяеонаыбиьсрль\_т** | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 9 | 16 | 2 | 7 | | 6 | 3 | 13 | 12 | | 15 | 10 | 8 | 1 | | 4 | 5 | 11 | 14 | |

|  |  |  |  |
| --- | --- | --- | --- |
| 9 | 16 | 2 | 7 |
| 6 | 3 | 13 | 12 |
| 15 | 10 | 8 | 1 |
| 4 | 5 | 11 | 14 |

|  |  |  |  |
| --- | --- | --- | --- |
| 9 - Т | 16 - Я | 2 - Е | 7 – О |
| 6 – Н | 3 – А | 13 – Ы | 12 – Б |
| 15 – И | 10 - Ь | 8 - С | 1 –Р |
| 4 - Л | 5 – Ь | 11 - \_ | 14 - Т |

**Реальность\_бытия**

**Вывод:** при выполнении данной практической работы я научился пользоваться различными криптографическими алгоритмами симметричного шифрования, такие как: шифрование с использованием метода магического квадрата, систем Цезаря, системы Трисемуса, алгоритма Плейфера, системы Вижинера