Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №4**

**«Криптографическая защита информации»**

Выполнила:

Студентка 2 курса 1 группы ФИТ

Самсоник Анастасия Ивановна

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

1. Зашифровать сообщение (свою Фамилию Имя Отчество) с использованием:

○ Шифра Цезаря

○ Трисемуса,

○ Плейфейра

○ Вижинера

и полученного секретного ключа

(по номеру варианта (22) и ключевому слову «Защита»)

**Шифр Цезаря**

http://kriptografea.narod.ru/13.png*шифрование*

*http://kriptografea.narod.ru/14.png дешифрование*



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | С | А | М | С | О | Н | И | К | \_ | А | Н | А | С | Т | А | С | И | Я |
| Номер 1 | 19 | 1 | 14 | 19 | 16 | 15 | 10 | 17 | 16 | 1 | 15 | 1 | 19 | 20 | 1 | 19 | 10 | 33 |
| Номер 1+22 | 8 | 23 | 3 | 8 | 5 | 4 | 32 | 5 | 34 | 23 | 4 | 23 | 8 | 9 | 23 | 4 | 32 | 22 |
| Шифр | Ж | Х | В | Ж | Д | Г | Ю | А | \_ | Х | Г | Х | Ж | З | Х | Ж | Ю | Ф |

Исходный текст: САМСОНИК\_АНАСТАСИЯ

Зашифрованный: ЖХВЖДГЮА\_ХГХЖЗХЖЮФ

**Шифрующая система Трисемуса**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В |
| Г | Д | Е | Ж | Й | К | Л |
| М | Н | О | П | Р | С | У |
| Ф | Х | Ц | Ч | Ш | Ъ | Ы |
| Ь | Э | Ю | Я |  | . | , |

Исходный текст: САМСОНИК АНАСТАСИЯ

Зашифрованный: ЪДФЪЦХЖСТДХДЪЙЪЖИ

**Алгоритм шифрования Плейфера**

Ключ: Protection (защита)

З а щ и т б в г

Д е ж и к л м н

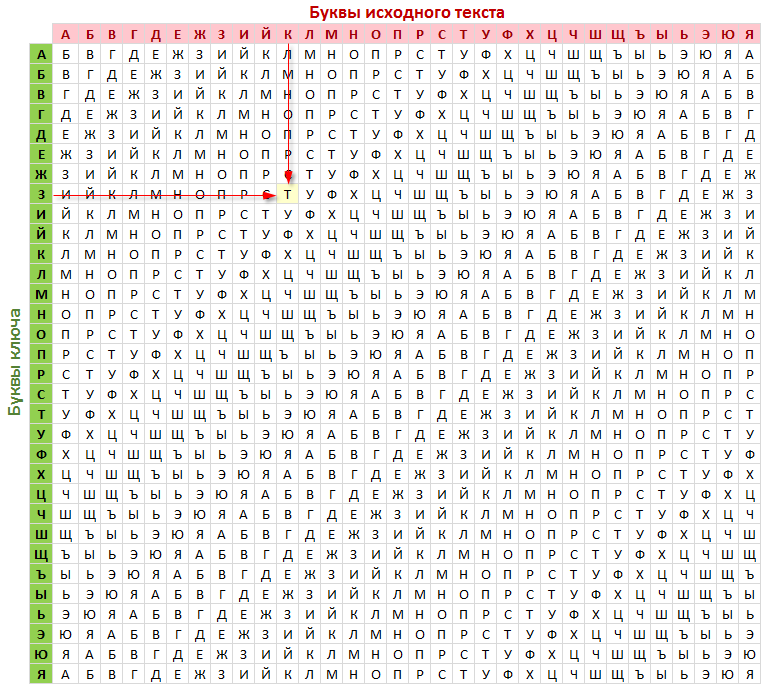
О п р с у ф х ц

Ч ш ъ ы ь э ю я

Исходный текст: СА МС ОН ИК АН АС ТА СИ ЯЪ

Зашифрованный: ПИ ХИ ДЦ КЛ ЕГ ИП БЩ ЫС ЧЫ

**Система Вижинера**



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Текст** | С | А | М | С | О | Н | И | К | А | Н | А | С | Т | А | С | И | Я |
| **Ключ** | З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т |
| **Шифр** | Щ | Б | Ж | Ъ | Б | Л | Ч | П | Ъ | С | А | Т | Ч | Б | Ь | Ф | Б |

1. Расшифровать следующие сообщения:

|  |  |
| --- | --- |
| **АМУМАФАССИ\_ТКРК\_** | Расшифровать с помощью Двойной перестановки по ключу.  **Ключ 1 ЗИМА**  **Ключ2 2341** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **А** | **З** | **И** | **М** |
| **1** | **2** | **3** | **4** |
| 1 | А | М | У | М |
| 2 | А | Ф | А | С |
| 3 | С | И | \_ | Т |
| 4 | К | Р | К | \_ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **А** | **З** | **И** | **М** |
| **1** | **2** | **3** | **4** |
| 2 | А | Ф | А | С |
| 3 | С | И | \_ | Т |
| 4 | К | Р | К | \_ |
| 1 | А | М | У | М |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **З** | **И** | **М** | **А** |
|  | **2** | **3** | **4** | **1** |
| 2 | Ф | А | С | А |
| 3 | И | \_ | Т | С |
| 4 | Р | К | \_ | К |
| 1 | М | У | М | А |

Расшифрованный текст: ФИРМА\_КУСТ\_МАСКА

Вывод: в ходе лабораторной работы изучены и применены на практике основы криптографических алгоритмов.