Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №4.1**

**Тема «Криптографическая защита информации»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 1 группы ФИТ

Немкович Анастасия Вадимовна

Минск 2023

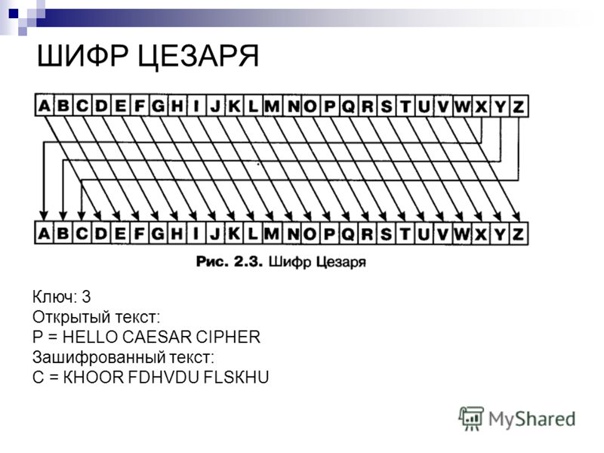
**Цель**

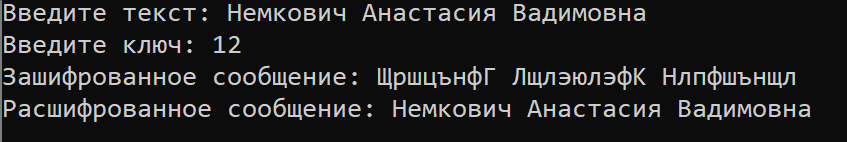
Овладеть основными криптографическими алгоритмами симметричного шифрования.

**Ход работы**

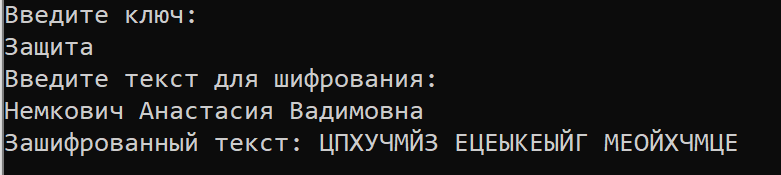
Симметричное шифрование – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

1) Зашифровать сообщение «Немкович Анастасия Вадимовна» шифром Цезаря с ключом 12. 

**Ответ**: 

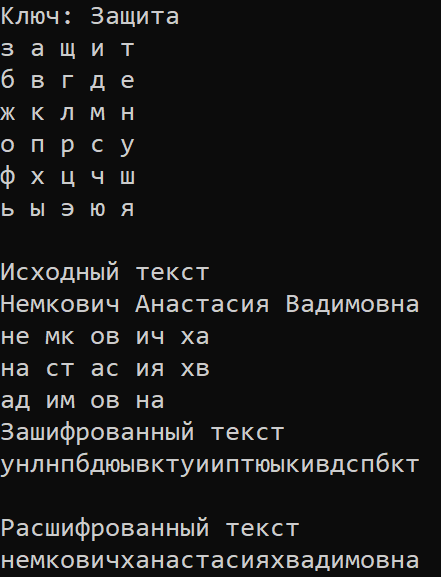
2) Зашифровать сообщение «Немкович Анастасия Вадимовна» шифром Трисемуса с ключевым словом «Защита» – таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку как в системе Цезаря с ключевым словом. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце.

**Ответ**: 

**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 Ь Ы Ъ Э Ю Я

3) Зашифровать сообщение «Немкович Анастасия Вадимовна» шифром Плейфейра с ключевым словом «Защита»

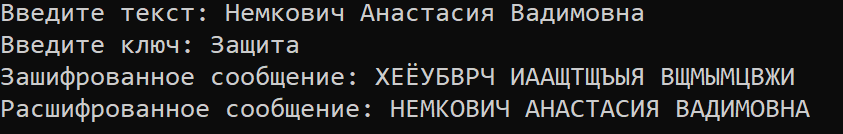
**Ответ:**

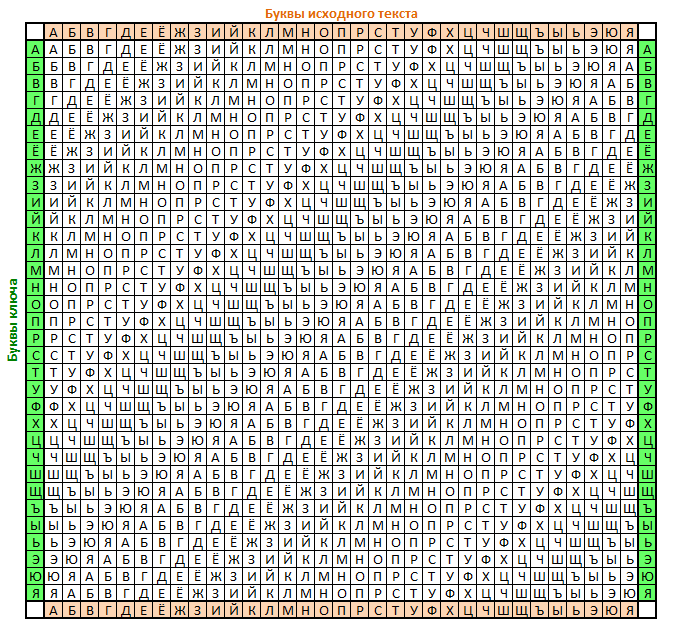


Шифрование происходит по следующим правилам:

1. Если обе буквы биграммы исходного текста не лежат в одной строке или в одном столбце, тогда находят буквы в углах прямоугольника, определяемого данной парой букв. Первой буквой биграммы шифртекста становится буква, расположенная в той же строке, что и первая буква исходной биграммы, и в том же столбце, что и вторая буква открытого текста. Вторая буква биграммы шифртекста находится на пересечении строки, содержащей вторую букву, и столбца, содержащего первую букву открытого текста.
2. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то первой и второй буквами биграммы шифртекста считаются буквы, лежащие справа, соответственно, от первой и второй букв биграммы открытого текста. При этом считается, что таблица циклически замкнута по строкам, то есть конец любой строки связан с ее началом. Поэтому если буквы биграммы расположены в одной строке и одна из них находится в последнем столбце таблицы, то для шифртекста берется буква из первого столбца этой строки.
3. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то первой и второй буквами биграммы шифртекста считаются буквы, лежащие, соответственно, под первой и под второй буквами биграммы открытого текста. При этом считается, что таблица циклически замкнута по столбцам, то есть конец любого столбца замыкается на его начале. Поэтому если буквы биграммы расположены в одном столбце и одна из них находится в последней строке таблицы, то для шифртекста берется буква из первой строки этого столбца.

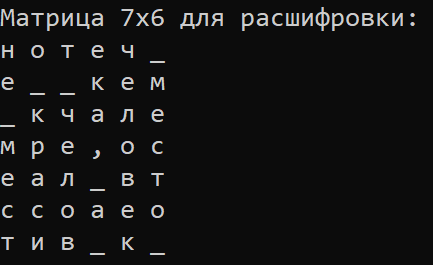
4) Зашифровать сообщение «Немкович Анастасия Вадимовна» шифром Вижинера с ключевым словом «Защита»

**Ответ**: 



|  |  |  |
| --- | --- | --- |
| 12. | нотеч\_е\_ \_кем\_кчалемре,осеал\_втссоаеотив\_к\_ | Расшифровать с помощью Метода простой перестановки Таблица6х7 |

Ответ: Не место красит человека, а человек место

****

**Вывод**

Криптография – это наука, изучающая и описывающая модели информационной безопасности (далее – ИБ) данных. Она позволяет разрешить многие проблемы, что присущи информационной безопасности сети: конфиденциальность, аутентификация, контроль и целостность взаимодействующих участников.

Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации.

Для защиты информации применяется шифрование – метод представления открытого текста в виде набора символов, скрывающего его содержания. Шифрование используется повсеместно: зашифровываются документы, информация в БД, пересылаемые по сети сообщения, в зашифрованном виде хранятся пароли пользователей компьютера. Для зашифровывания и расшифровывания используются программные и аппаратно-программные системы и комплексы криптографической защиты. Шифрование – это преобразование информационных данных в форму, которая будет не читабельной для программных комплексов и человека без ключа шифрования-расшифровки. Благодаря криптографическим методам защиты информации обеспечиваются средства информационной безопасности, поэтому они являются основной частью концепции ИБ.

Защита конфиденциальной информации, которая основана на криптографической защите, зашифровывает информационные данные посредством обратимых преобразований, каждое из которых описывается ключом и порядком, что определяет очередность их применения.

Ключ – это определенная последовательность символов, которая настраивает шифрующий и дешифрующий алгоритм системы криптозащиты информации. Каждое преобразование определяется ключом, задающим криптографический алгоритм, который обеспечивает безопасность информационной системы и информации в целом.