Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №4.1**

**«Криптографическая защита информации»**

Выполнил:

Студент 2 курса 2 группы ФИТ

Турчинович Никита

**Шифр Цезаря**

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении К = 3. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста.

**Текст для зашифровки:** Турчинович Никита Александрович

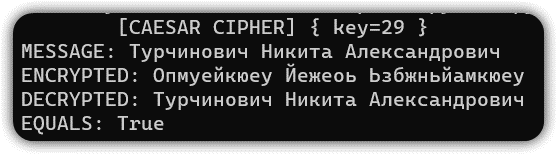
**Ключ:** 29

**Результат шифровки:** Опмуейкюеу Йежеоь Ьзбжньйамкюеу

**Код:**



**Вывод:**



**Шифр Трисемуса**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифрования.

**Текст для зашифровки:** Турчинович Никита Александрович

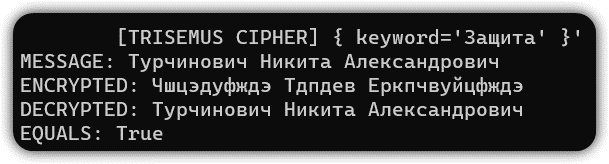
**Секретное слово:** Защита

**Результат шифровки:** Чшцэдуфждэ Тдпдев Еркпчвуйцфждэ

**Код:**



**Вывод:**



**Шифр Плейфейра**

Шифр Плейфейра, изобретенный в 1854 г., является наиболее известным биграммным шифром замены. Он применялся Великобританией во время первой мировой войны. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущего раздела.

Процедура шифрования включает следующие шаги:

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

2а. Если обе буквы биграммы открытого текста не попадают на одну строку или столбец , тогда находят буквы в углах прямоугольника, определяемого данной парой букв.

2б. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними. Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца.

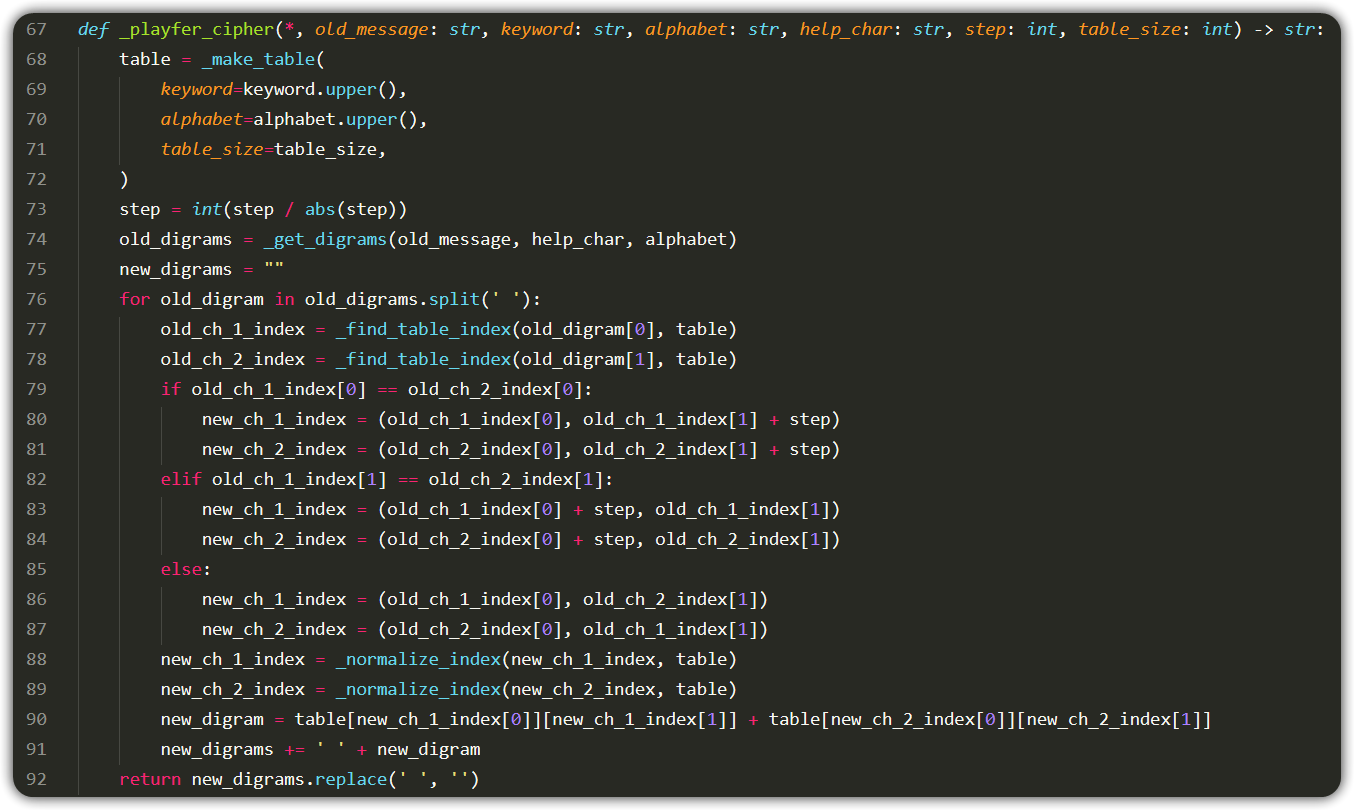
2в. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке.

**Текст для зашифровки:** Турчинович Никита Александрович

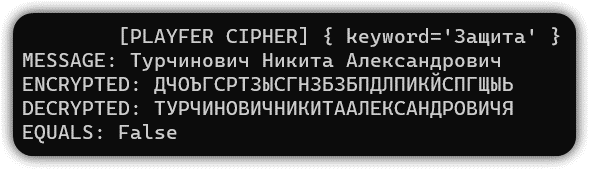
**Секретное слово:** Защита

**Результат шифровки:** ДЧОЪГСРТЗЫСГНЗБЗБПДЛПИКЙСПГЩЫЬ

**Код:**



**Вывод:**



**Шифр Виженера**

В 15 веке был впервые придуман, а потом в 16 веке французским дипломатом Блезом Виженером официально представлен более совершенный метод на основе шифра Цезаря, получивший впоследствии название "шифр Виженера". Его принцип в том, что каждая буква в исходном шифруемом тексте сдвигается по алфавиту не на фиксированное, а переменное количество символов. Величина сдвига каждой буквы задается ключом (паролем) - секретным словом или фразой, которая используется для шифрования и расшифровки.

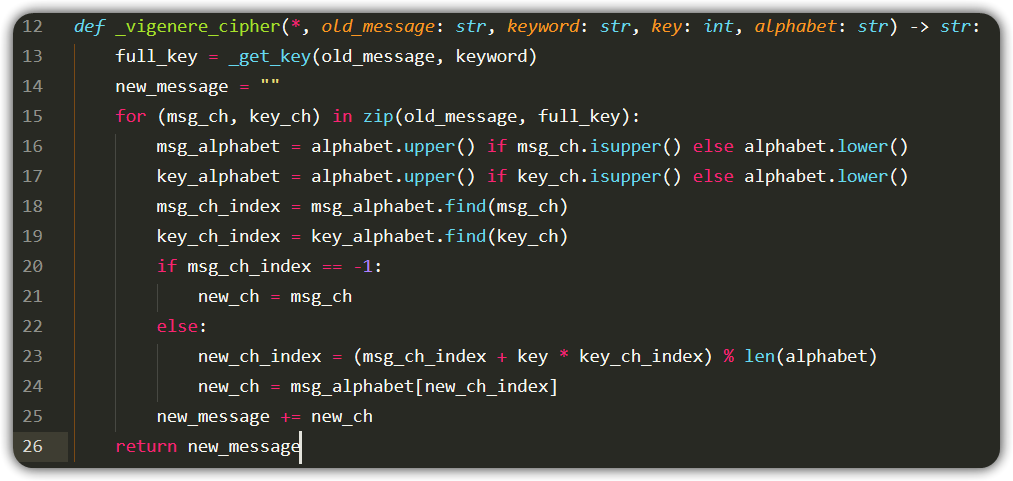
**Текст для зашифровки:** Турчинович Никита Александрович

**Ключ:** 29

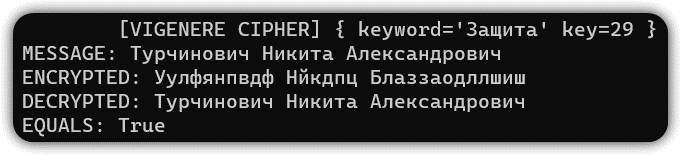
**Секретное слово:** Защита

**Результат шифровки:** Уулфянпвдф Нйкдпц Блаззаодллшиш

**Код:**



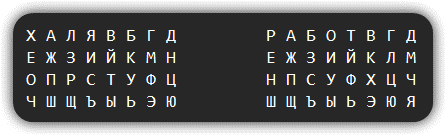
**Вывод:**



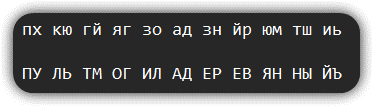
**Задание по варианту**

|  |  |  |
| --- | --- | --- |
|  | Расшифровать с помощью шифра **Двойного квадрата Уитстона** | **Ключ 1 ХАЛЯВА Ключ 2 РАБОТА** |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **пх** | **кю** | **гй** | **яг** | **зо** | **ад** | **зн** | **йр** | **юм** | **тш** | **иь** | | | |

**Таблицы для шифра**



**Дешифровка**



**Код**



**Вывод**

