Министерство образования Тульской области
Государственное профессиональное образовательное учреждение
Тульской области
«Донской политехнический колледж»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКОЙ РАБОТЫ

по МДК.02.02 «Криптографические средства защиты информации»

по теме «Симметричное шифрование: шифрование по таблице Виженера»

для обучающихся по программе подготовки специалистов среднего звена

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Автор:

Е.А. Филатова, преподаватель ГПОУ ТО «ДПК»

2025 г.

Лист согласования:

Автор разработки:

Филатова Е.А., преподаватель ГПОУ ТО «ДПК»

Рецензенты:

Евтехова О.А., заместитель директора по учебно-методической и научной работе ГПОУ ТО «ДПК»

Панченко Т.А., заместитель директора по организации образовательного процесса ГПОУ ТО «ДПК»

Ишутина О.В., заведующий методическим кабинетом ГПОУ ТО «ДПК»

Методические рекомендации предназначены для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, изучающих курс «Криптографические средства защиты информации» по теме «Симметричное шифрование: шифрование по таблице Виженера» и содержат основные теоретические сведения по применению алгоритма шифрования Виженера, приводится образец выполнения задания, представлены варианты индивидуальных практических заданий.

СОГЛАСОВАНО
на заседании предметной (цикловой) комиссии дисциплин профессионального цикла отделения «Информационная безопасность и администрирование»
Протокол № 1
от «01» сентября 2025 г.
Председатель ПЦК Панкова М.А.

СОДЕРЖАНИЕ

Практическая работа

Тема работы: Шифрование по таблице Виженера

Цель работы: получение навыков создания зашифрованного (расшифрованного) сообщения с использованием алгоритма шифрования Виженера.

Задачи:

- научиться зашифровывать и расшифровывать сообщения с использованием алгоритма шифрования Виженера;
- закрепить навыки работы в программной среде Microsoft Excel для реализации алгоритма шифрования Виженера;
- закрепить навыки работы в среде Visual Studio с использование языка программирования Python для реализации алгоритма шифрования Виженера.

Теоретические сведения:

Шифр Виженера (фр. Chiffre de Vigenère) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Таблица Виженера (табл. 1) представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. Ниже показана таблица Виженера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размешается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе. Пример такой рабочей матрицы для ключа ДОНСКОЙ приведен на рис. 1.

Таблица Виженера *Таблица 1*

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

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

Рисунок 1 - Рабочая матрица для ключа ДОНСКОЙ

Процесс шифрования осуществляется следующим образом:

1) под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;

2) каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;

3) полученный текст может разбиваться на группы по несколько знаков.

Пусть, например, требуется зашифровать сообщение: БЮРЯ МГЛОЮ НЕБО КРОЕТ. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа получаем:

б	у	р	я	м	г	л	о	ю	н	е	б	о	к	р	о	е	т
д	о	н	с	к	о	й	д	о	н	с	к	о	й	д	о	н	с

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (Б) и соответствующую ей букву ключа (Д); по букве шифруемого текста (Б) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (Д), — в нашем примере такой буквой является Е; выбранную таким образом букву помещаем в шифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

На рис. 2 представлена схема шифрования.

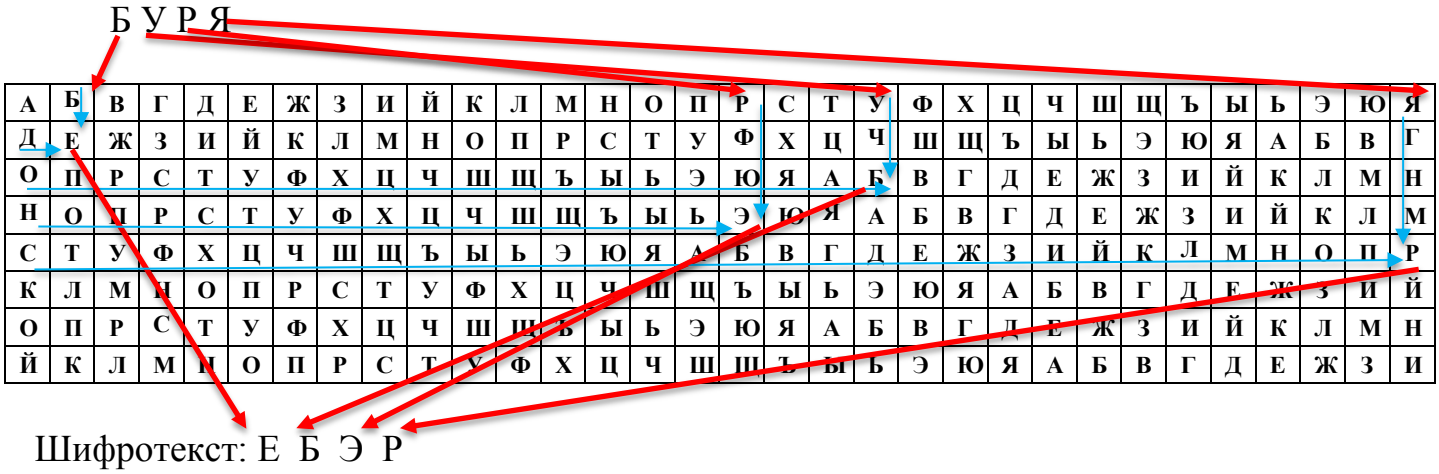


Рисунок 2 - Последовательность шифрования по таблице Виженера с использованием ключа «ДОНСКОЙ»

Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по таблице Виженера эквивалентна простой замене с циклическим изменением алфавита, т. е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т. е. на число букв в ключе.

Расшифровка текста производится в следующей последовательности:
1) над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз;
2) в строке подматрицы Виженера, соответствующей букве ключа, отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста;
3) полученный текст группируется в слова по смыслу.

д	о	н	с
е	б	э	р

На рис. 3 данная процедура представлена в наглядном виде.

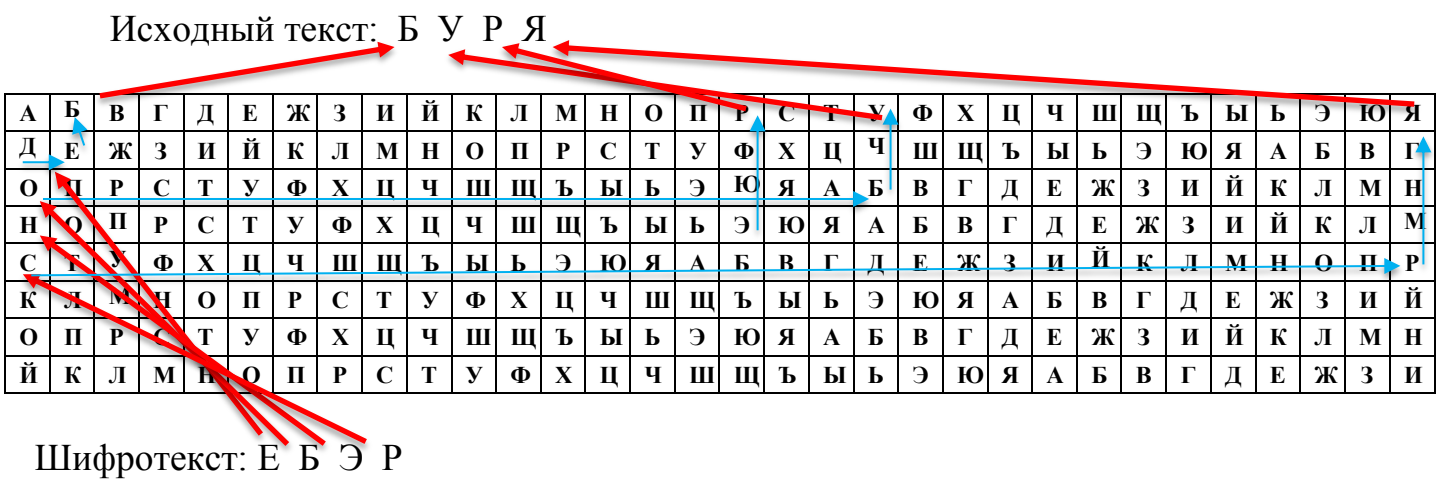


Рисунок 3 - Последовательность расшифровки по таблице Виженера с использованием ключа «ДОНСКОЙ»

Нетрудно видеть, что процедуры как прямого, так и обратного преобразований являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Виженера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

Задания к практической работе

Задание 1. Используя таблицу Виженера (табл.1), составьте рабочую матрицу для ключа и зашифруйте сообщение. Ключ и сообщение выбираются по варианту из таблицы 2.

Задание 2. Используя таблицу Виженера (табл.1), составьте рабочую матрицу для ключа и дешифруйте сообщение. Ключ и сообщение выбираются по варианту из таблицы 2.

Варианты сообщений к заданиям 1, 2 *Таблица 2*

вариант	*ключ*	*Сообщение к заданию 3*	*Сообщение к заданию 4*
1	БРАУЗЕР	ЗИМОЙ И ЛЕТОМ ОДНИМ ЦВЕТОМ.	ФЗЕАППРНЗТБИАЯСХУДЦК ВЭЭАЧХЙЮДЮНТЩБВЖЕК ЕХЗЯЖАЕЧПНЭЖЦДУЩБВ ЖЕКЕХФЮИРДЫ
2	ЛЕОНАРД	ГУСЬ СВИНЬЕ НЕ ТОВАРИЩ.	ШНШНКЮЙПКЩЫНХПЗМ НВОАТГУЯСЕЫДЭБУЮЛШ СРНХПЕБЦШУЕТГЮЩЩЧН ЯДЮХЭНСЪУВА
3	ЭЙДЕЛЬМАН	НА ВКУС И ЦВЕТ ТОВАРИЩЕЙ НЕТ.	ЯЪЦЕЫКЭТХКОЦРЮУДЕРЛ ЬЦКГБЩИМФОРЦЩГЩАЪЕ ОЦУОКГТЫЯЪЙЦУЗЗВЩЛФ ТЙЩНЮИЫПНДТЖАСЛАЗЧ ЦУЫКСНТОЫДХРБЮ
4	АЛГОРИТМ	СЫТЫЙ ГОЛОДНОГО НЕ РАЗУМЕЕТ.	ОМУОЧЩФМНУИЛВЦДЪЧЭ СЬБЪТСТЬВЭЮЩЭСТЩЖЬ ЪИЬУАМЮРРНДЭЯНФУТГЕ ГЕШРЬХККЦОЦИ
5	МАТЕРИК	ГЛАЗА БОЯТСЯ, А РУКИ ДЕЛАЮТ.	ОДФУЩХПЮЯШКЫНПЫЕВ КЭЦЫФТОУСРОЗСАЦВЦЪЪ ННЧХЭХКДЧОЮЪФЪТАХЛ ЭЦЗВГКУЦЦСНЧКТЧЪМВЧ УЦРОМТОНЕ
6	КОНВЕРТ	ДАЛЬШЕ ЗЕМЛИ НЕ УПАДЕШЬ.	ЭЯЬЗЪЮГЬЮЫЕУБЭШРНЙЕ ТЪЫЦЯГУЫЧПЬЯХЪРГХБЕ ВГЙЧНЬДЗСЮДЙХИМЕУА МЬЭБЮХХШ
7	ДИЗАЙНЕР	ДЕЛО МАСТЕРА БОИТСЯ.	ПЖИОЛЙЖХКРЩОЫЯКЕОЪ ХГЧЪНВХЗОАЦТГРЦНУКЫ ЫФАТЯГБОУНВОРЛАОЯЦП СИЯЕЗ

8	ТЕХНИКУМ	ДРУЗЬЯ ПОЗНАЮТСЯ В БЕДЕ.	ЬУШСИОГЯШЖХЪИБЫЩТ КЗЮУКФСДБЭЫЭХУТЦЕЗЙ ЩЙБЩТЗЖТЛОУЫВНЦТЛК ШЮЬШЖХУПАЩАОЧТОХ ЫОАЦЗХ
9	КАМЕРТОН	ЖИЗНЬ ПРОЖИТЬ — НЕ ПОЛЕ ПЕРЕЙТИ.	БТЪЖЛААТЛЕЩНФЕЪНХИР КЫТЧЯШЧЮУВНЯДТТМКИ ОЯЬЪАОКФЭЦПЕМ
10	МАРКЕТИНГ	КАК АУКНЕТСЯ, ТАК И ОТКЛИКНЕТСЯ.	ЩЕУШТССЮВУАББЕГЪЙИ ШОЭШЗГНРЗМНРЯУЦРЯФЛ ВВПЖЧЩНПЪМ
11	ГОСУДАРЬ	КАШУ МАСЛОМ НЕ ИСПОРТИШЬ.	НБТБОЖШГРЦТОПБЛНООХ БОДЮЛУЦГБФНЮНХЦЦДП ИСЧРУАУИАЫКЕЫЦЦТГЮ МЯШЩИХЛХГ
12	ТРАПЕЦИЯ	ЛЕС РУБЯТ — ЩЕПКИ ЛЕТЯТ.	ЯХУУЕНИЬДЮВЭМВЦЕЯЮ СББГИЦТВЬАТДКЯЯЮУХК ЧЦКЧХМВЙЖЦ
13	ДОКУМЕНТ	МЯГКО СТЕЛЕТ, ЖЁСТКО СПАТЬ.	ООЪУЩЙНКЫАШФЗФХГДА ЖУШУШАЦЕЬБНАЧАЖОЬП
14	КОМПЬЮТЕР	НА ВОРЕ ШАПКА ГОРИТ.	ХМРЧЖМДУАЕУЩПИЛЕЛЭ ЕРЭФЯВТМРЧНЮКЭМЭБИП ЫМА
15	МЕЛЬНИЦА	НАШ ПОСТРЕЛ ВЕЗДЕ ПОСПЕЛ.	ТКШХХХСЭЮУШБЮУЦБЗО ЪКШЩБАНАФЛЫУУТЪИШ ДШГЫДЪЦХД
16	ЛЕЙКОЦИТ	СТАРЫЙ ДРУГ ЛУЧШЕ НОВЫХ ДВУХ.	ШЕНФБЗРФКЖФШШДКГРИ НКЭЖРСЭТОУБШРЦРЧЕМЫ ЫФИРРЧНЬННВНДУКЕЫФБ ЩРЧМЦГТЕ
17	ГИПОТЕЗА	УЧЕНЬЕ СВЕТ, А НЕ УЧЕНЬЕ ТЬМА.	НЪЭЫЪПХГЗИЬЦЯЕЮТСХФ ЮТЦШЧЛЪКРТКЩНЛТЭСЦ ЕФЕДЫУУДХЗЗСЯПЮАЗЗН
18	РОДИНКА	НЕ ИМЕЙ СТО РУБЛЕЙ, А ИМЕЙ СТО ДРУЗЕЙ.	ЭОЗЦШШДЭЙНОТХУФЬОШ АЫСЪЦНЯТХОТУОХХБЕУЬ ИНШКТМЦИЫЩКТМЫЙЭЫ БЕВОСИЮЕТЛЧСНЩШЖХА
19	ФЕОДАЛИЗМ	РЫБУ ЗА ХВОСТ НЕ УДЕРЖАТЬ.	ЪНХСЬЬУПДЮУЪООЫЦЩЦ ФЬАТБЖЪЧМЖНААЕРХЗРЬ КАЯЖЛМФЗЙСБКЧУХПЫЯ УГТЕШИШЮДУУСИР

20	СУВЕНИР	КТО МАЛО ВИДЕЛ, ТОТ МНОГО ПЛАЧЕТ.	ЦДННДНЫЯХЗПРЦТЯГКЧД ЪЮЮШЧУДНВХЖОЕЯДЮИ ШОЧЫПЭСККЧЫХЬЯЩЗЧС ЫЬСЕЮЧЫУМЫБРЖКЪЮЭ
21	ТЕКСТИЛЬ	АППЕТИТ ПРИХОДИТ ВО ВРЕМЯ ЕДЫ	ЪТШФЦИЪКЭКСЮАЦЭЦЧЪ КГОЧЩАТРЖЙЧЯЭКУАЪС ЩЛЦЫЦКЬНДЦВОАФШВДЦ КЙЯУЧСЗЦПДДЦЙДДНМЫБ КЪЦЦЛЦЬЩЕЦЩ
22	ФУНКЦИЯ	БОЛЬШОЕ ВИДИТСЯ НА РАССТОЯНИИ	ЯШЧКЖЩСЦУСПЯЩСЦЖЛ ЬШГАВГЫБГЦСЩЭЯШШХЗ ЙХТЪХЪБПЪСШЖИБЯЫПК ФЪЯЮЕЫЧЫКДДЫЯЩЖЦГ ВЮУКФЪАВЮТЬТ
23	ФАКТОРИАЛ	СВЕЖО ПРЕДАНИЕ — ДА ВЕРИТСЯ С ТРУДОМ	ЩСХЪТЛФСЭЩЛПДЯПЧОТ ЩМХЧРХШНУЖЕЫОЦТГК ЦТЧТДУГЪЮОЩСХЪЭЮМ НУААПДЯПЩТЩЯБШЮЪЮ ОЕЭЩУРЧЫХКОТЦРКЛОВД СК
24	СРЕДСТВО	СЕМЬ РАЗ ОТМЕРЬ — ОДИН ОТРЕЖЬ	ЭГЙФЯГФКААНЩЯЦКАЫЮ ИИСЩПОРУХДЮЪШЙВТУ МЖФРХЭЮЛСЯГФУЪТЦЙБ ТДЫЯТАОЬТЖЙУРКЬНГБТЯ ЪУСЗТ
25	КОМБАЙН	СЧАСТЛИВЫЕ ЧАСОВ НЕ НАБЛЮДАЮТ	БУЧПВОЧЛУУИНЙЪТЧОТЕ ЩНМЫЪШТЧРЪЦНЦОЫМЧ ООИГФМОЦЦСЕШЧТЧМИА РТЦЩКРЛЧВШТССЖСЯЫН

Задание 3. Освоить технологию шифрования и дешифрования информации в среде Excel с использованием шифра Виженера. Сообщение выбирается по варианту из табл. 2.

Порядок выполнения задания 3

1. Загрузите программу Microsoft Excel. Создайте новый документ.
2. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).

	A	B	C
1	а	0	а
2	б	1	б
3	в	2	в
4	г	3	г
5	д	4	д
6	е	5	е
7	ж	6	ж
8	з	7	з
9	и	8	и
10	й	9	й
11	к	10	к
12	л	11	л
13	м	12	м
14	н	13	н
15	о	14	о
16	п	15	п
17	р	16	р
18	с	17	с
19	т	18	т
20	у	19	у
21	ф	20	ф
22	х	21	х
23	ц	22	ц
24	ч	23	ч
25	ш	24	ш
26	щ	25	щ
27	ъ	26	ъ
28	ы	27	ы
29	ь	28	ь
30	э	29	э
31	ю	30	ю
32	я	31	я

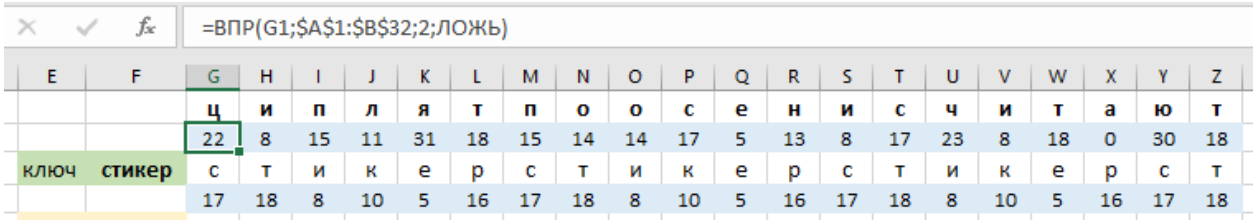
3. Введите побуквенно шифруемое слово в ячейки строки;

G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ц	**и**	**п**	**л**	**я**	**т**	**п**	**о**	**о**	**с**	**е**	**н**	**и**	**с**	**ч**	**и**	**т**	**а**	**ю**	**т**

4. Строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР

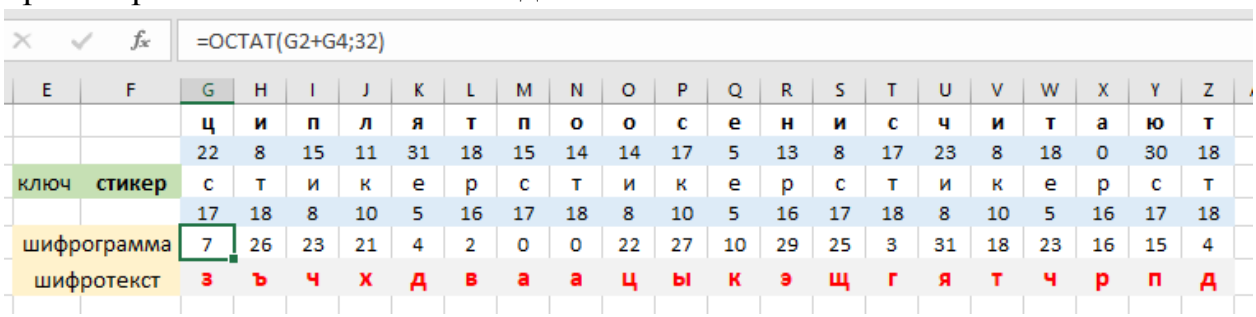
5. Строкой ниже ввести побуквенно ключ шифра Виженера, циклические повторяя его, пока не будет достигнут конец шифруемого слова

6. Строкой ниже получить числовой код символов ключевой строки с помощью функции ВПР;



7. Строкой ниже получить код символа криптограммы, сложив по модулю (по количеству букв в алфавите) полученный код текущего символа шифруемого слова с кодом текущего символа ключевой строки, используя функцию ОСТАТ;

8. Строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид



		G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		ц	и	п	л	я	т	п	о	о	с	е	н	и	с	ч	и	т	а	ю	т
		22	8	15	11	31	18	15	14	14	17	5	13	8	17	23	8	18	0	30	18
ключ	стикер	с	т	и	к	е	р	с	т	и	к	е	р	с	т	и	к	е	р	с	т
		17	18	8	10	5	16	17	18	8	10	5	16	17	18	8	10	5	16	17	18
шифрограмма		7	26	23	21	4	2	0	0	22	27	10	29	25	3	31	18	23	16	15	4
шифротекст		з	ъ	ч	х	д	в	а	а	ц	ы	к	э	щ	г	я	т	ч	р	п	д

9. Сравните полученный закрытый текст с результатом в задании 1.
10. Ниже приготовьте место для дешифрования информации. Впишите закрытый текст побуквенно в ячейки строки.
11. Строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР;
12. Строкой ниже сформировать ключевую строку;
13. Строкой ниже получить числовой код символов ключевой строки с помощью функции ВПР;
14. Строкой ниже получить код символа открытого текста, вычтя по модулю 32 (по количеству букв в алфавите) код текущего символа ключевой строки из кода текущего символа криптограммы, используя функцию ОСТАТ;
15. Строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид.

		з	ъ	ч	х	д	в	а	а	ц	ы	к	э	щ	г	я	т	ч	р	п	д
		7	26	23	21	4	2	0	0	22	27	10	29	25	3	31	18	23	16	15	4
ключ	стикер	с	т	и	к	е	р	с	т	и	к	е	р	с	т	и	к	е	р	с	т
		17	18	8	10	5	16	17	18	8	10	5	16	17	18	8	10	5	16	17	18
шифрограмма		22	8	15	11	31	18	15	14	14	17	5	13	8	17	23	8	18	0	30	18
шифротекст		ц	и	п	л	я	т	п	о	о	с	е	н	и	с	ч	и	т	а	ю	т

16.Сравните полученный результат с результатом в задании 2.
17.Предъявите работу преподавателю.

Задание 4. Составить программу шифрования и дешифрования информации работы в среде Visual Studio с использование языка программирования Python для реализации алгоритма шифрования. Сообщение выбирается по варианту из табл. 2.

Порядок выполнения задания 4

1. Создать проект в среде Visual Studio с использование языка программирования Python для шифровки и дешифровки.
2. Выполнить шифровку и дешифровку шифротекстов.
3. Сравнить полученный результат с результатом в задании 2.

ПРИЛОЖЕНИЕ А

ОТВЕТЫ

вариант	***ключ***	***зашифровка***	***расшифровка***
1	браузер	ишмбрныжвояхйэйьцхмчюн	Ученикам, чтобы преуспеть, надо догонять тех, кто впереди, и не ждать тех, кто позади.
2	леонард	ошяйстмшбуъевтнеюхщ	Никакое дело нельзя хорошо сделать, если неизвестно, чего хотят достигнуть.
3	эйдельман	кйжпюнфцпвыцунььижвтскэ	В старости нет лучшего утешения, чем сознание того что все силы в молодости отданы делу, которое не стареет.
4	алгоритм	сжхйщлачопрьуцясрлкбьнчю	Образование - это то, что остаётся после того, как забывается всё выученное в школе.
5	материк	плтмрйшлтгдршэцицкыиию	Вдвойне тяжелее переносить обиды со стороны тех людей, от которых мы всего менее вправе ожидать их.
6	конверт	оошюэхщпъшктхещосзэм	Успех острого слова зависит более от уха слушающего, чем от языка говорящего.
7	дизайнер	интохнцвйшзбчхчбг	Любовь бежит от тех, кто гонится за нею, а тем, кто прочь бежит, кидается на шею.
8	техникум	цхифдйвъщтхлъытоукщт	Когда дружба начинает слабеть и охлаждаться - она всегда прибегает к усиленной вежливости.
9	камертон	риутмбюыриюбэчэыхеыкаччят	Что бы о тебе ни думали, делай то, что ты считаешь справедливым.
10	маркетинг	цаъкшьхтхэявкпъцянчиъчкдщм	Не гоняйся за счастьем: оно всегда находится в тебе самом.
11	государь	нойжрабзсъюшмсякуащла	Кубок жизни был бы сладок до приторности, если бы не падало в него горьких слез.
12	трапеция	эхсяшчзслхпщнбнссв	Неудача это возможность начать снова, но уже более мудро.

13	документ	рннэъцячпуьщсцяьтящуюб	Карандаш, чтобы писать, а молот, чтобы ковать.
14	компьютер	чооэмгкеяфопэмжд	Люди, которые нам нужны, всегда заняты больше нас.
15	мельница	щеглыщирсрнбфмыпъцъбш	Женщины – это не слабый пол, слабый пол – это гнилые доски.
16	лейкоцит	ьчйъйямвюифэеонящздятшыз	Надкусив яблоко, всегда приятней увидеть в нем целого червяка, чем половинку.
17	гипотеза	цяфыокшвиъпычшюердфаосз	Кто никогда ни на что не рассчитывает, никогда не будет разочарован.
18	родинка	эумфтусвьфыохещомфтусвьишасещ	На голодный желудок русский человек ничего делать и думать не хочет, а на сытый - не может.
19	феодализм	дапчзлэйъечыйупнчтфчк	Жизнь слишком коротка, чтобы тратить ее на диеты, жадных мужчин и плохое настроение.
20	сувенир	ыерснуюуыжкшъюгяпурцяьущкя	Если человек говорит, что не хочет думать о чем-то, значит, он может думать только об этом.
21	текстиль	тфщцдрэлвняяцрэюазъцюзран	Иногда полезно отъехать подальше, чтобы разглядеть то, что постоянно находится у тебя перед глазами
22	функция	хбшжоцдцыстищюбуэкзщсвтътю	Лекарства действуют выборочно: те, кто в них верят, выздоравливают, а кто не верит — продолжают болеть.
23	факториал	евпшьяшепфнтчтркеыьтысявшупвм	Если дым стелется по земле - вернитесь и выключите утюг, если поднимается столбом - можете уже не возвращаться
24	средство	вхсабтйьгькфнажцюючфцшю	Мудрость приходит, когда, зная границы своих возможностей, все равно выкладываешься до конца
25	комбайн	ыемттфхмйсшаъымысоакшитмят	Человек без знаний – все - равно, что гриб: хотя на взгляд и крепкий, а за землю плохо держится

ПРИЛОЖЕНИЕ Б

Критерии оценивания

«Отлично» — Выполнены верно все 4 задания.

В задании 1, 2 полностью понимает и правильно применяет алгоритм шифрования и расшифровки Виженера; успешно демонстрирует навыки шифрования и расшифровки без ошибок; может объяснить принцип работы.

В задании 3 создана полностью рабочая таблица с формулами, корректно реализует шифрование и расшифровку.

В задании 4 программа выполняет поставленную задачу без ошибок с любыми введёнными строками и ключами. Написан чистый, структурированный и эффективный код, правильно реализован алгоритм шифрования и расшифровки; имеются комментарии, код структурирован.

Результаты выполнения совпадают во всех заданиях.

«Хорошо» — Выполнены 4 задания.

В задании 1, 2 в целом правильно использует алгоритм, допускает незначительные ошибки; способен зашифровать и расшифровать сообщения, показывает хорошее понимание.

В задании 3 реализованы основные функции без ошибок, допускает небольшие недочеты в оформлении или комментировании.

В задании 4 программа выполняет задачу, но может содержать незначительные ошибки или недоработки. Основная часть кода работает корректно, есть небольшие недочеты или комментарии, но алгоритм реализован верно.

Результаты выполнения совпадают во всех заданиях.

«Удовлетворительно» — Выполнены 4 задания.

В задании 1, 2 владеет базовыми навыками, допускает некоторые ошибки или пропуски в понимании; выполняет задания с подсказками или повторно.

В задании 3 реализовано шифрование/расшифровка с помощью таблиц, но есть ошибки или недочеты в логике или оформлении.

В задании 4 программа выполняет задачу с ошибками и может не справляться с некоторыми случаями, требуется доработка для полной работоспособности.

Результаты выполнения совпадают во всех заданиях.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М.Е.Ильин, Т.И.Калинкина, В.Н.Пржегорлинский. — М.: Издательский центр «Академия», 2019. — с. 272
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие [Текст] / В.Ф. Шаньгин – М : ИД «Форум»: ИНФА-М, 2024. – 416 с.: ил.– (Профессиональное образование).