МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ИНСТИТУТ ЦИФРОВЫХ ТЕХНОЛОГИЙ, ЭЛЕКТРОНИКИ И ФИЗИКИ (ИЦТЭФ)

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ЭЛЕКТРОНИКИ (ВТиЭ)

**Отчет по лабораторной работе № 5**

по курсу “Защита информация”

**“Конфиденциальность информации.**

**Простейшие методы шифрования данных.”**

Выполнил студент 506 гр.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Осипенко

Проверил: ст. преп. кафедры ИБ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.С. Ладыгин.

Лабораторная работа защищена

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 1. Шифр Цезаря

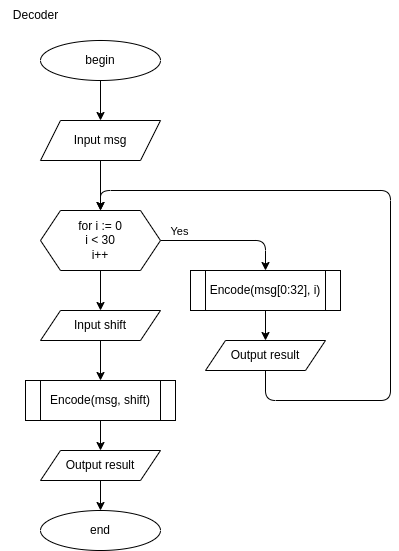
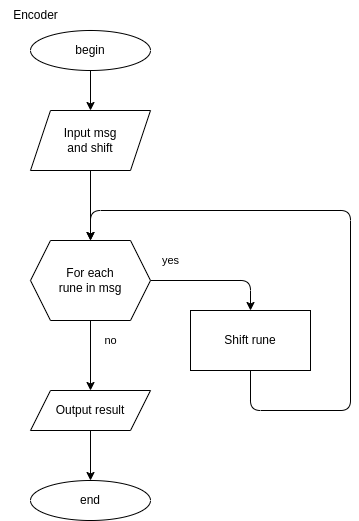


Рис 1.1 Блок схемы шифратора и дешифратора

**Листинг 1.1:** Исходный код шифратора и дешифратора.

func CEAEncoder(msg string, shift int) string {

msg = strings.ToLower(msg)

msgArray := []rune(msg)

var outBuf bytes.Buffer

for \_, rn := range msgArray {

res := MakeShift(rn, shift)

outBuf.WriteRune(res)

}

return outBuf.String()

}

func CEADecode(msg string) string {

for i := 0; i < len(alphabet); i++ {

res := CEAEncoder(msg[:32], i)

fmt.Printf("Shift #%d: %s...\n", i, res)

}

var shift int

fmt.Print("Select mode: ")

fmt.Scanf("%d", &shift)

return CEAEncoder(msg, shift)

}

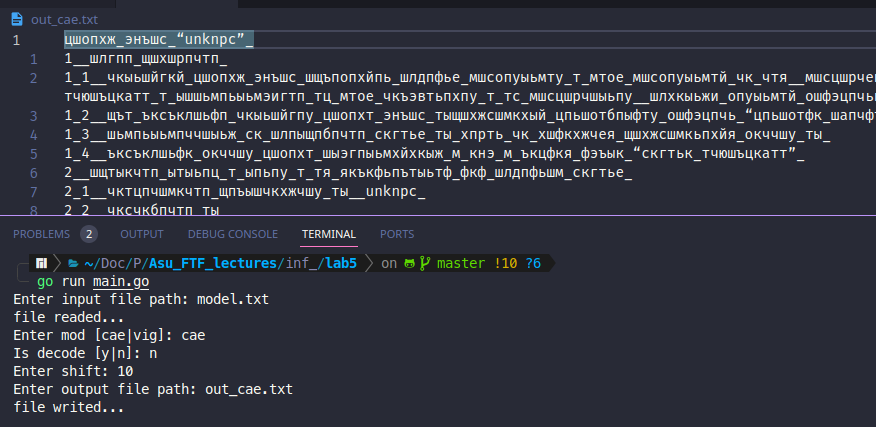


Рис 1.2 Пример использования шифров Цезаря

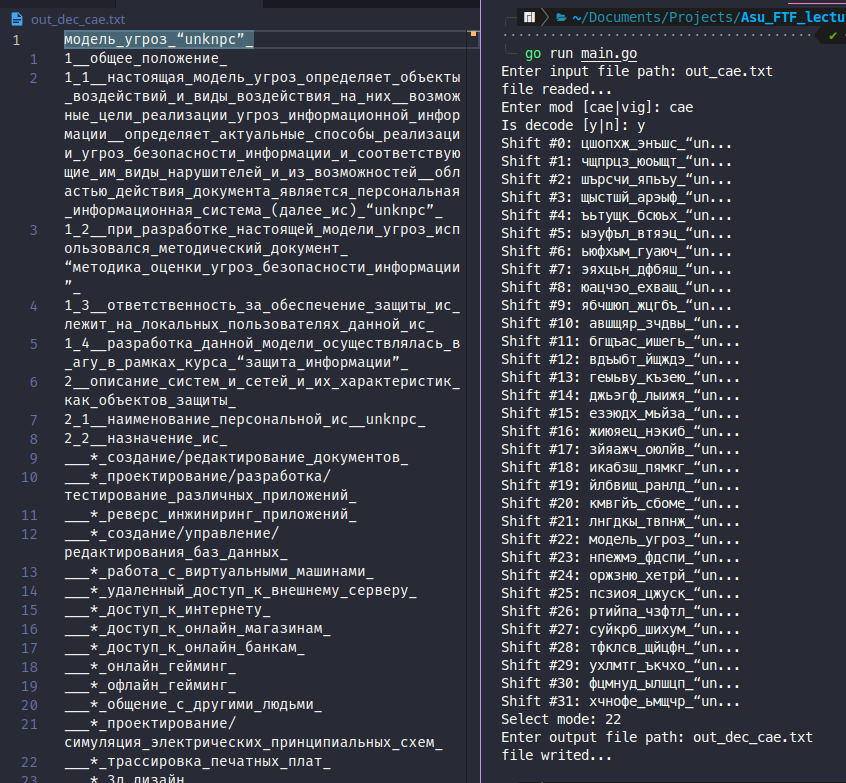


Рис. 1.3 Пример декодирования шифра Цезаря.

# 2. Шифр Виженера

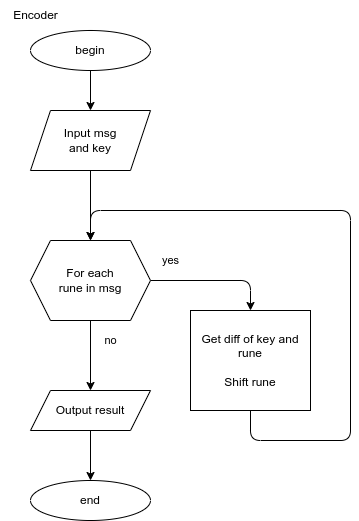


Рис 2.1 Блок схемы шифратора

**Листинг 2.1:** Исходный код шифратора.

func VIGEncoder(msg string, key string) string {

msg = strings.ToLower(msg)

key = strings.ToLower(key)

msgArray := []rune(msg)

keyArray := []rune(key)

var resBuf bytes.Buffer

for i, ch := range msgArray {

k := keyArray[i%len(keyArray)]

resBuf.WriteRune(MakeShift(ch, int(k-alphabet[0])))

}

return resBuf.String()

}

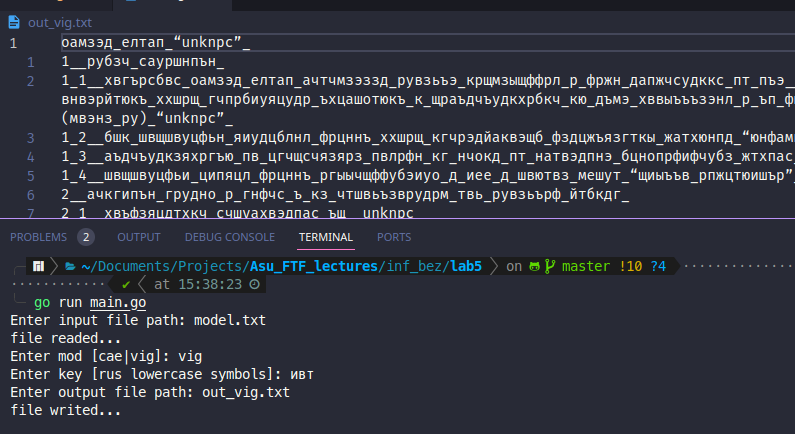


Рис 2.1 Пример работы шифра Виженера

# Вывод

В ходе данной работы были изучены и разработаны программы для работы с шифрами Цезаря и Виженера.

# Контрольные вопросы

1) Какой метод шифрования данных наиболее надежен на сегодняшний день?

*На сегодняшний день, наиболее надежными методами шифрования данных считаются алгоритмы, основанные на криптографии с открытым ключом (Public Key Cryptography, PKC), такие как RSA, ECC (Elliptic Curve Cryptography), и алгоритмы, основанные на криптографии симметричным ключом (Symmetric Key Cryptography, SKC), такие как AES (Advanced Encryption Standard).*

2) В каких сферах деятельности обычного пользователя встречается потребность в шифровании данных?

*1. Персональные и семейные архивы: Шифрование помогает защитить семейные фотографии, документы и другие личные данные от несанкционированного доступа.*

*2. Социальные сети и мессенджеры: Шифрование используется для защиты личных сообщений, фотографий и других данных пользователей.*