Российский университет дружбы народов
Научный факультет
Математические основы защиты информации и информационной безопасности

Модель шифрования цезаря и atbash

Подготовлено студентом:

Елиенис Санчес Родригес.

Преподаватель:

Дмитрий Сергеевич

шифрование

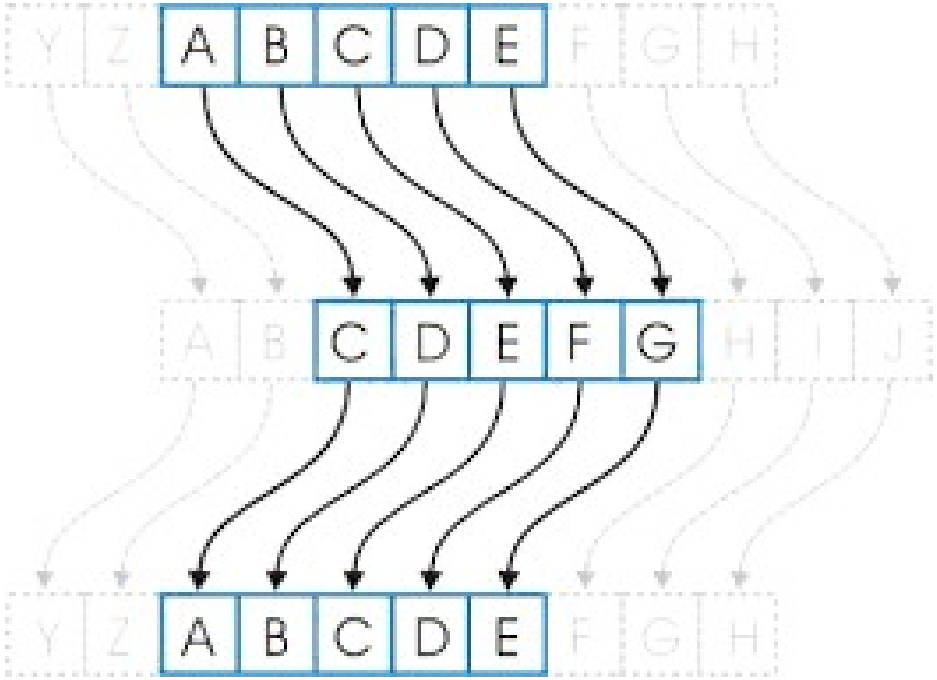
Зашифровать или зашифровать информацию

это скрыть сообщение паролем.С компьютерной точки зрения он состоит в применении алгоритма, связанного с одним или несколькими паролями, который преобразует информацию в строку бессмысленных букв, цифр и символов.

Следующая лабораторная работа была выполнена для того, чтобы показать, как работает кодирование caesar и кодирование atbash. Далее мы покажем код на языке python и его работу.

шифр Цезаря.

Шифр Цезаря — один из старейших известных методов шифрования. Очень просто - меняются только позиции алфавита. Преобразование называется ROTN, где N — значение изменения положения, а ROT означает «ПОВОРОТ».

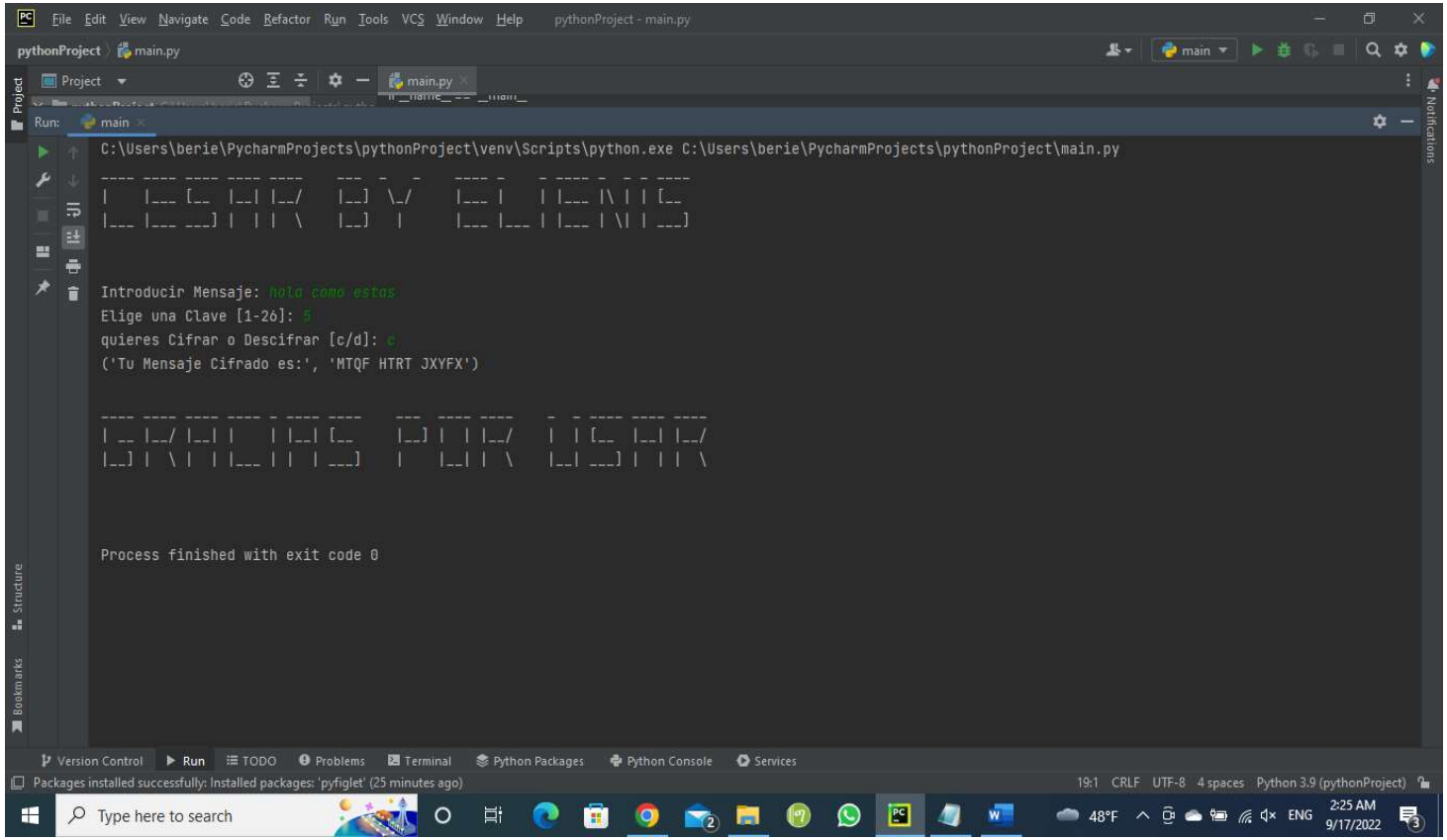


шифр Цезаря.

```
from __future__ import print_function
from pyfiglet import figlet_format


print( figlet_format("Cesar by Elienis", font = "cybermedium" ) )


def main():
    message = input("Introducir Mensaje: ")
    key = int(input("Elige una Clave [1-26]: "))
    mode = input("quieres Cifrar o Descifrar [c/d]: ")

    if mode.lower().startswith('c'):
        mode = "cifrar"
    elif mode.lower().startswith('d'):
        mode = "descifrar"

    translated = encdec(message, key, mode)
    if mode == "cifrar":
        print(("Tu Mensaje Cifrado es:", translated))
    elif mode == "descifrar":
        print(("Tu Mensaje Descifrado es:", translated))


def encdec(message, key, mode):
    message = message.upper()
    translated = ""
    LETTERS = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    for symbol in message:
        if symbol in LETTERS:
            num = LETTERS.find(symbol)
            if mode == "cifrar":
                num = num + key
            elif mode == "descifrar":
                num = num - key
```

```
            if num >= len(LETTERS):
                num -= len(LETTERS)
            elif num < 0:
                num += len(LETTERS)

            translated += LETTERS[num]
        else:
            translated += symbol
    return translated


if __name__ == '__main__':
    import doctest

    doctest.testmod()
    main()
    input()

    print(figlet_format("gracias por usar",
font="cybermedium"))
```

шифр Цезаря. выполнение кода и работа

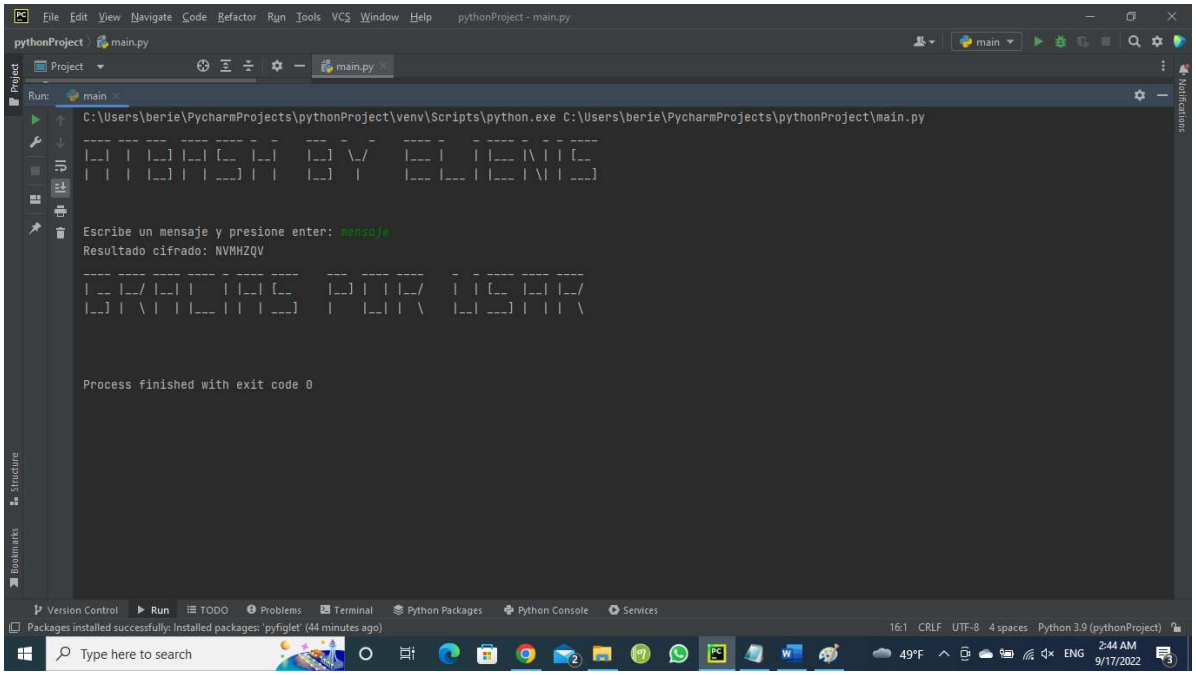


шифрование Атбаша

Шифр Атбаша (также называемый зеркальным шифром, обратным алфавитом или обратным алфавитом) — это название, данное моноалфавитному шифру замены, который обязан своим названием и происхождением еврейскому алфавиту.

шифрование Атбаша выполнение кода и работа

```
from pyfiglet import figlet_format


print( figlet_format("Atbash by Elienis", font =
"cybermedium" ) )



def atbash(message):
    ABC = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
    ZYX = 'ZYXWVUTSRQPONMLKJIHGFEDCBA'
    result = ''

    for letter in message:
        result += ZYX[ABC.index(letter)]

    return result

if __name__ == "__main__":
    message = input('Escribe un mensaje y presione
enter: ')
    print(f'Resultado cifrado: {
atbash(message.upper()) }')
    print(figlet_format("gracias por usar ",
font="cybermedium"))
```



- **выводы.**

- **С развитием информационных технологий во второй половине прошлого века и с использованием Увеличение использования компьютерных сетей и массового хранения информации.**

- **совершил большой скачок в изучении криптографических систем. В 1975 году Диффи и Хеллман заложили теоретические основы алгоритмов с открытым ключом. До этого не было изобретено никакой системы шифрования, кроме секретного ключа. В настоящее время используются несколько криптографических методов, DES (секретный ключ), метод RSA, Метод Меркла и Хеллмана и др.**

- **Современные системы шифрования, доступные на рынке (все, большинство или лучшие), построены из компонентов, конструкция и работа которых хорошо известны. Единственный секрет в них — это ключ шифрования**

- **Библиографическая информация**

- **Cuzco Naranjo, R., Mantilla Cabrera, C., Vaca Barahona, B., & Acosta Velarde, R. (2018). Mejora en la seguridad de un método esteganográfico aplicando criptografía. *Ciencia Digital*, *2*(3), 61-74. https://doi.org/10.33262/cienciadigital.v2i3.137**

- **David Arboledas Brihuega , (2017). Criptografía sin secretos con Python *Digital*, https://books.google.com.sv/books?hl=es&lr=&id=eo6fDwAAQBAJ&oi=fnd&pg=PA77&dq=CRIPTOGRAFIA+ATBASH&ots=0Jns3M5GV3&sig=Mn-fl-1eUVB42Qg76oLn-21BYeo#v=onepage&q=CRIPTOGRAFIA%20ATBASH&f=false**

- **Dos Santos B, (2014). CriptoMat1: ensinando Matemática utilizando conceitos de Criptografia - cifra de César e César estendida *Digital*, 34 http://ojs.sector3.com.br/index.php/wcbie/article/view/3175**

- **Scott B. Noegel Chair, (1996), 82-89.Dept. of Near Eastern Languages and Civilization University of Washington "Atbash in Jeremiah and Its Literary Significance: Part 1." First Published in: Jewish Bible Quarterly 24/2 *Digital*, https://faculty.washington.edu/snoegel/PDFs/articles/Noegel%2015%20-%20JBQ%201996a.pdf**

Спасибо вам большое за ваше внимание

Российский университет
дружбы народов