МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №6

“Тема №6”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

Завдання

Виконати шифрування тексту наступними методами

1. ШИФРУВАЛЬНІ ТАБЛИЦІ

«Світ ловив мене, та не спіймав» (Григорій Сковорода).

Наприклад, візьмемо повідомлення:

Світ\_ловив\_мене,\_та\_не\_спіймав

Потім запишемо його до таблиці нижче. Візьмемо таблицю, яка складається з 6 рядків і 5 стовпців.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| С | л | \_ | , | н | і |
| в | о | м | \_ | е | й |
| і | в | е | т | \_ | м |
| т | и | н | а | с | а |
| \_ | в | е | \_ | п | в |

Після заповнення таблиці текстом вхідного повідомлення стовпцями для формування зашифрованого тексту зчитуємо вміст таблиці рядками. Якщо зашифрований текст записувати групами по шість символів, то отримаємо такий шифротекст:

Сл\_,ні вом\_ей івет\_м тин аса \_ве\_пв

1. МАГІЧНИЙ КВАДРАТ

Заповнимо таблицю нашим повідомленням:

Скільки\_зла\_таїться\_всередині\_за\_гарною\_подобою:\_гадюка\_ховається\_в\_ траві.\_

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 0 | С | к | і | л | ь | к | и | \_ | з | л | а | \_ | т | а | ї | т | ь | с | я | \_ | в | с | е | р | е |
| 25 | д | и | н | і | \_ | з | а | \_ | г | а | р | н | о | ю | \_ | п | о | д | о | б | о | ю | : | \_ | г |
| 50 | а | д | ю | к | а | \_ | х | о | в | а | є | т | ь | с | я | \_ | в | \_ | т | р | а | в | і | . | \_ |

Розподіл символів вхідного повідомлення блоками по 25 символів.

Магічний Квадрат №1

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 11 | 24 | 7 | 20 | 3 | 65 | а | р | И | \_ | і |
|  | 4 | 12 | 25 | 8 | 16 | 65 | л | \_ | Е | \_ | т |
|  | 17 | 5 | 13 | 21 | 9 | 65 | ь | ь | Т | в | з |
|  | 10 | 18 | 1 | 14 | 22 | 65 | л | с | С | а | с |
|  | 23 | 6 | 19 | 2 | 15 | 65 | е | к | Я | к | ї |
| 65 | 65 | 65 | 65 | 65 | 65 | 65 |  |  |  |  |  |

Магічний Квадрат №2

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 11 | 24 | 7 | 20 | 3 | 65 | р | \_ | А | б | н |
|  | 4 | 12 | 25 | 8 | 16 | 65 | і | н | Г | \_ | п |
|  | 17 | 5 | 13 | 21 | 9 | 65 | о | \_ | О | о | г |
|  | 10 | 18 | 1 | 14 | 22 | 65 | а | д | Д | ю | ю |
|  | 23 | 6 | 19 | 2 | 15 | 65 | : | з | О | и | \_ |
| 65 | 65 | 65 | 65 | 65 | 65 | 65 |  |  |  |  |  |

Магічний Квадрат №3

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 11 | 24 | 7 | 20 | 3 | 65 | є | . | Х | р | ю |
|  | 4 | 12 | 25 | 8 | 16 | 65 | к | т | \_ | о | \_ |
|  | 17 | 5 | 13 | 21 | 9 | 65 | в | а | Ь | а | в |
|  | 10 | 18 | 1 | 14 | 22 | 65 | а | \_ | А | с | в |
|  | 23 | 6 | 19 | 2 | 15 | 65 | і | \_ | Т | д | я |
| 65 | 65 | 65 | 65 | 65 | 65 | 65 |  |  |  |  |  |

Зашифрований текст, що отримуємо при зчитуванні вмісту магічних квадратів рядками, має цілком загадковий вигляд:

ари\_іл\_е\_тььтвзлссасекякїр\_абнінг\_по\_оогаддюю:зои\_є.хрюкт\_о\_ваьава\_сві\_тдя

1. ШИФР ЦЕЗАРЯ З КЛЮЧОВИМ СЛОВОМ

Виберемо деяке число k, 0 ≤ k ≤ 36 і слово або коротку фразу як ключове слово.

Наприклад, k = 20 і ключове слово – барвінок.

В таблиці в першому рядку випишемо український алфавіт, в другому рядку напишемо ключове слово, яке зсуваємо на 20 елементів вперед.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | є | ж | з | и | і | ї | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ю | я | ь | \_ | . | , | ‘ |
| л | м | п | с | т | у | ф | х | ц | ч | ш | щ | ю | я | ь | \_ | . | , | ‘ | б | а | р | в | і | н | о | к | г | д | е | є | ж | з | и | ї | й |

Спробуємо зашифрувати вхідний текст "У\_кожному\_слові\_є\_сенс.". Результати його шифрування матимуть такий вигляд:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| У | \_ | к | о | ж | н | о | м | у | \_ | с | л | о | в | і | \_ | є | \_ | с | е | н | с | . |
| в | з | я | , | х | . | , | \_ | в | з | а | ь | , | п | ш | з | ф | з | а | у | . | а | и |

тобто, отримаємо на виході такий зашифрований текст:

взя,х. ,\_взаь,пшзфзау.аи

1. ТАБЛИЦЯ ТРИСЕМУСА

Виберемо як ключове слово, наприклад, кібербезпека, яке матиме такий вигляд після відкидання однакових букв:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| к | і | б | е | р | б | е | з | п | Е | к | а |
| к | і | б | е | р |  |  | з | п |  |  | а |

тобто, отримаємо ключ кіберзпа.

Розглянемо приклад використання шифрувальних таблиць Трисемуса стосовно українського алфавіту. Тут, при m = 36 та ключового слово кіберзпа отримуємо таку таблицю підставлянь:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е |  | к | і | Б | е | р | з |
| є | ж | з | и | і | ї |  | п | а | В | г | д | є |
| й | к | л | м | н | о | => | ж | и | Ї | й | л | м |
| п | р | с | т | у | ф |  | н | о | С | т | у | ф |
| х | ц | ч | ш | щ | ю |  | х | ц | Ч | ш | щ | ю |
| я | ь | \_ | . | , | ‘ |  | я | ь | \_ | . | , | ‘ |

Як і у випадку полібіанського квадрата, при шифруванні вхідного повідомлення

знаходимо в цій таблиці чергову букву початкового тексту і записуємо в зашифрований текст букву, розташовану нижче за неї в тому ж самому стовпці. Якщо буква тексту опиниться в нижньому рядку таблиці, тоді для зашифрованого тексту беремо верхню букву з того ж самого стовпця. Спробуємо зашифрувати вхідний текст «Мир\_необхідно\_здобувати.». Результати його шифрування матимуть такий вигляд:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| М | и | р | \_ | н | е | о | б | х | і | д | н | о | \_ | з | д | о | б | у | в | а | т | и | . |
| ф | о | д | б | х | г | ц | в | я | а | л | х | ц | б | є | л | ц | в | щ | ї | и | ш | о | е |

тобто, отримаємо на виході такий зашифрований текст:

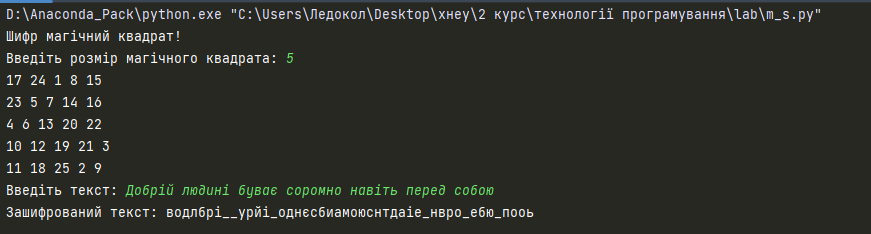
фодбхгцвяалхцбєлцвщїишое

РЕАЛІЗАЦІЯ ШИФРІВ

МАГІЧНИЙ КВАДРАТ

* Реалізація програми:
* # Шифр магічний квадрат!  
  print("Шифр магічний квадрат!")  
    
    
  # створюємо функцію генерації магічного квадрата  
  *def* magic\_square(*n*):  
   length = *n* \* *n* mx = [[*None for* z *in* range(*n*)] *for* z *in* range(*n*)]  
   y = 0  
   x = *n* // 2  
   mx[y][x] = 1  
   *for* i *in* range(2, length + 1):  
   old\_x, old\_y = x, y  
   x = (x + 1) % *n* y = (y - 1) % *n  
   if not* mx[y][x] *is None*:  
   x = old\_x  
   y = (old\_y + 1) % *n* mx[y][x] = i  
   a = []  
   *for* y *in* mx:  
   a += y  
   print(' '.join(map(str, y)))  
   *return* a  
    
  n1 = int(input("Введіть розмір магічного квадрата: "))  
  # Вносимо значення магічного квадрату у нову змінну  
  m = magic\_square(n1)  
    
    
  # Створюємо функцію кодування  
  *def* enc(*message*):  
   # Записуємо розмір таблиці у нову змінну  
   size = n1 \*\* 2  
    
   # Визначаємо кількість рядків, на які буде ділитись наш текст  
   *if* len(*message*) % size != 0:  
   a = len(*message*) // size + 1  
   *else*:  
   a = len(*message*) // size  
    
   # У тексті міняємо пробіли на підкреслення  
   message = *message*.replace(' ', '\_')  
    
   # Шифруємо наш текст за допомогою сгенерованих значень магічного квадрата  
   f1 = ''  
   *for* i *in* range(0, a):  
   *for* j *in* range(size):  
   el = m[j] + i \* size - 1  
   # Так як текст не завжди може заповняти конжу клітинку таблиці, то потрібно виключити з циклу  
   # можливість брати ті номера знаків, які більше довжини самого тексту  
   *try*:  
   f1 += str(*message*[el])  
   *except* IndexError:  
   *continue  
   return* f1  
    
    
  message1 = input('Введіть текст: ').lower()  
  print("Зашифрований текст: " + enc(message1))

Вивід програми:

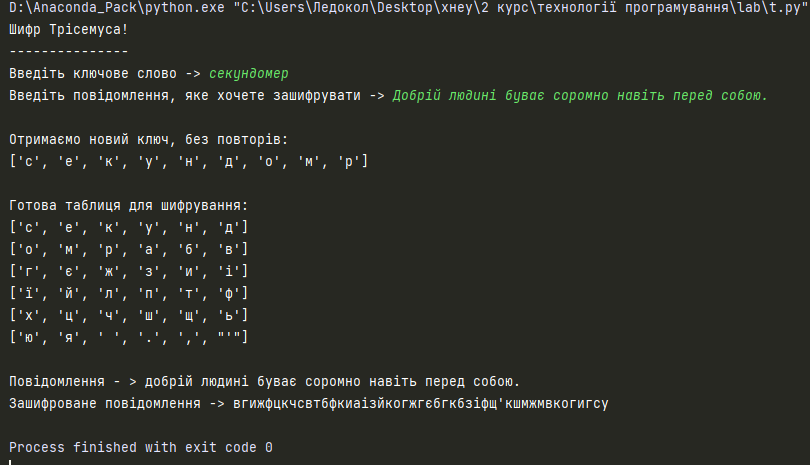


ТАБЛИЦЯ ТРИСЕМУСА

Реалізація програми:

# Шифр Трісемуса до українського алфавіту  
  
print(f'Шифр Трісемуса!\n{"-"\*15}')  
alphabet\_UK = "абвгдеєжзиіїйклмнопрстуфхцчшщьюя .,'"  
key\_word = input("Введіть ключове слово -> ").lower()  
message = input("Введіть повідомлення, яке хочете зашифрувати -> ").lower()  
  
# Формуємо список і відкидаємо літери, які повторюються  
new\_key = []  
*for* i *in* key\_word:  
 *if* i *not in* new\_key:  
 new\_key.append(i)  
print(f'\nОтримаємо новий ключ, без повторів:\n{new\_key}')  
  
# Формуємо новий алфавіт, видаливши літери з нового ключового слова  
*for* i *in* new\_key:  
 *if* i *in* alphabet\_UK:  
 alphabet\_UK = alphabet\_UK.replace(i, '')  
  
# Формуємо таблицю представлень  
my\_list = []  
my\_list.extend(new\_key)  
my\_list.extend(alphabet\_UK)  
  
# Формуємо таблицю, тобто матрицю 6х6  
count = 0  
table = [[0] \* 6 *for* i *in* range(6)]  
*for* i *in* range(6):  
 *for* j *in* range(6):  
 table[i][j] = my\_list[count]  
 count += 1  
  
# Виводимо таблицю в зручному форматі  
print("\nГотова таблиця для шифрування:")  
*for* i *in* table:  
 print(i)  
  
# Зашифровуємо текст  
mylist = list(message)  
cipher\_text = []  
*for* e *in* mylist:  
 *for* i *in* range(len(table)):  
 *for* j *in* range(len(table[0])):  
 *if* table[i][j] *in* e:  
 *if* i == len(table) - 1:  
 cipher\_text.append(table[0][j])  
 *else*:  
 cipher\_text.append(table[i + 1][j])  
print("\nПовідомлення - >", message)  
print("Зашифроване повідомлення ->", "".join(cipher\_text))

Вивід програми:



ВИСНОВОК

В цій лабораторній роботі, я шифрував тексти різними методами. Та реалізувала всі ці шифри у програмі.