**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 1**

**за дисципліною: *“*** **Теоретичні основи криптографії** ”

**на тему: “Програмна реалізація шифру Вернама”**

**Виконав: студент факультету Інформаційних технологій**

**2 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

**ХНЕУ ім. С. Кузнеця**

**2023**

Мета: Реалізувати шифр Вернама

Завдання: Розробити програмну реалізацію шифру Вернама

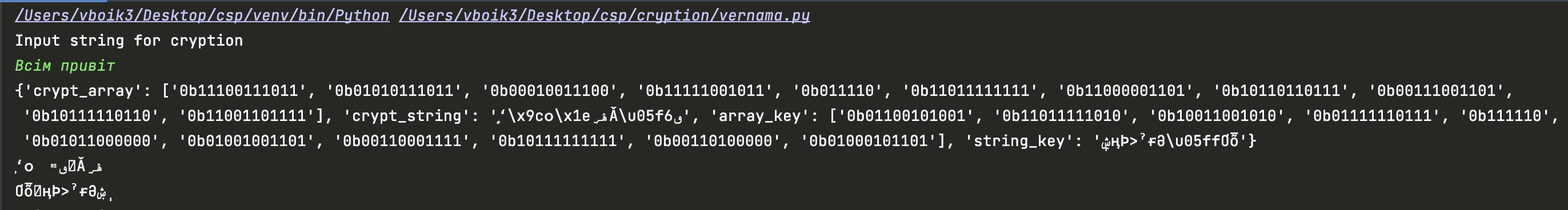
Я реалізував таке ришення

*from* random *import* randint  
  
*def* generate\_key(*binary\_array* = []):  
 array\_key = []  
 *for* b *in binary\_array*:  
 binary\_key = '0b'  
 *for* \_ *in* range(2, len(b)):  
 binary\_key += str(randint(0, 1))  
 array\_key.append(binary\_key)  
 *return* array\_key  
  
*def* generate\_key\_string(*binary\_array\_key* = []):  
 string\_key = ''  
 *for* b *in binary\_array\_key*:  
 string\_key += chr(int(b, 2))  
 *return* string\_key  
  
*def* xor(*a* = [], *b* = []):  
 result = []  
 *for* i *in* range(len(*a*)):  
 res = '0b'  
 *while* len(*a*[i]) != len(*b*[i]):  
 *if* len(*a*[i]) > len(*b*[i]):  
 *b*[i] = '0b0' + *b*[i][2::]  
 *else*:  
 *a*[i] = '0b0' + *a*[i][2::]  
 *for* j *in* range(2, len(*a*[i])):  
 res += str(int(*a*[i][j], 2) ^ int(*b*[i][j], 2))  
 result.append(res)  
 *return* result  
  
*def* cryption(*string* = ''):  
 binary\_array = [bin(ord(x)) *for* x *in string*]  
 array\_key = generate\_key(binary\_array)  
 string\_key = generate\_key\_string(array\_key)  
 crypt\_array = xor(binary\_array, array\_key)  
 crypt\_string = ''  
 *for* k *in* crypt\_array:  
 crypt\_string += chr(int(k, 2))  
 *return* {  
 'crypt\_array': crypt\_array,  
 'crypt\_string': crypt\_string,  
 'array\_key': array\_key,  
 'string\_key': string\_key,  
 }  
  
*def* encryption(*string* = '', *key* = ''):  
 encrypt\_string = ''  
 binary\_array\_encrypt\_string = [bin(ord(x)) *for* x *in string*]  
 binary\_array\_key = [bin(ord(x)) *for* x *in key*]  
 en\_a = xor(binary\_array\_key, binary\_array\_encrypt\_string)  
 *for* k *in* en\_a:  
 encrypt\_string += chr(int(k, 2))  
 *return* encrypt\_string  
  
operations = {  
 'cryption': cryption,  
 'encryption': encryption,  
}  
  
string = input('Input string for cryption\n')  
crypto = cryption(string)  
print(crypto)  
print(encryption(crypto['crypt\_string'], crypto['string\_key']))

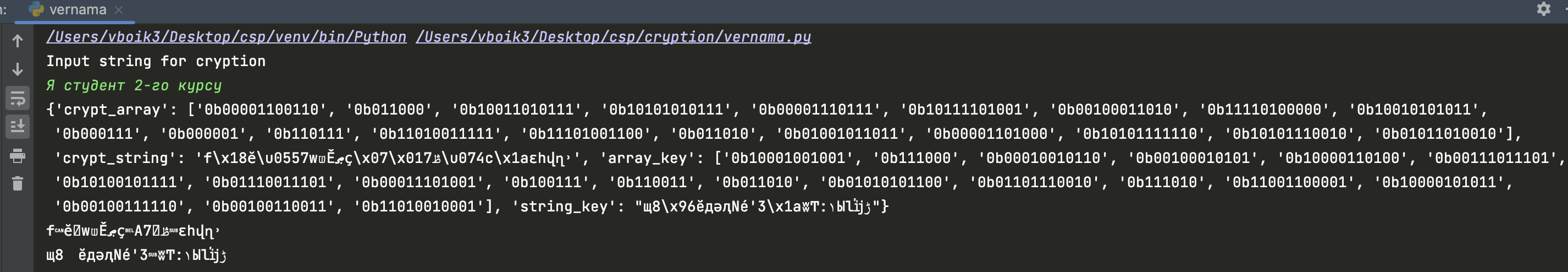
Тести

Ширування

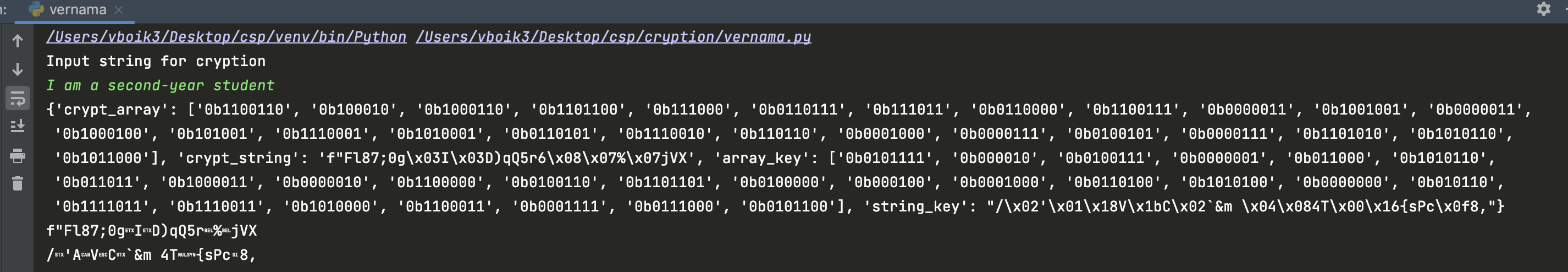
|  |  |  |  |
| --- | --- | --- | --- |
| Вхідна строка | Отриманий ключ | Отримана шифрована строка | Рисунок |
| Всім привіт | ̩ۺӊϷ>ˀɍƏ׿Ơȭ | ܻʻߋ‑ۿ؍ַǍ׶ٯ | 1.1 |
| Я студент 2-го курсу | щ8ĕдǝԯΝé'3ʬͲ:١Ыľĳڑ | fӗ՗wשĚޠҫ7ڟ݌ɛhվղ˒ | 1.2 |
| I am a second-year student | /'VC`&m 4T | f"Fl87;0gID)qQ5r%jVX | 1.3 |
| Hi everyone | y j!@OTw | 1I0W%`e : | 1.4 |



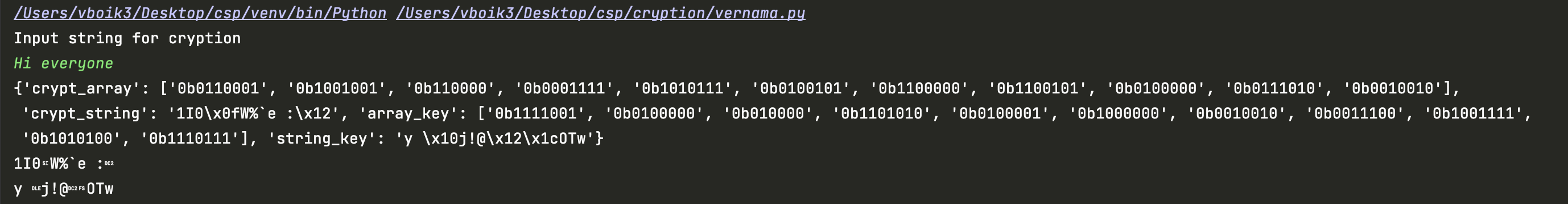
(рис 1.1)



(рис 1.2)



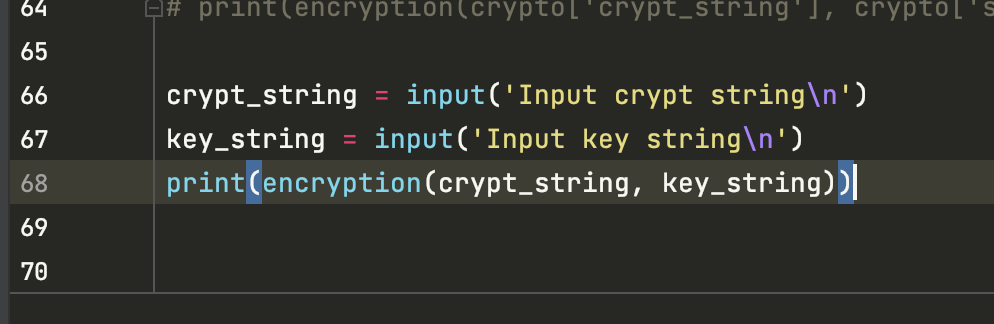
(рис 1.3)



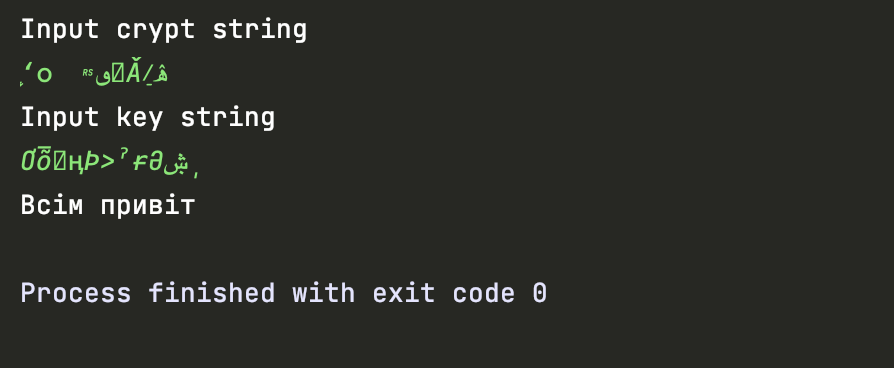
(рис 1.4)

Дешифрування

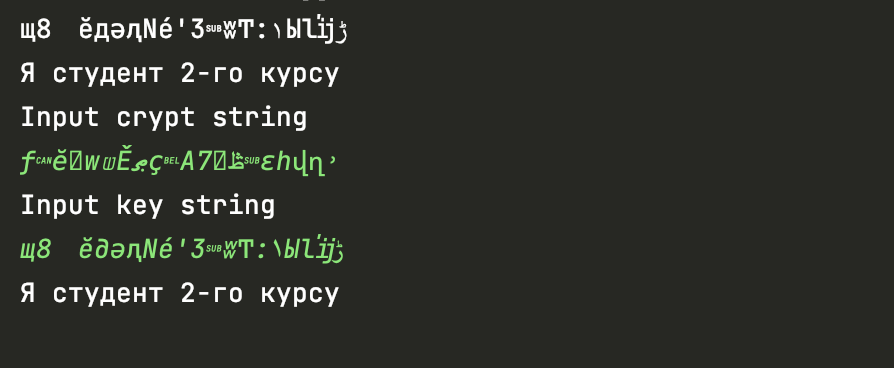
Додав дані строки



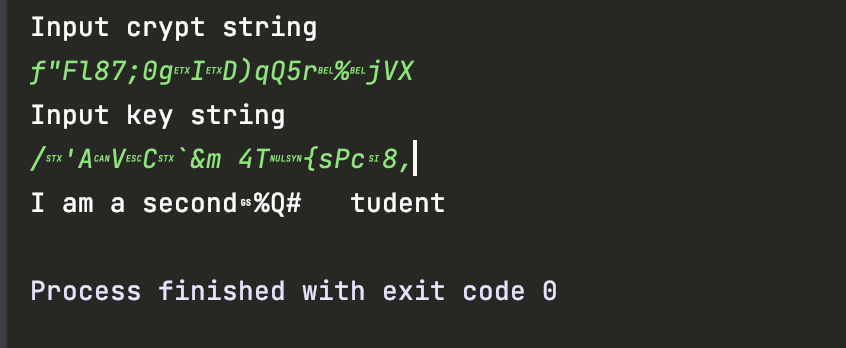
|  |  |  |  |
| --- | --- | --- | --- |
| Ключ | Шифрована строка | Вихідні данні | Рисунок |
| ۺӊϷ>ˀɍƏ׿Ơȭ | ܻʻߋ‑ۿ؍ַǍ׶ٯ | Всім привіт | 2.1 |
| щ8ĕдǝԯΝé'3ʬͲ:١Ыľĳڑ | fӗ՗wשĚޠҫ7ڟ݌ɛhվղ˒ | Я студент 2-го курсу | 2.2 |
| /'VC`&m 4T | f"Fl87;0gID)qQ5r%jVX | I am a second%Q# tudent | 2.3 |
| y j!@OTw | 1I0W%`e : | Hi everyone | 2.4 |



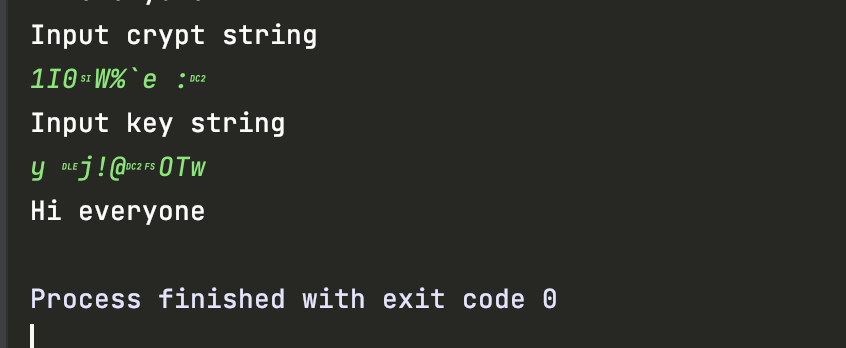
(рис 2.1)



(рис 2.2)



(рис 2.3)



(рис 2.4)

Висновок я реалізував шифр Вернама