**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 7**

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

**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**

Завдання:

Реалізувати програму, яка дозволяє виконувати такі дії:

Генерувати великі прості числа для алгоритму Діффі-Хеллмана

Моделювати обмін ключами між абонентами за схемою Діффі-Хеллмана

Я написав наступний код

*class* DH\_Endpoint(object):  
 *def \_\_init\_\_*(self, *public\_key1*, *public\_key2*, *private\_key*):  
 self.public\_key1 = *public\_key1* self.public\_key2 = *public\_key2* self.private\_key = *private\_key* self.full\_key = *None  
 def* generate\_partial\_key(self):  
 partial\_key = self.public\_key1\*\*self.private\_key  
 partial\_key = partial\_key%self.public\_key2  
 *return* partial\_key  
 *def* generate\_full\_key(self, *partial\_key\_r*):  
 full\_key = *partial\_key\_r*\*\*self.private\_key  
 full\_key = full\_key%self.public\_key2  
 self.full\_key = full\_key  
 *return* full\_key  
 *def* encrypt\_message(self, *message*):  
 encrypted\_message = ""  
 key = self.full\_key  
 *for* c *in message*:  
 encrypted\_message += chr(ord(c)+key)  
 *return* encrypted\_message  
 *def* decrypt\_message(self, *encrypted\_message*):  
 decrypted\_message = ""  
 key = self.full\_key  
 *for* c *in encrypted\_message*:  
 decrypted\_message += chr(ord(c)-key)  
 *return* decrypted\_message  
  
message="This is a very secret message!!!"  
s\_public=197  
s\_private=199  
m\_public=151  
m\_private=157  
Sadat = DH\_Endpoint(s\_public, m\_public, s\_private)  
Michael = DH\_Endpoint(s\_public, m\_public, m\_private)  
  
s\_partial=Sadat.generate\_partial\_key()  
print(s\_partial) #147  
  
m\_partial=Michael.generate\_partial\_key()  
print(m\_partial)  
  
s\_full=Sadat.generate\_full\_key(m\_partial)  
print(s\_full) #75  
  
m\_full=Michael.generate\_full\_key(s\_partial)  
print(m\_full) #75  
  
m\_encrypted=Michael.encrypt\_message(message)  
print(m\_encrypted) #'\x9f³´¾k´¾k¬kÁ°½Äk¾°®½°¿k¸°¾¾¬²°lll'  
  
message = Sadat.decrypt\_message(m\_encrypted)  
print(message) #'This is a very secret message!!!'

Та запускаю для тесту

