

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Криптографія»

Лабораторна робота №4.

**«Вивчення криптосистеми RSA та алгоритму електронного
підпису; ознайомлення з методами генерації параметрів для
асиметричних криптосистем»**

Виконали:

Варіант - 5

студенти гр. ФБ-92

Кудряшов М.О. та Курганський Л. С.

Мета роботи: Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Загальний код програми знаходиться в файлі "main.py"

Хід роботи:

1. При запуску програма створює двох абонентів "А" і "В", між якими передаються повідомлення;
2. При створенні абонентів, генеруються псевдопрості числа, які будуть використані для шифрування;
3. Абонент "А" генерує повідомлення для "В" для цього йому потрібно:
 - 3.1. Згенерувати відкритий ключ, котрий менший чим у "В" $n < n_1$;
 - 3.2. Закодувати і зашифрувати повідомлення;
 - 3.3. Згенерувати підпис.
4. Абонент "В" отримує пакет даних з повідомленням і підписом, та відкритий ключ "А";
5. Розшифрування повідомлення абонентом "В":
 - 5.1. Розшифровує повідомлення своїм секретним(d) і відкритим ключем (n);
 - 5.2. Розшифровує підпис своїм секретним(d) і відкритим ключем (n);
 - 5.3. Перевірка підпису з повідомленням;
 - 5.4. Вивід повідомлення або помилки;
6. Дії повторюються поки листування не закінчиться.

Приклад роботи:

```
A = Person()
B = Person()

text = "lol kek cheburek."

packet = A.create_message(text, B.open_key)
print(f"msg={packet[0]}\nsign={packet[1]}\n")
B.read_message(packet, A.open_key)

text = "Ok, Da."

packet = B.create_message(text, A.open_key)
print(f"msg={packet[0]}\nsign={packet[1]}\n")
A.read_message(packet, B.open_key)
```

Результат:

```
PS C:\Users\lkung\Desktop\03TEX 3.1\crypta\lab_4> & C:/Users/lkung/AppData/Local/Programs/Python/Python39/python.exe "C:\Users\lkung\Desktop\03TEX 3.1\crypta\lab_4\main.py"
msg=4870690465432927738642461802068979465980722408763435979713096946447014971122096307391057886163506718079509494778637648723509777770599754457664983142825264
sign=3913622885093954443100121114600035532652360419425693454420069290945969206600640295399820049641885839700820779770181842176198359670157680228026993846839659

message: "lol kek cheburek."
msg=526564882729483027879876318720597767222639796629126030072162169388167308007423973246357651253338271610044887598979080405629895546037217077893061487198857
sign=3616564875439871666626835116743042916809497825750101185182383758373490464269275784942979502453490617785582816607448078028616068313376676954595559714579551

message: "Ok, Da."
PS C:\Users\lkung\Desktop\03TEX 3.1\crypta\lab_4> █
```