КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

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

Варіант 12

Виконали:   
ФБ-05 Левицький Євген   
ФБ-05 Дегтярьов Микола

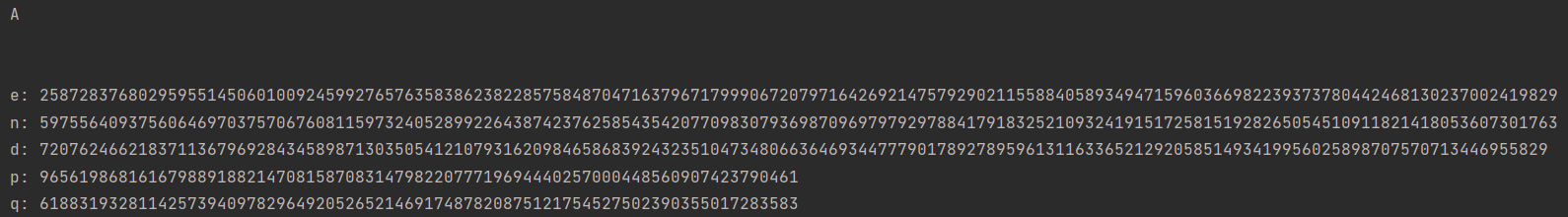
Київ – 2022

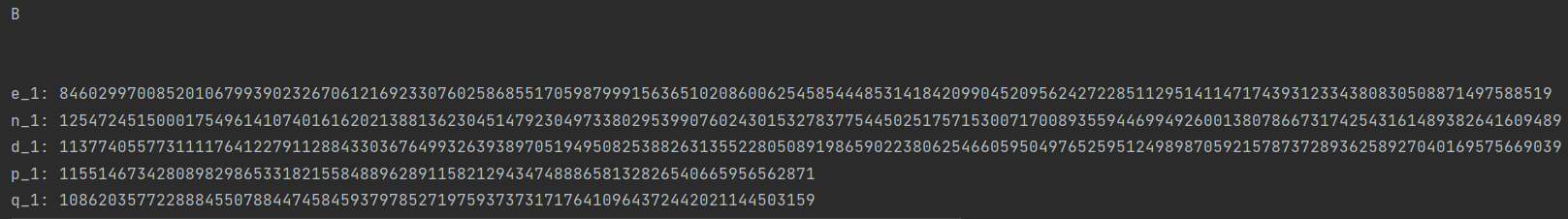
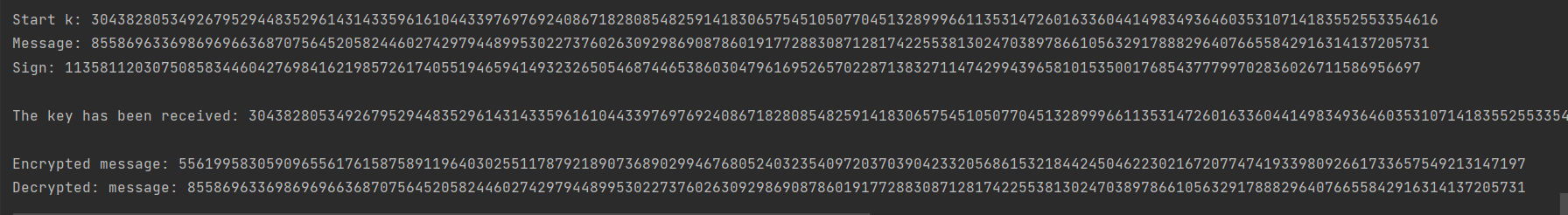
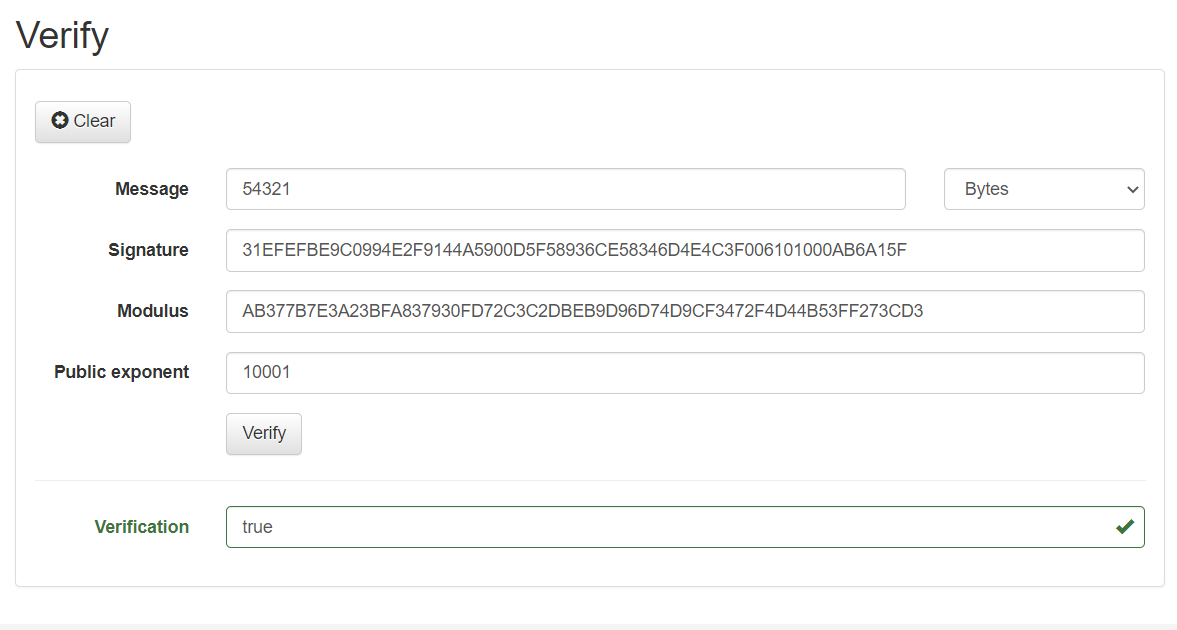
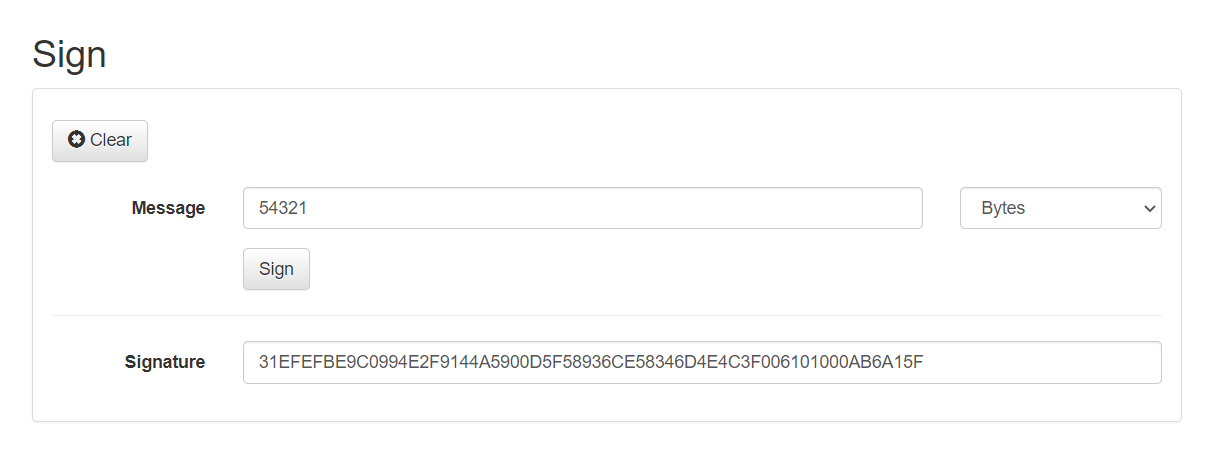
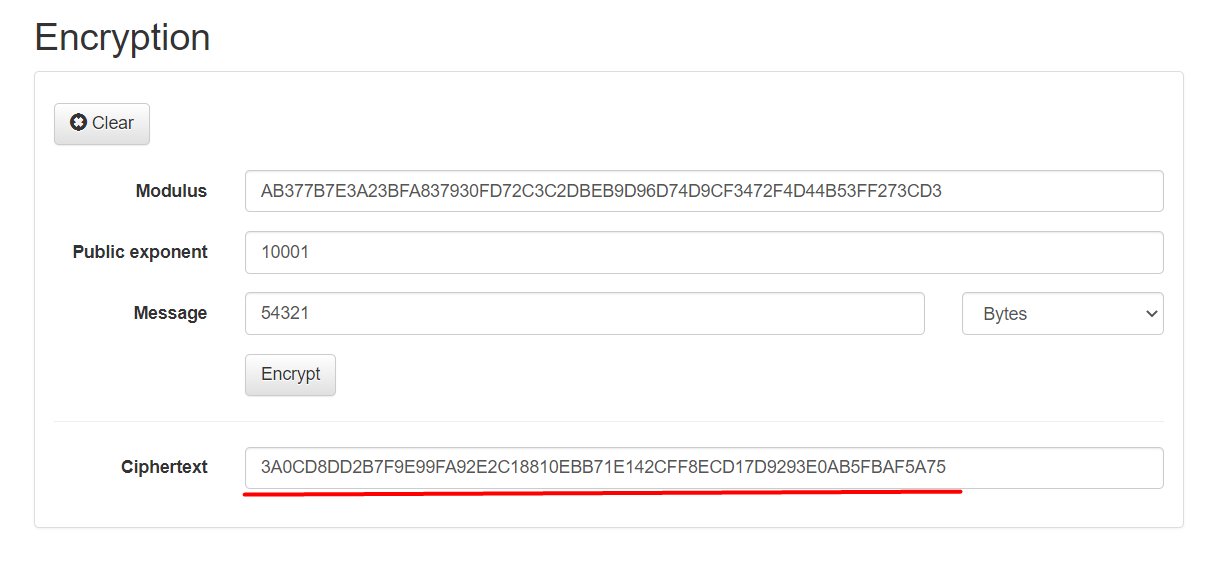
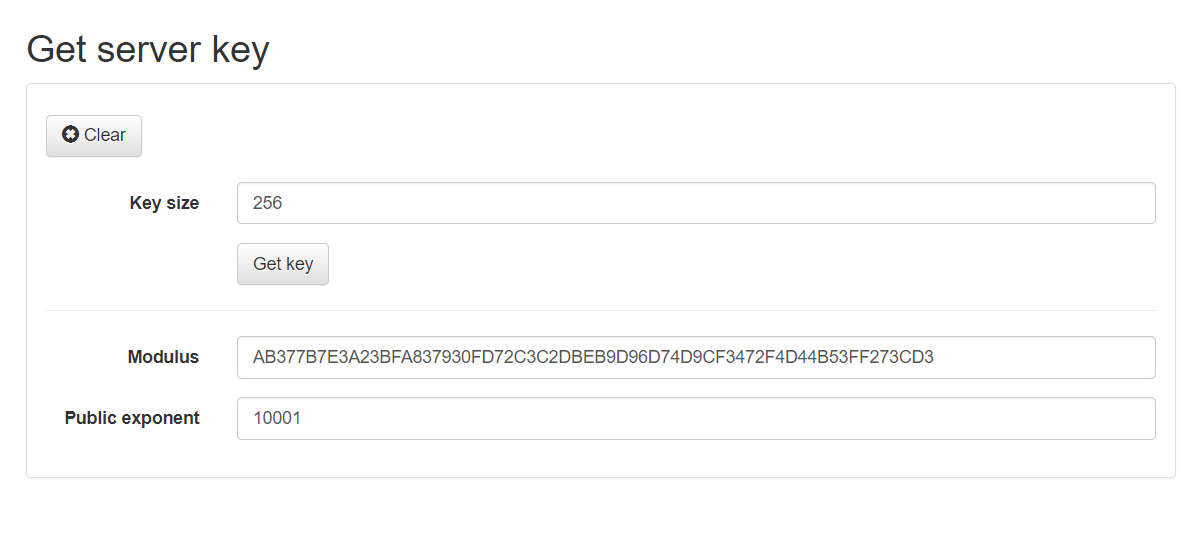
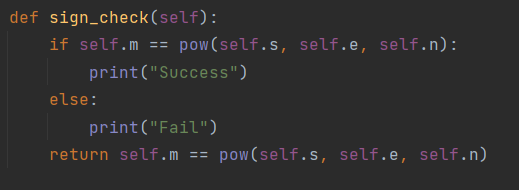
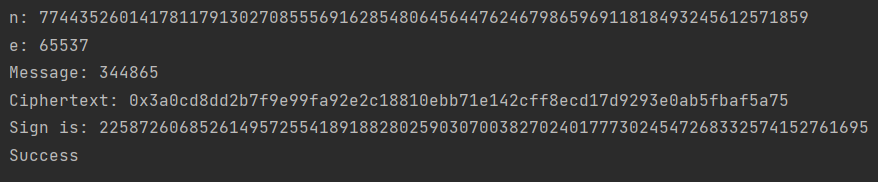
**Мета та основні завдання роботи:** Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й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

**Хід роботи:**

В рамках виконання практикуму було створено функції:  
test\_number – перевірка числа на простоту на основі тесту Міллера  
find\_number – генерує число, перевіряє його тестом Міллера  
generate\_keys – генерує p, q, p1, q1  
extended\_evclid – розширений алгоритм Євкліда  
inverse\_mod – функція пошуку оберненого  
rsa\_pair – генерує d,n,e   
enc\_msg – шифрує повідомлення  
Decryption – розшифровує повідомлення  
sign – функція підпису повідомлення

sign\_check – перевірка надісланого підпису  
send\_key – надсилання шифрованого повідомлення  
receive\_key – отримує повідомлення і перевіряє підпис  
  
Вивід виконання програми:   
Для користувача А

  
  
Для користувача B

  
  
Вивід к, повідомлення, підпису, зашифрованого і розшифрованого повідомлення  
  
  
  
  
  
  
  
  
  
  
  
Починаємо перевірку за сайтом  
  
Перевірка кодом значень шифротексту і підпису з сайту  
Зробивши маленьку модифікацію  
  
Пишемо код з переведенням і функціями  
  
Можемо порівняти результат, шифротекст сходиться, підпис підтвердився  


Висновки

В результаті виконання практикуму ми практично ознайомились з системою захисту інформації на основі криптосхеми RSA. Було засвоєно і практично використано тест Міллера-Рабіна для перевірки чисел на простоту і генерації простих чисел. Мали змогу використати Asym Crypto Lab Environment і з його допомогою перевірити нами створені функції криптосхеми RSA.