



Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

«Криптографія»

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Виконали:

Студенти групи ФБ-92,94

Прохорська Олександра

Рябко Дмитро

Київ 2021

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) Спочатку написали функцію перевірки простоти числа тест МіллераРабіна
- 2) Згенерували дві пари простих чисел
- 3) Написали функцію генерації відкритого та закритого ключів для двох абонентів для RSA
- 4) Написали функції: шифрування та розшифрування і створення цифрового підпису
- 5) Організували обмін повідомленнями між абонентами А і В

Генеруємо випадковий ключ на сайті

The screenshot shows a web form titled "Get server key". At the top left is a "Clear" button with a trash icon. Below it, the "Key size" is set to "256" in a text input field, with a "Get key" button underneath. A horizontal line separates this from the next section. Below the line, the "Modulus" is displayed as "917FDA63F4EE1B3E219A02E8EBB093F227B319D3FA4DE5D38f" in a text input field. Below that, the "Public exponent" is set to "10001" in a text input field.

Check function

Message: 130

mod = 1161373746568415653074263912687440563077

exp = 65537

Encrypted: 1117590204217780742852568581874083047049

Signature: 868697827761734443096979458663945797103

SignVer: True

Process finished with exit code 0



Перевод из одной системы счисления в другую

Исходное основание

10

Основание системы счисления исходного числа

Исходное число

130

Число которое необходимо преобразовать

Основание результата

16

Основание системы счисления переведенного числа

Переведенное число

82



Перевод из одной системы счисления в другую

Исходное основание

10

Основание системы счисления исходного числа

Исходное число

111759020421778074285256858187408:

Число которое необходимо преобразовать

РАССЧИТАТЬ

Основание результата

16

Основание системы счисления переведенного числа

Переведенное число

348C80B42A55F2B1293E943C
E47022689



СОХРАНИТЬ



ВИДЖЕТ

Перевіряємо за допомогою сайту:

Server
Key

Encryption

Decryption

Signature

Verification

Send
Key

Receive
Key

Encryption

✖ Clear

Modulus

369B87290493AC8520954BAF362A50B85

Public exponent

10001

Message

82

Bytes



Encrypt

Ciphertext

0348C80B42A55F2B1293E943CE47022689

Verify

 Clear

Message

82

Bytes



Signature

028D891DAC58AC06D4322D7FD6330AFDEF

Modulus

369B87290493AC8520954BAF362A50B85

Public exponent

10001

Verify

Verification

true

