



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

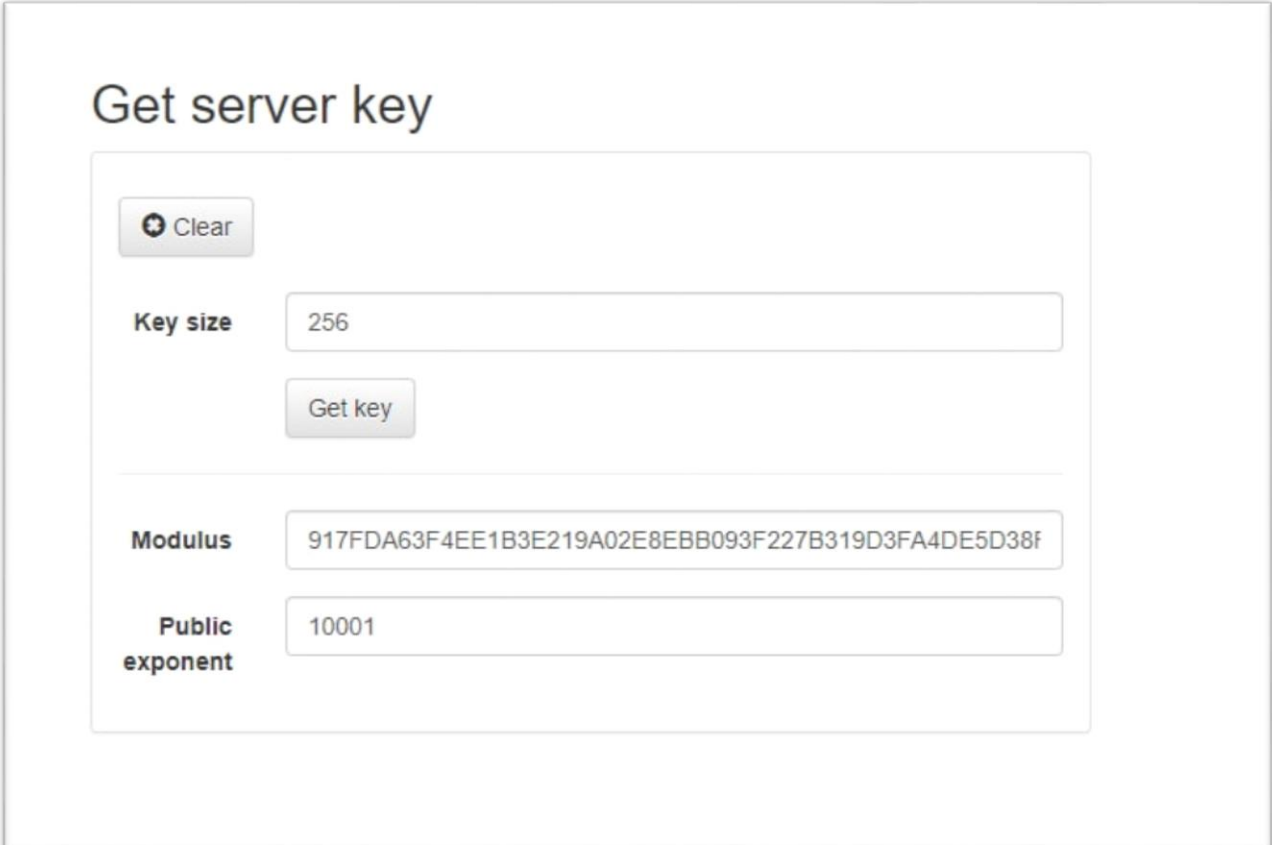
Мета роботи: Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення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

Загальний код програми знаходиться в файлі "*main.py*"

Хід роботи:

- 1) Спочатку написали функцію перевірки простоти числа тест Міллера-Рабіна
- 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 is a "Key size" label next to a text input field containing the value "256". To the right of the input field is a "Get key" button. A horizontal line separates this section from the one below. The lower section has a "Modulus" label next to a text input field containing the hexadecimal value "917FDA63F4EE1B3E219A02E8EBB093F227B319D3FA4DE5D38f". Below that is a "Public exponent" label next to a text input field containing the value "10001".

Check function

|


Message: We did it

mod = 7BF2EEC4523C768E05EA8D0FB61BA1B14953FF6CCB207715DF082A37491534AC978A2A8D321884E97350401CB47864A780EF78F421920396622B030530CFFF49

exp = 261B8DD82C4A7E8E1FAE547B91F131C6C0C86A7A3AE657C06F7049AF026A61E28213FA61266C1994EE4A0CF24492CC131A52197C6361AD75768C7F421DC9A07D

Encrypted: 31760061BBA9E97A14C54A56E2138DBC53EBCD217E2E07829295A4A90E3C45082F41826A40A963DB612FDC1FE099BFCBF7DCA6D309AD27EB11AD4AFFDF466C08

Перевіряємо за допомогою сайту:

 Clear

Modulus

Public exponent

Message

Text

Encrypt

Ciphertext