

Комп'ютерний практикум №4

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

Виконали: студенти групи ФБ-01
Оліферчук Владислав
Корабельський Тарас

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.

Хід роботи:

- 1) Реалізували тест Міллера-Рабіна для перевірки простоти числа
- 2) Реалізували генерацію пар випадкових простих чисел
- 3) Реалізували функцію генерації відкритого і закритого ключів для 2 абонентів для RSA
- 4) Реалізували функції шифрування/дешифрування та створення цифрового підпису
- 5) Організували обмін повідомленнями між абонентами для перевірки роботи програми.

Результати роботи програми:

Get server key

✖ Clear

Key size

128

Get key

Modulus

BFF0CEC9F2700B0C3F92B2E1BCD94307

Public exponent

10001

Encryption




Modulus	<input type="text" value="BFF0CEC9F2700B0C3F92B2E1BCD94307"/>	
Public exponent	<input type="text" value="10001"/>	
Message	<input type="text" value="70"/>	Bytes <input type="button" value="v"/>
	<input type="button" value="Encrypt"/>	

Ciphertext	<input type="text" value="13541427AFE928966189F2C836B2770F"/>	
------------	---	--


Check function

```
Message: 112
mod = 255132892617237132207249163071828607751
exp = 65537
Encrypted: 25691893648562486299091478032218748687
Signature: 186307443963895519869963180022938153092
SignVer: True
```

Verify



Message	<input type="text" value="70"/>	Bytes <input type="button" value="v"/>
Signature	<input type="text" value="8C29822E50FBF97DDB83ADFB95CF3084"/>	
Modulus	<input type="text" value="BFF0CEC9F2700B0C3F92B2E1BCD94307"/>	
Public exponent	<input type="text" value="10001"/>	
	<input type="button" value="Verify"/>	

Verification	<input type="text" value="true"/>	
--------------	-----------------------------------	---

Код програми було надіслано окремим файлом (lab4.py)

Висновок: Під час виконання даної лабораторної роботи ми ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; також ознайомилися з системою захисту інформації на основі криптосхеми RSA, організували з використанням цієї системи засекречений зв'язок й електронний підпис, вивчили протокол розсилання ключів.