

## **Криптографія**

### **Лабораторна робота 4. Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем**

ФБ-13 Ігнатенко Данило

Варіант 5

#### **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

#### **Задача**

0. Прочитати методичку. Напевно, більше трьох разів
1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини. Перевірити простоту числа тестом Міллера-Рабіна
2. Написати функцію генерування ключових пар для RSA та згенерувати ключові пари для абонентів А та В
3. Написати функції шифрування, розшифрування, підпису, перевірки підпису повідомлення, надсилання та отримання секретного ключа по відкритій мережі
4. Перевірити роботу всього цього добра за допомогою [наданого ресурсу](#)

#### **Хід роботи**

Спершу були написані допоміжні функції – тест Міллера-Рабіна та генерація випадкового простого числа потрібної довжини

З їх використанням були написані 7 основних функцій лабораторної роботи

Останнім етапом стала перевірка коректності реалізації усіх функцій за наданим посиланням

#### **Труднощі**

Допоміжні функції зайняли трохи часу, але без бетонних стін – потихеньку все зробилося

Основні функції труднощів, загалом, не викликали

#### **Шляхи розв'язання**

Вони точно існують

## Результати

Далі наведені скріни використання реалізованих процедур. В якості абонента В виступає сервер

Генерація ключової пари

### Get server key

✖ Clear

Key size

256

Get key

Modulus

82D4DBA2BCAC56F2F386A67507D01AE4BE0841A02850718BBB86EBF3177101F5

Public exponent

10001

```
#####
Keypair generation
B Modulus: 82D4DBA2BCAC56F2F386A67507D01AE4BE0841A02850718BBB86EBF3177101F5
B Public exponent: 10001
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d
A secret exponent: 1ccbb960850908db4416b92d1575f6308d41e0d900fa00905cf25fcbd3b990a9
#####
```

Перевірка правильності шифрування та розшифрування

### Encryption

✖ Clear

Modulus

5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81

Public exponent

14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d

Message

177c8c81dbc31285b583a26e92f601b509c6f9603f2368fb5c4b49cc141672cb

Bytes ▼

Encrypt

Ciphertext

4491C40F16C19131CD15F3F6739888BF44C519E16078A66573D9C8945416FE6C

```
#####
Encryption
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d
Message: 177c8c81dbc31285b583a26e92f601b509c6f9603f2368fb5c4b49cc141672cb
B Encrypted message: 4491C40F16C19131CD15F3F6739888BF44C519E16078A66573D9C8945416FE6C
B Encrypted message and A Encrypted message match: True
Original Message and A Decrypted message match: True
#####
```

Ще одна подібна

## Decryption

Ciphertext

2f4e655099212bcf68d58bd5c027b45f92ee10fb45cf63259d627e73617e96fd

Bytes

▼

---

Message

3F5E58773F4108EEC3BF80B10C434D3FAB6589A4A85454702C0477B8C79920A6

```
#####
Decryption
Message: 3f5e58773f4108eec3bf80b10c434d3fab6589a4a85454702c0477b8c79920a6
A Encrypted message: 2f4e655099212bcf68d58bd5c027b45f92ee10fb45cf63259d627e73617e96fd
B Decrypted message: 3F5E58773F4108EEC3BF80B10C434D3FAB6589A4A85454702C0477B8C79920A6
Message and B Decrypted message match: True
#####
```

Перевірка підпису

## Sign

Message

6a8167cce1b688663f6420cbd890c76f743d809f56edf57536aaa137241ed4ee

Bytes

▼

---

Signature


4C570FDFF525B825E5A5C6D9126E4213BF2A83DB699E9A8CC3B852DC61F20F64


```
#####  
Sign verification  
Message: 6a8167cce1b688663f6420cbd890c76f743d809f56edf57536aaa137241ed4ee  
B Sign: 4C570FDFF525B825E5A5C6D9126E4213BF2A83DB699E9A8CC3B852DC61F20F64  
B signed message correctly: True  
#####
```

## Підписування повідомлення

```
#####  
Signing  
Message: 1776e14e6657472a3a29ac2034a8af6128354cbb7722bb647bcd8be667e6a3b  
A Sign: 3198d1aed306c7b01d30936739f695b8419a4daf683a212c3a211e4a26794467  
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81  
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d  
#####
```

## Verify

 Clear

Message	<input type="text" value="1776e14e6657472a3a29ac2034a8af6128354cbb7722bb647bcd8be667e6a3b"/>	<input type="text" value="Bytes"/>
Signature	<input type="text" value="3198d1aed306c7b01d30936739f695b8419a4daf683a212c3a211e4a26794467"/>	
Modulus	<input type="text" value="5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81"/>	
Public exponent	<input type="text" value="14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d"/>	
	<input type="button" value="Verify"/>	
Verification	<input type="text" value="true"/> 	

## Отримання ключа

# Send key

✖ Clear

Modulus

5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81

Public exponent

14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d

Send

Key

251DB8164A514CA788AEC31D6526C0F46734D04D152EABD459B5EA8FFCA6FE86

Signature

5A539CE5BEA3383B00E1CCF640F6BCDDF62352C7FDC01DF5996EC27509047862

```
#####
Key receiving and verification
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d
B Key: 251DB8164A514CA788AEC31D6526C0F46734D04D152EABD459B5EA8FFCA6FE86
B Sign: 5A539CE5BEA3383B00E1CCF640F6BCDDF62352C7FDC01DF5996EC27509047862
B Sent key: 5db51ff5f91b0fc5
#####
```

## Надсилання ключа

# Receive key

✖ Clear

Key

8127c917361f465e2abe23e03785f02f589aa659fa8e39b89d5ca462aa8d0cca

Signature

312026251f4bf302a1f3a3f427ef82a8cb70940fbb4eb056cfb01a2f6346d53

Modulus

5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81

Public exponent

14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d

Receive

Key

33AEE361F2D0AC3EA7C6D29768FCAFCEE5962B13B138A82E0302072613C0CF22

Verification

true

✓

```
#####  
Key sending  
Key: 33aee361f2d0ac3ea7c6d29768fcafc5e5962b13b138a82e0302072613c0cf22  
A Modulus: 5e1c6c4bca5592e2a7cc73745541d53963a0de9bbc5451b56defc00c3b522c81  
A Public exponent: 14a89048abf330c11f26245c5c72ac33cf48fc190b8b02d7ffc37f77a2ac3e2d  
A Encrypted key: 8127c917361f465e2abe23e03785f02f589aa659fa8e39b89d5ca462aa8d0cca  
A Key sign: 312026251f4fbf302a1f3a3f427ef82a8cb70940fbb4eb056cfb01a2f6346d53  
B Key: 33AEE361F2D0AC3EA7C6D29768FCAFC5E5962B13B138A82E0302072613C0CF22  
B Got correct key: True
```

## Висновки

Було реалізовано процедуру перевірки числа на простоту за тестом Міллера-Рабіна, процедуру генерації випадкового простого числа заданої довжини, основні процедури схеми RSA, а також процедури для розсилання ключів відкритою мережею. Усі процедури пройшли перевірку на коректність