

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія

Лабораторна робота №4.

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

Виконали:

Студентки групи ФБ-92

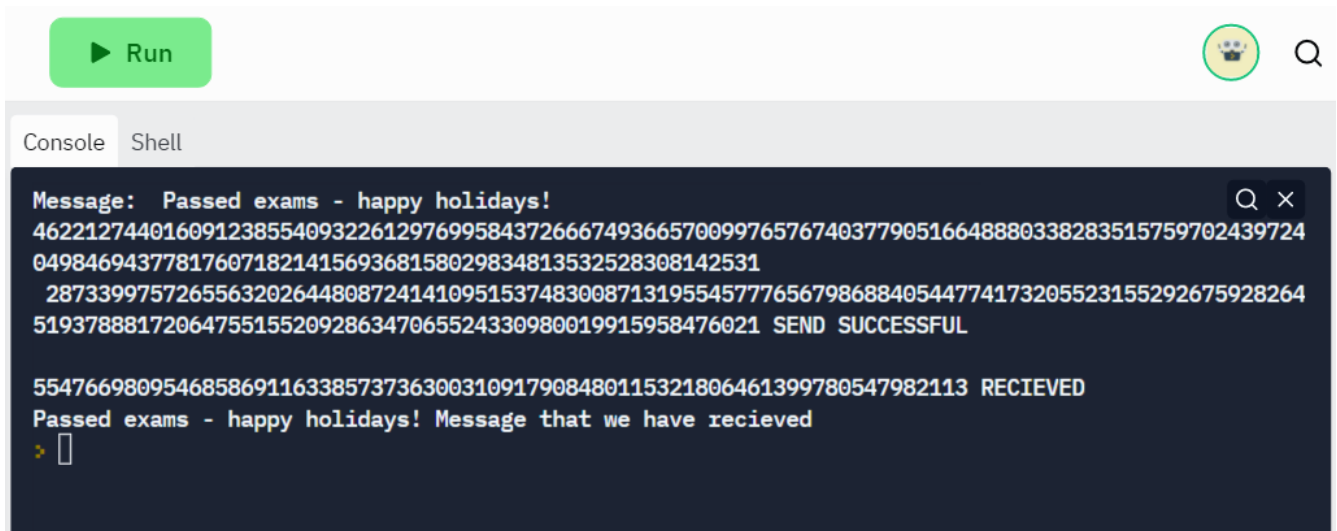
Казанкова Марина та Шаповал Ольга

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) 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

Скріни виконання:



The screenshot shows a code execution interface with a green 'Run' button at the top. Below it, there are tabs for 'Console' and 'Shell'. The 'Console' tab is active, displaying the following output:

```
Message: Passed exams - happy holidays!  
46221274401609123855409322612976995843726667493665700997657674037790516648880338283515759702439724  
04984694377817607182141569368158029834813532528308142531  
2873399757265563202644808724141095153748300871319554577765679868840544774173205523155292675928264  
51937888172064755155209286347065524330980019915958476021 SEND SUCCESSFUL  
  
554766980954685869116338573736300310917908480115321806461399780547982113 RECIEVED  
Passed exams - happy holidays! Message that we have recieved  
> 
```

Перевірка за допомогою сайту:

```
Console Shell

Message: Passed exams - happy holidays!
n = 945A0507D916A6EE8741B4113D1D605C90776CDD5A7EACB78F6553AB68A729873894FFD8CE7FD90751FE69111ABD27739F7280C125E36A2C4B5E4D3FF3C61297
e = 18D49074A67B2CF89260D529FEC362FD6961F007F3FCDA2FAE26AF57AC74A54DF402CEAF0F09920F1A96553495D2E0D67540721D16FA2AABCB520E4848797AAB
Encrypted: 36A42E4936BCB90C344041E5BE8603385D8EDDA2BEF43B3C0955516E7443B8937148E40019B839DDA9DBD155D8A79DD217E6A48E40847FC97AF9D47B008B738C
Decrypted: Passed exams - happy holidays!
```

Encryption

Clear

Modulus

945A0507D916A6EE8741B4113D1D605C90776CDD5A7EACB78F6553AB68A729873894FFD8CE7FD90751FE6

Public exponent

18D49074A67B2CF89260D529FEC362FD6961F007F3FCDA2FAE26AF57AC74A54DF402CEAF0F09920F1A965

Message

Passed exams - happy holidays!

Text

Encrypt

Ciphertext

36A42E4936BCB90C344041E5BE8603385D8EDDA2BEF43B3C0955516E7443B8937148E40019B839DDA9DBD