

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія
Лабораторна робота №4
Варіант 8

Виконав:
студент 3 курсу ФТІ
групи ФБ-05
Тимченко Юрій

Перевірила:
Селюх П.В.

Київ – 2022

Мета та основні завдання 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.

```
Ключі персонажа - В
e2: 607873463872906882194578207542606136103510266785735067345097567657170590979746576041169914687736837288701107721832141154105696340101636871575739919343765
n2: 7179141584549664301005700144243416282463894029321400067041998525524293677393998583173501207923228434937011800055113487145589363153320126271308313098612051
d2: 3867282130907934100899174420888481573394633899588149385960760530820127153104316116370043451922970855220805525094883856081005884252747310049033522734957773
p2: 68740169587663571514678760833046775825509716423101379896496449134972375281589
q2: 10443881107092971479770979020064594049172355101923113352998755324313798774759

Початковий ключ - 3804330157275861789626298657456990500359536151386007561742002560109848446892383551551364779031056421270931647612218398476696971663344227746426435218152625
Повідомлення - 1773768919750478515423723519615247961743520207090247081675668743691890445724840401794571087282033047193226184872556774890754278180574148992408649759257200

Зашифроване повідомлення - 3623010683950147901292067785480412784661002233407417213335719749677625450589696803121246079684782603353759336909183262964272690376416262341973423307986933
Розшифроване повідомлення 1773768919750478515423723519615247961743520207090247081675668743691890445724840401794571087282033047193226184872556774890754278180574148992408649759257200
```

Get server key

✖ Clear

Key size

256

Get key

Modulus

A8D847C53C34C368D1CE41272FF9829265DB4773977A13F112BA18692BA61DF5

Public exponent

10001

384210381293129

10

= Convert

✖ Reset

↕ Swap

Hex number

15D6FF34BC649

16

Encryption

Modulus

A8D847C53C34C368D1CE41272FF9829265DB4773977A13F112BA18692BA61DF5

Public exponent

10001

Message

15D6FF34BC649

Bytes

Ciphertext

702801701039F0AC418CC3FE8C781D81D20A90002BCFC119D40569F79D39B2F4

Decryption

Ciphertext

702801701039F0AC418CC3FE8C781D81D20A90002BCFC119D40569F79D39B2F4

Bytes

Message

015D6FF34BC649

Висновки : під час виконання лабораторної роботи ми отримали навички реалізації та розуміння роботи критпосистеми RSA, алгоритму електронного підпису та генерації ключів та простих чисел, їх перевірка на простоту ймовірнісним тестом Міллера-Рабіна.