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

Виконав:

студент 3 курсу ФТІ

групи ФБ-91:

Журибіда Юрій

Перевірили:

Завадська Л.О.

Савчук М.М.

Чорний О.М.

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
Розробив генерацію простих чисел використовуючи алгоритм Міллера-Рабіна. Отримав

такі ключі:

Не підішли

p	87712318261378620149198826970027921569334876550367817178720576404166341115467
q	99146022764343390573419076584380170396845524721195828708439227458418771270617
p1	78562029269744047537695109603016771320531893923877976946228510894737541365103
q1	88443801083041512879370012353283014479424569640998305798833951792877735429213

p	69964978581136015001099940326223900140061805537718315936135244481477645422091
q	76851878662829645256946521328283394587830776704439344766844121494534456915919
p1	57899346535013841978539748209593324543281142033485981142443454883756709310921
q1	83475390646453016537421100282238302588494403101874284302942258306573380419301

Підішли:

p	74922627183685304053722884322805637745690272692523044793486349668123438040829
q	75324767041681899148494173923250897223405873538487952032903781718006914781417

p1	11190167162897700156414740494209623893097631015523692082845262487195348172562 1
q1	95361536723636825973566889979596239333188200025823244746304352097879684478703

Реалізував RSA алгоритм та передачу приватних ключів.

ВТ:

184807115158686520813678882990735931223271643193820529512169610251491692837581536519750652961436368756959464082923489352085949430520466839340102893248269 6

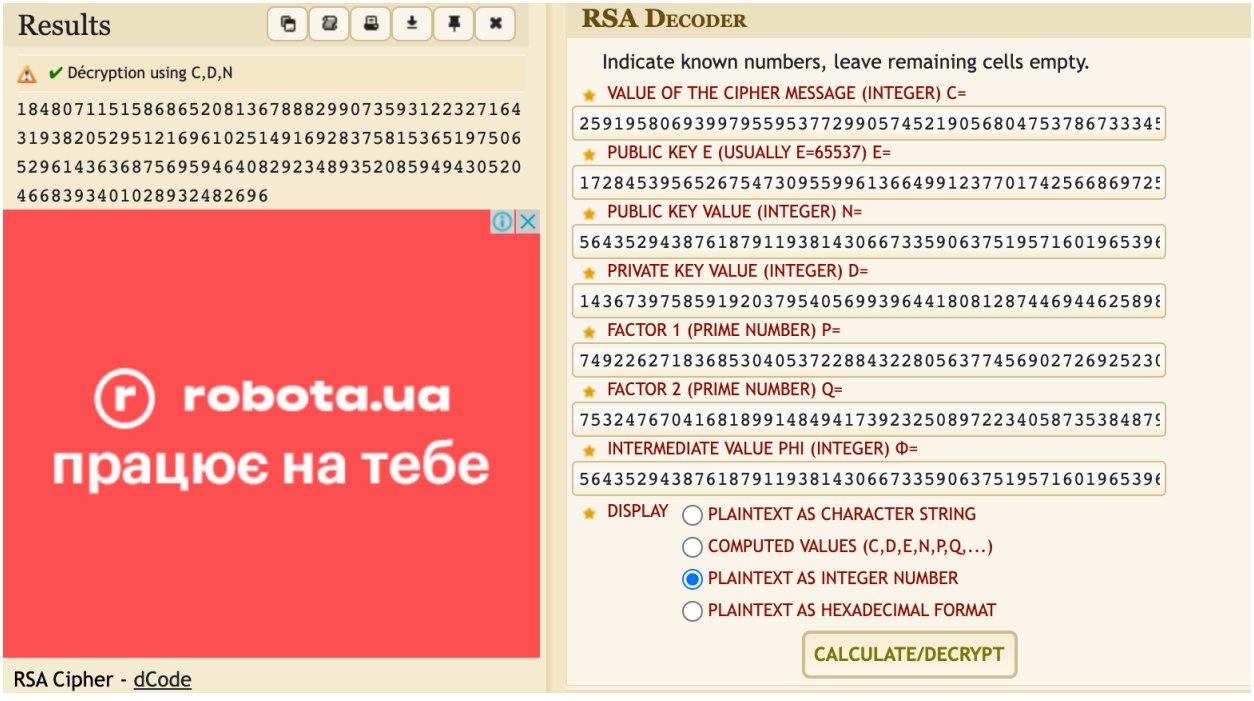
ШТ:

259195806939979559537729905745219056804753786733345878414435822987049541894974012873642091326230573700678269695686999235610642038059349550697199346736210 3

Перевірка локально:

```
/usr/local/bin/python3.8 /Users/uuriyzhuribeda/Documents/stud5sem/cryptolab/fb-labs-2021/cp_4/lab4.py
n:  564352943876187911938143066733590637519571601965396676255339481286532782340352617472468953113059913713926232306854538111943819819646329183084887 5
e: 172845395652675473095599613664991237701742566869725486144281691604653027307523120045247669362001458711128880994991957733551210349668407917346731 71
d: 143673975859192037954056993964418081287446944625898381696801180679583669231996350335619362056204862239581330854229419098408848537090630160333807 8
M:  184807115158686520813678882990735931223271643193820529512169610251491692837581536519750652961436368756959464082923489352085949430520466839340102 8
C:  259195806939979559537729905745219056804753786733345878414435822987049541894974012873642091326230573700678269695686999235610642038059349550697199 3
f: 564352943876187911938143066733590637519571601965396676255339481286532782340337592733046416392739692008101626653357628497320718719963690169946274 49
Text verification:  True
Key verification:  True
```

За допомогою онлайн ресурсу:



Висновки:

В ході лабораторної роботи отримав навички з генерації великих простих чисел. Реалізував RSA алгоритм. Основні труднощі виникли з оптимізацією коду для півищення швидкодії. Для цього використав бітові операції та схему горнера.