Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут» Фізико-технічний інститут

Лабораторна робота №4

З дисципліни:" КРИПТОГРАФІЯ"

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

Перевірила:
Байденко П. В.

_____

Виконали:
студенти III курсу
групи ФБ-95
Корольова В.Р.
Групи ФБ-96
Гуменюк О.О.

Мета: Навчитись проводити тести щодо перевірки чисел на простоту дослідити та реалізувати схему RSA ,а також цифровий підпис відносно RSA та розсилання ключів.

Постановка задачі:згененерувати пари ключів для Аліси та Боба (qp),(q1p1)для шифрування відносно системи RSA ,з використанням закритому ключі та розшифруванням на відкритих ключах.

Варіант 2

p:90537879588897465387133326884708486476041471186471324048449300458247492416481

q:86150101796519139448559302808615911065040892953424399390382754402822117919089

p1:10630854118054641013925473535264731387091319367071045223527093390088853623536 1

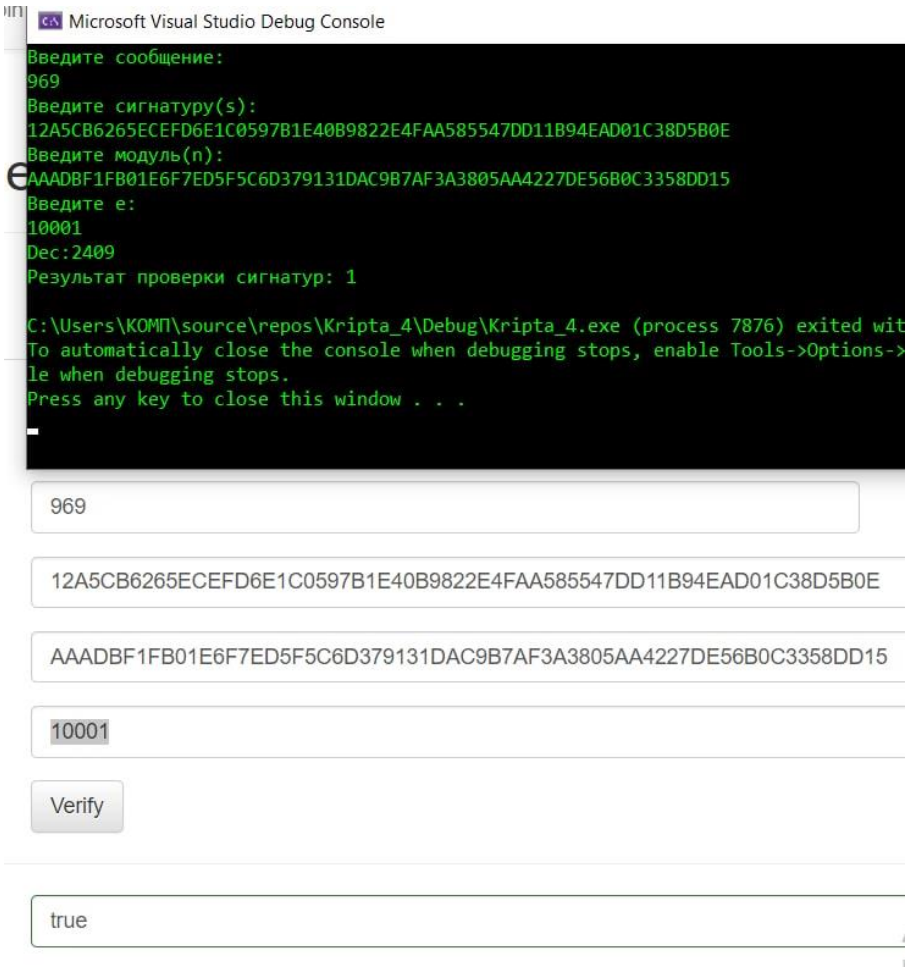
q1:78603014483957224374389812927464060860199976595920782564577255051874782387819

BT: 2148

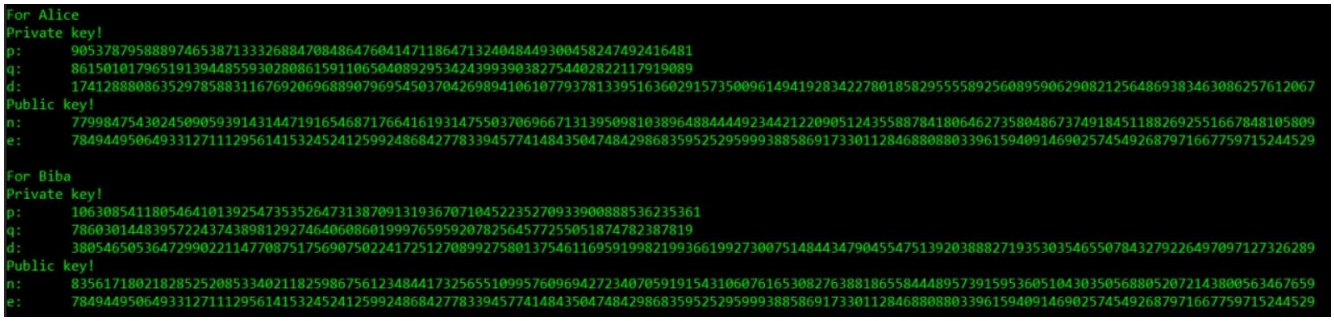
ШТ:22466593055797464643665705711922181013958012057064306617387849480780145618376097620938237141683685930887330896766045592397163526150363877223921714189926 12

```
5789604461865809771178549250434395392663499233282028201972879200395656481996 8
1157920892373161954235709850086879078532699846656405640394575840079131296399 35

For Alice
Private key!
p:      90537879588897465387133326884708486476041471186471324048449300458247492416481
q:      86150101796519139448559302808615911065040892953424399390382754402822117919089
d:      17412888086352978588311676920696889079695450370426989410610779378133951636029157350096149419283422780185829555589256089590629082125648693834630862576120 67
Public key!
n:      77998475430245090593914314471916546871766416193147550370696671313950981038964884444923442122090512435588784180646273580486737491845118826925516678481058 09
e:      78494495064933127111295614153245241259924868427783394577414843504748429868359525295999388586917330112846880880339615940914690257454926879716677597152445 29

For Biba
Private key!
p:      10630854118054641013925473535264731387091319367071045223527093390088853623536 1
q:      78603014483957224374389812927464060860199976595920782564577255051874782387819
d:      38054650536472990221147708751756907502241725127089927580137546116959199821993661992730075148443479045547513920388827193530354655078432792264970971273262 89
Public key!
n:      83561718021828525208533402118259867561234844173256551099576096942723407059191543106076165308276388186558444895739159536051043035056880520721438005634676 59
e:      78494495064933127111295614153245241259924868427783394577414843504748429868359525295999388586917330112846880880339615940914690257454926879716677597152445 29

Biba send Alice messege!
Enter messege Hex:
2148
Entcripted text:
22466593055797464643665705711922181013958012057064306617387849480780145618376097620938237141683685930887330896766045592397163526150363877223921714189926 12
M:
12373303375738502417570571861396448916497716592916900041308377761155390029571741678652441441659580882179539032475111726518879694226454802720989291376923 55
S:
10213088765570303925605323586864140908449529807263486080963209057980061929073951117540785629238458972636178369809148901669250478398023834944591482232917 31

Dec:12373303375738502417570571861396448916497716592916900041308377761155390029571741678652441441659580882179539032475111726518879694226454802720989291376923 55
Результат проверки сигнатур: 1
Decripted text Dec:
8520
Decripted text Hex:
2148
```

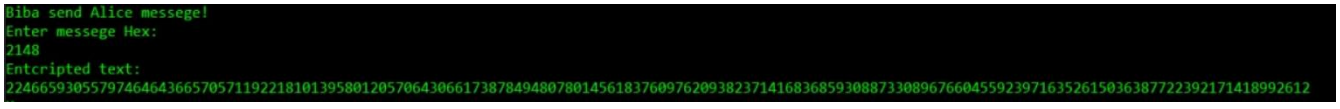
Перевірка:



Опис кроків протоколу конфіденційного розсилання ключів з підтвердженням справжності, чисельні значення характеристик на кожному кроці:

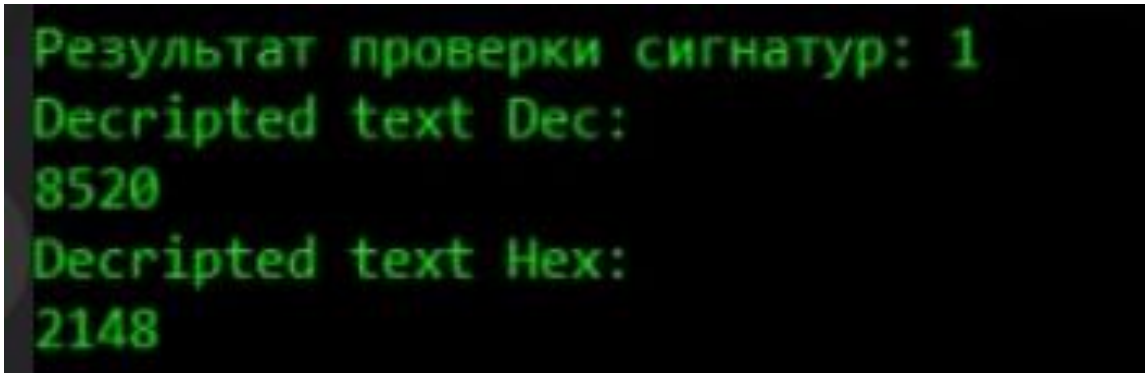


Генеруємо числа p і q для А та Б. Також генеруємо n, e та d для кожного.Далі у наступному кроці ми шифруємо наш текст. CipherTextRSA()



Робимо цифровий підпис DigitalSignatureRSA

Відправляємо наш шифрований текст абоненту б.Абонент б приймає повідомлення і перевіряєм його цифровий підпис зі своїм.Після перевірки цифрового підпису якщо він правильний, то дешифруємо наше повідомлення. Check_Signature().



Висновок:навчились генерувати прості числа,з перевіркою відносно тестів,які призвели для правильної реалізації криптосистеми RSA, та відповідного електронного підпису,для якого також було створено перевірку щодо відповідності до ВТ.