МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

з дисципліни

Криптографія

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

Перевірила:
Селюх П.В

Виконала студентка
групи ФБ-94
Спільна А.С.

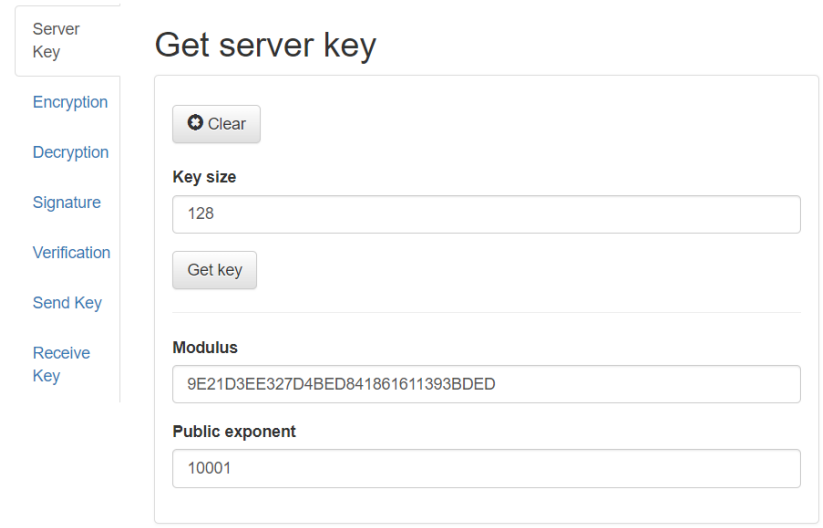
Мета та основні завдання роботи:

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.

Результат роботи програми:

```
Числа для создания ключей для абонента A:
 p = 60451694040390738481677253328507785690689048666500487118567980050868969632161
 q = 65609363449604380774604288186708352308856088315139816887792721618210048891807

Числа для создания ключей для абонента B:
 p1 = 83452631297909239878096649311628164786217910937140377178199436340198168618863
 q1 = 11561994645852206212292988380754953198643750255048004937021454653599332439167

Открытые ключи абонента A:
 e = 17808756392552958053892290273782719310971850750728256509000361098455801715670912656450625536629355210837323719592852291121295392690394367810752070064874 79
 n = 39661971654402790886881461271072158145275626563602967691032149945632620492074667917784485770474212492411626560414103667105787408380860433150973544766049 27
Секретный ключ абонента A:
 d = 11731921779001206236244325837777448630977773278905723842448820160340150416573756389732349986031879796535374253992876451682832254975594529710887594521563 59

Открытые ключи абонента B:
 e = 37547769787775532499952749561654679984648573528563159623339350320993490993047747878242240218520765262893420759526569597695637183446805101662121336448658 1
 n = 96487887624870488199084844028351442128169316073069496739601277379687901158305230853063037842795347038475679080065069899975629962794629767543403507262071 21
Секретный ключ абонента B:
 d = 35864981758972664221895908093947956483180475443578027034806088382814222710315083714731293335692025094297775931657757195797634310642144500303517794305546 57

Секретное значение :
 k = 38009032352219892791744923174701107154853058845657321104531136164164026218916983654569065660144408334800653324682799732377073172418133891711819207632318 61

Сообщение :
  33899036771909424669296939427911370311704773820640318951509568235924474221101248798897947509299960545347897739296548358371537297482835114439366709611000 01

Аутентификация прошла успешно !!!
Текст прошел верификацию !
```

```
Зашифрованное сообщение :
 27541172731194776119931390989779141060349332328850832089915317994162850832806626318136163430322904240836002900185483079307565187242530281161770757206947 28

Дешифрованное сообщение :
 33899036771909424669296939427911370311704773820640318951509568235924474221101248798897947509299960545347897739296548358371537297482835114439366709611000 01
[Finished in 15.3s]
```



```
Открытые ключи абонента с сайта:
 e = 65537
 n = 21019366759070313090531692969428803530 9
Сообщение в 16-ричной системе :
 31
Зашифрованное сообщение :
 196672383617115507957143020825737936 62
[Finished in 35.7s]
```

Encryption

Clear

Modulus 9E21D3EE327D4BED841861611393BDED

Public exponent 10001

Message 31 Bytes

Encrypt

Ciphertext 0ECBC5B750C2F70DF9869BDD946DF97E

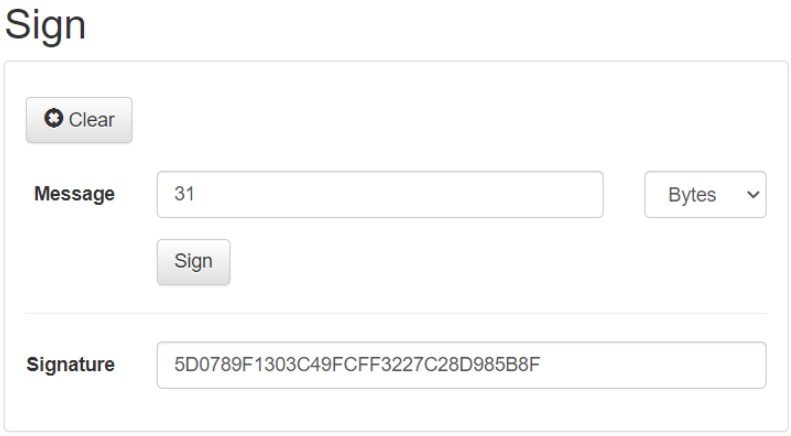
Исходное основание
10
Основание системы счисления исходного числа

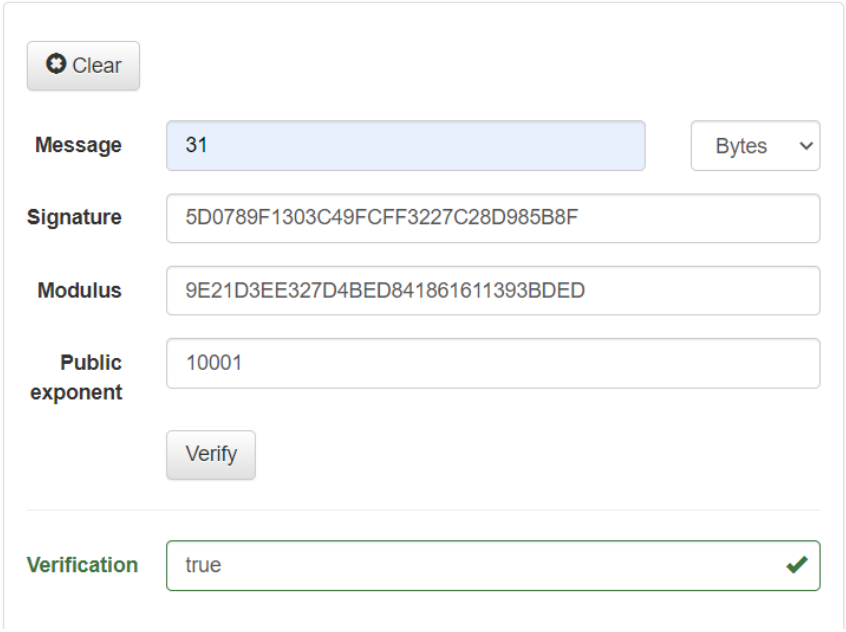
Исходное число
196672383617115507957143020825737
Число которое необходимо преобразовать

РАССЧИТАТЬ

Основание результата
16
Основание системы счисления переведенного

Переведенное число
ECBC5B750C2F70DF9869BDD
946DF97E






```
Открытые ключи абонента с сайта:
 e = 65537
 n = 21019366759070313090531692969428803530 9
Сообщение в 16-ричной системе :
 31
Зашифрованное сообщение :
 19667238361711550795714302082573793662
Цифровая подпись :
 12365734748503795161033021195113413723 1
Верификация :
 1
[Finished in 41.0s]
```

Код:

```
modulus = int("9E21D3EE327D4BED841861611393BDED",16)
exponent = int("10001",16)
print("Открытые ключи абонента с сайта: \n", "e =", exponent, "\n n =", modulus)
text = 49
print("Сообщение в 16-ричной системе :\n",31)
A = [exponent,modulus]
encrypt_text = Encrypt(A,text)
print("Зашифрованное сообщение :\n", encrypt_text)
sign_text = int("5D0789F1303C49FCFF3227C28D985B8F",16)
print("Цифровая подпись :\n", sign_text)
vr = Verify(A,text,sign_text)
print("Верификация :\n", vr)
B = GenerateKeyPair(p1,q1)
key_s_B = [B[2],p1,q1]
k = random.randint(1, A[1])
send_key = SendKey(A,key_s_B,k)
print("moduls = ", B[1])
print("exponent = ", B[0])
print("\nSignature : ",send_key)
```

Висновок:

Під час виконання комп’ютерного практикуму я ознайомилась з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. А також з системою захисту інформації на основі криптосхеми RSA, з використанням цієї системи засекреченого зв'язку й електронного підпису.

Вивчила протокол розсилання ключів.