Міністерство освіти і науки України 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 Живодьоров 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.

Робота функцій

```
C = Encrypt(123456789,e1,n1)
                                               C:\Users\artem\AppData\Local\Programs\P
 M = Decrypt(C,d1,n1)
                                              123456789
 print(M)
                                              Proved
                                              54321
 S= Sign(M,d1,n1)
                                              Press any key to continue . . .
 if Prove(M,S,e1,n1):
     print("Proved")
∃if n1 < n2:
     k1,S1 = Send_Key(e1,n1,n2,d1,54321)
     k = Receive_Key(k1,S1,d2,n2,e1,n1)
⊟else:
     k1,S1 = Send Key(e2,n2,n1,d2,54321)
     k = Receive_Key(k1,S1,d1,n1,e2,n2)
 print(k)
```

Робота з Сайтом

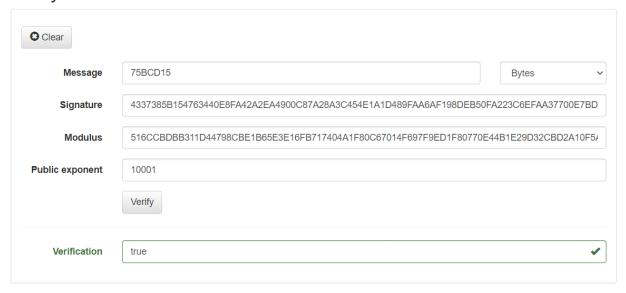


Encryption

• Clear			
Modulus	63FA0913D45B3A01A8C9C0A89C6153FCA5AD60D500EA9572CFCA958490728A18A	AAF08FC12C30AD9F	E0E
Public exponent	10001		
Message	75BCD15	Bytes	~
	Encrypt		
Ciphertext	D90164609F673614F02CB81C9A326E4DB3AE80DED610EBC0775616DE0476EE1EA	5E3840120F1387FFFI	D61

```
C:\Users\artem\AppData\Local\Programs\Python\Python39\python.exe
Message 75BCD15
Sign 4337385B154763440E8FA42A2EA4900C87A28A3C454E1A1D489FAA6AF198DEB50FA223C6EFAA37700E7B<u>D</u>62AFC3F42ACF4A482955994921F4D
956CC876949270
lodulus 516CCBDBB311D44798CBE1B65E3E16FB717404A1F80C67014F697F9ED1F80770E44B1E29D32CBD2A10F5AF473EEC35369889703A7CC2E8B
DEFD142A350F75107D
Public exponent 10001
S= Sign(M,d1,n1)
Sign = conv(str(S), 10,16)
Modulus = conv(str(n1), 10,16)
Message = conv(str(M), 10,16)
print("Message ",Message)
print("Sign ",Sign)
print("Modulus ",Modulus)
E1 = conv(str(e1), 10,16)
print("Public exponent ",E1)
if Prove(M,S,e1,n1):
      print("Proved")
```

Verify



Висновок

Після виконання даної лабораторної роботи я практично ознайомився з системою захисту інформації на основі RSA, навчився генерувати прості числа. Навчився шифрувати та розшифровувати текст, ставити та перевіряти підпис. Організував функції обміну ключами.