Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

Криптографія

Лабораторна робота No4.

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

Виконав:

Студент групи ФБ-95

Спориш Євгеній

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:

1) Спочатку написали функцію перевірки простоти числа тест Міллера-Рабіна
2) Згенерували дві пари простих чисел
3) Написали функцію генерації відкритого та закритого ключів для двух абонентів для RSA
4) Написали функції: шифрування та розшифрування і створення цифрового підпису
5) Організували обмін повідомленнями між абонентами A і B

Скріни виконання:

462373215600765212545785735100583165313691408777848196222561240403560873097651062132096195489988471850124208269580790024527918381118976700496932243041321601618484672062541760819375957886666605985737232623907097881738409797955804287423669906957782664527556016132650348665239344918940557173258595640289020343526103137020568013622082924196530529959754252977465904222340391921381412991020041

#----------#

Кінець відкинутих простих чисел

A

p 537622754019000684631595615594905938710604249199205645313183575106781068647831

q 611550433203217944628691156926775805815095023432930608309384208341728936778331

B

p 288749685612907942767021758318008655294761598509016148915953625599022747232431

q 544520634335113299058948890200728053146279116801497464061708474412556294503031

A_key

n

3287834281202269499711064714777564853196718698006583709791410686828105290679867691877449090337782727252557820221061805629900959441690684554668137695455239

e

1499890623913261698591263069503488715502417456453795090227604271961960955501248641942567294893548529280008108183816990522894865916946415576454774798070827

d

3192189509384739290345834961037615658138327643479423294578318480370798521655767836923136423333859469575665270302113580624305204444509256073572942823016835

B_key

n
15723016197400517132711029332776675157129824735208512503935245623350362233505628982475434432433583221101028870534332708837703182270948551680648995474926629
e
11991086630256027420713218358725220542715633768361721721628398732498079114802968866252971174523579177104540547783063049622273900695217181172192479035781277
d
15536996164677458442529779167366335421297411189105918332388536915370487136415942157160845102953844616616402606100239806627239436499229436628661632596 7
data
my message 255
Message
66208711253914093521723726710196325897550212316603060984370141364559035379273894124404117923907050254542382309115471651262960237104360554763682391629379277151637981725189886720385336507175761208922583084945845907286598088080318348394082486181382745613792953725589494643902575911232082901127573048852323287
Checking Auth
255
Checking Conf
255

Перевірка за допомогою сайту

Working with remote server
We encrypt, server dercrypts
input: 0xff
encrypted:
23145223481626104007010206306840214316494081406502731925699440418123250446322877984364211541444534509456726176440081972057733697406043002012770974053897 62
response: b'{"message":"FF"}'
server signs
b'{"signature":"18E7FF7A10687465ABFFA07A399F11B1AA38AA03DB3A616DF5799050E8651461307CE8C5A68538E3AC69EC364A5A248AEA601FD892DA0937304F9B2997D39BCF"}'
server encrypts
{'cipherText':
'3D6ED67FF4BE6637B8B165246168168FE4BAF2E74BA57439DA792E62EBBF86E1E2DFD083A1FA2F912D5DA1321427EF21056392B32F7970E2C8FCEEFC1BC69823'}
result 255
server verifies
b'{"verified":true}'
Receive key
b'{"key":"FF","verified":true}'
Receive key
b'{"key":"26AAEC7082F351DAA0554EE7254E92CE8199247E515D5BAE78FC054E50BADEC34EBD1F13751090BAEBBD84927E18986783D60DEB05C5A20AA9C76190F3A67D03","signature":"229440D751E75890A4A0121381418D1ACEF5FF660CF59EBBFC1F2CA507A6D0EDFADADDA4477674651BBB8EB9D93416BDD7FAA1D7FDF5A1F44EF5BCE4FE90C6AB"}'

Process finished with exit code 0