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 А і В

Скріни виконання:

46237321560076521254578573510058316531369140877784819622256124040356087309765 106213209619548998847185012420826958079002452791838111897670049693224304132160 16184846720625417608193759578866666059857372326239070978817384097979558042874 23669906957782664527556016132650348665239344918940557173258595640289020343526 103137020568013622082924196530529959754252977465904222340391921381412991020041 Кінець відкинутих простих чисел p 53762275401900068463159561559490593871060424919920564531318357510678106864783 q 61155043320321794462869115692677580581509502343293060830938420834172893677833 p 28874968561290794276702175831800865529476159850901614891595362559902274723243 q 54452063433511329905894889020072805314627911680149746406170847441255629450303 A_key 328783428120226949971106471477756485319671869800658370979 141068682810529067986769187744909033778272725255782022106 1805629900959441690684554668137695455239 е 149989062391326169859126306950348871550241745645379509022 760427196196095550124864194256729489354852928000810818381 6990522894865916946415576454774798070827 d 319218950938473929034583496103761565813832764347942329457 831848037079852165576783692313642333385946957566527030211 3580624305204444509256073572942823016835 **B_key**

n

157230161974005171327110293327766751571298247352085125039 352456233503622335056289824754344324335832211010288705343

3270883770318227094855168064899547492629

е

119910866302560274207132183587252205427156337683617217216 283987324980791148029688662529711745235791771045405477830 6304962227390069521718117219247903578127

d

155369961646774584425297791673663354212974111891059183323 885369153704871364159421571608451029538446166164026061002 398066272394364992294366286616325967

data

my message 255

Message

66208711253914093521723726710196325897550212316603060984370141364559035379273894124404117923907 050254542382309115471651262960237104360554763682391629379

2

77151637981725189886720385336507175761208922583084945845907286598088080318348394082486181382745 613792953725589494643902575911232082901127573048852323287

8

Checking Auth 255 Checking Conf 255

Перевірка за допомогою сайту

Working with remote server We encrypt, server dercrypts input: 0xff encrypted:

> 231452234816261040070102063068402143164940814065027319256 994404181232504463228779843642115414445345094567261764400 8197205773369740604300201277097405389762

response: b'{"message":"FF"}'

server signs

b'{"signature":"18E7FF7A10687465ABFFA07A399F11B1AA38AA03DB3A616DF5799050E8651461307CE8C5A68538E3 AC69EC364A5A248AEA601FD892DA0937304F9B2997D39BCF"}'

server encrypts {'cipherText':

> '3D6ED67FF4BE6637B8B165246168168FE4BAF2E74BA57439DA792E6 2EBBF86E1E2DFD083A1FA2F912D5DA1321427EF21056392B32F7970 E2C8FCEEFC1BC69823'}

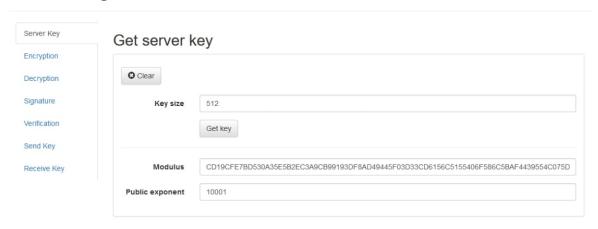
result 255
server verifies
b'{"verified":true}'
Receive key
b'{"key":"FF","verified":true}'
Receive key

b'{"key":"26AAEC7082F351DAA0554EE7254E92CE8199247E515D5BAE78FC054E50BADEC34EBD1F13751090BAEBBD
84927E18986783D60DEB05C5A20AA9C76190F3A67D03","signature":
"229440D751E75890A4A0121381418D1ACEF5FF660CF59EBBFC1F2CA
507A6D0EDFADADDA4477674651BBB8EB9D93416BDD7FAA1D7FDF5
A1F44EF5BCE4FE90C6AB"}'

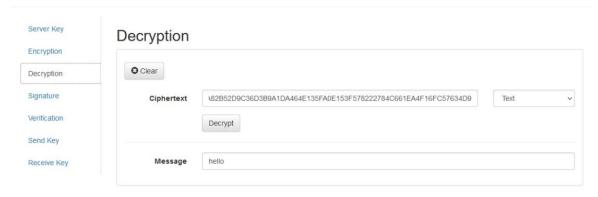
Частина 1

Генеруємо ключі на сервері, шифруємо у себе, розшифровуємо на сервері

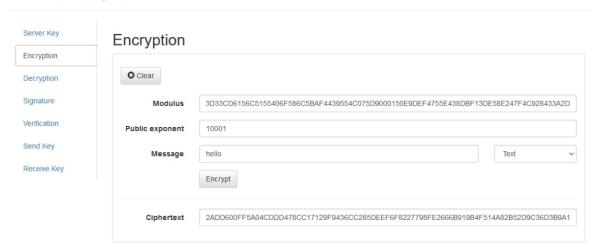
RSA Testing Environment



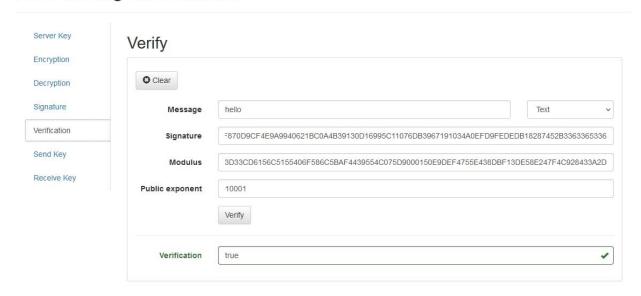
RSA Testing Environment



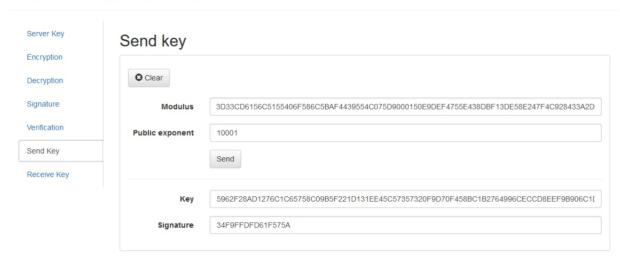
RSA Testing Environment



RSA Testing Environment



RSA Testing Environment



RSA Testing Environment

