КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

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

Варіант 12

Виконали:
ФБ-05 Левицький Євген
ФБ-05 Дегтярьов Микола

Київ – 2022

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.

Хід роботи:

В рамках виконання практикуму було створено функції:
test_number – перевірка числа на простоту на основі тесту Міллера
find_number – генерує число, перевіряє його тестом Міллера
generate_keys – генерує p, q, p1, q1
extended_evclid – розширений алгоритм Євкліда
inverse_mod – функція пошуку оберненого
rsa_pair – генерує d,n,e
enc_msg – шифрує повідомлення
Decryption – розшифровує повідомлення
sign – функція підпису повідомлення
sign_check – перевірка надісланого підпису
send_key – надсилання шифрованого повідомлення
receive_key – отримує повідомлення і перевіряє підпис

Вивід виконання програми:
Для користувача A

```
A


e: 258728376802959551450601009245992765763583862382285758487047163796717999067207971642692147579290211558840589349471596036698223937378044246813023700241982
9
n: 597556409375606469703757067608115973240528992264387423762585435420770983079369870969779292788417918325210932419151725815192826505451091182141805360730176
3
d: 720762466218371136796928434589871303505412107931620984658683924323510473480663646934477790178927895961311633652129205851493419956025898707570713446955829
p: 96561986816167988918821470815870831479822077719694440257000448560907423790461
q: 61883193281142573940978296492052652146917487820875121754527502390355017283583
```

Для користувача B

```
B


e_1: 84602997008520106799390232670612169233076025868551705987999156365102086006254585444853141842099045209562427228511295141147174393123343808305088714975885
19
n_1: 12547245150001754961410740161620213881362304514792304973380295399076024301532783775445025175715300717008935594469949260013807866731742543161489382641609489
d_1: 11377405577311117641227911288433036764993263938970519495082538826313552280508919865902238062546605950497652595124989870592157873728936258927040169575669039
p_1: 11551467342808982986533182155848896289115821294347488865813282654066595656 2871
q_1: 10862035772288845507884474584593797852719759373731717641096437244202114450 3159
```

Вивід к, повідомлення, підпису, зашифрованого і розшифрованого повідомлення

```
Start k: 3043828053492679529448352961431433596161044339769769240867182808548259141830657545105077045132899966113531472601633604414983493646035310714183552553354616
Message: 85586963369869696636870756452058244602742979448995302273760263092986908786019177288308712817422553813024703897866105632917888296407665584291631413720573 1
Sign: 113581120307508583446042769841621985726174055194659414932326505468744653860304796169526570228713832711474299439658101535001768543777997028360267111586956697

The key has been received: 3043828053492679529448352961431433596161044339769769240867182808548259141830657545105077045132899966113531472601633604414983493646035310714183552553354

Encrypted message: 5561995830590965561761587589119640302551178792189073689029946768052403235409720370390423320568615321844245046223021672077474193398092661733657549213147197
Decrypted: message: 85586963369869696636870756452058244602742979448995302273760263092986908786019177288308712817422553813024703897866105632917888296407665584291631413720573 1
```

Починаємо перевірку за сайтом

Get server key

Clear

Key size 256

Get key

Modulus AB377B7E3A23BFA837930FD72C3C2DBEB9D96D74D9CF3472F4D44B53FF273CD3

Public exponent 10001

Encryption

Clear

Modulus AB377B7E3A23BFA837930FD72C3C2DBEB9D96D74D9CF3472F4D44B53FF273CD3

Public exponent 10001

Message 54321 Bytes

Encrypt

Ciphertext 3A0CD8DD2B7F9E99FA92E2C18810EBB71E142CFF8ECD17D9293E0AB5FBAF5A75

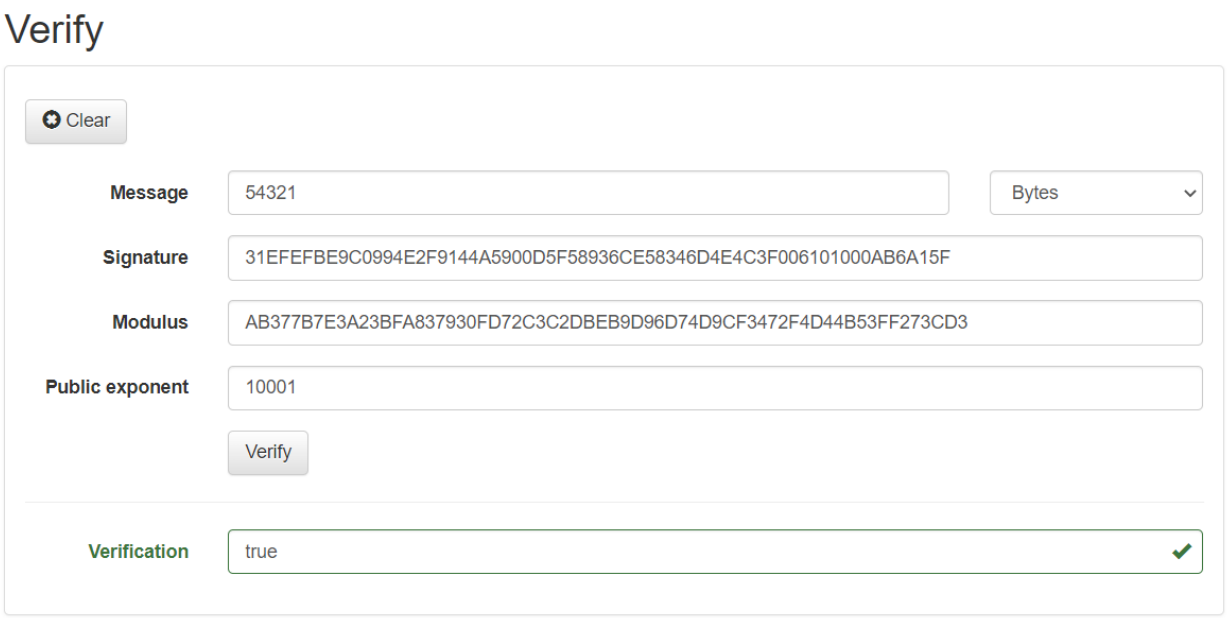
Sign

Clear

Message 54321 Bytes

Sign

Signature 31EFEFBE9C0994E2F9144A5900D5F58936CE58346D4E4C3F006101000AB6A15F



Перевірка кодом значень шифротексту і підпису з сайту
Зробивши маленьку модифікацію

```python
def sign_check(self):
    if self.m == pow(self.s, self.e, self.n):
        print("Success")
    else:
        print("Fail")
    return self.m == pow(self.s, self.e, self.n)
```

Пишемо код з переведенням і функціями

```python
n = int("AB377B7E3A23BFA837930FD72C3C2DBEB9D96D74D9CF3472F4D44B53FF273CD3", 16)
print(f'n: {n}')
e = int("10001", 16)
print(f'e: {e}')
msg = int("54321", 16)
print(f'Message: {msg}')
encrypted_msg = Encrypting(msg, e, n).enc_msg()
print(f"Ciphertext: {hex(encrypted_msg)}")
sign = int("31EFEFBE9C0994E2F9144A5900D5F58936CE58346D4E4C3F006101000AB6A15F", 16)
print(f"Sign is: {sign}")
SignCheck(msg,sign,e,n).sign_check()
```

Можемо порівняти результат, шифротекст сходиться, підпис підтвердився

```
n: 774435260141781179130270855569162854806456447624679865969118184932456125718 59
e: 65537
Message: 344865
Ciphertext: 0x3a0cd8dd2b7f9e99fa92e2c18810ebb71e142cff8ecd17d9293e0ab5fbaf5a75
Sign is: 225872606852614957255418918828025903070038270240177730245472683325741527616 95
Success
```

Висновки

В результаті виконання практикуму ми практично ознайомились з системою захисту інформації на основі криптосхеми RSA. Було засвоєно і практично використано тест Міллера-Рабіна для перевірки чисел на простоту і генерації простих чисел. Мали змогу використати Asym Crypto Lab Environment і з його допомогою перевірити нами створені функції криптосхеми RSA.