

НТУУ "КПІ ім Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

Вивчення системи RSA та електронного підпису

Виконав:

студент групи ФБ-14 Хаща Іван

Київ 2023

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.

```

1 9952264186728472799492773251726114560010685206748407194221865488484311963684861798
2 253982427219208593434854098019089728760878239794982109829129853378859559940520975
3 6455015688010537939182144442129456045651704997070487339848445026826918162196630814
4 6512133653218640875942967806818284057379432828330984743348142758343677293456693038
5 6219619026126259014483754896689720397990720253161260839496813429410371468305418837
6 988005062556769303356686947793253509544448996396795537393788084119050592007340651
7 1084830188874984134949495078778064919189114966292296927682509045661535572907550970
8 1640364823434526211796324496077482843525224705063040408836622863342485071804991668
9 3426276554557030978117741108026647382117069429565954281969029600268885694899292551
10 352729527720811033215446032614129330014444621288018319211632962348334960973428872
  
```

За допомогою цієї функції згенерувати дві пари простих чисел p, q і $1 < p, q$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $p \nmid q$; $p \nmid q$ – прості числа для побудови ключів абонента А, $1 < p < q$ – абонента В.

```

Користувач А
p = 23778263326614833014143846427873593517855462826671004956005332597576861484031899712821638204079854357888392929574663692419796136023803288134144038997921466261042773891993847656308989919872941424572240726
q = 8291954498657913580739668105135406223204871773618358623361567647557349158799364714611601481876564275698866534767395209378262039863522947187899846046017146288442501684440260153992565511160492955236477810
Public key: (1249817367621657155377457835652674855821745767384384855806001564134128633206373496733477627041573417054958922511255107108051915240903163326274851560636386714514664234739155934845894243170835256
Private key: 95311284911981801399055531175621463065646707188631747528097351104667437268751210881305342111857512898290521455603881720902382757131289570390292327748725061910544286105105755859670445239003416844

Користувач В
p = 23778263326614833014143846427873593517855462826671004956005332597576861484031899712821638204079854357888392929574663692419796136023803288134144038997921466261042773891993847656308989919872941424572240726
q = 8291954498657913580739668105135406223204871773618358623361567647557349158799364714611601481876564275698866534767395209378262039863522947187899846046017146288442501684440260153992565511160492955236477810
Public key: (19716827756139635009413286205427315940899525437958234154205283670847256418453193350530079367068624720089350471982789779759579615209984438821231373932722957666902136468372121223350497472647371156
Private key: 354732618325606309138075555002418210470695094968728182740047003078566312617019436289426824802877062950295732412973958117478725650257511301114471673111927519575859302357075870956746112860145110
  
```

Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення М і знайти криптограму для абонентів А и В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його

Повідомлення: 8227455934535141042140333525152174500659826452337044678455581855176808598831003736497384857496959585982815780845127965586268397456021517873063015599185506095916922667713165184200826862376056807480826647381219237166620675933371573819084336775094502445732011602194692859297748187588516783061189381554558055133976808428770284950930247456277157768329112101671198117416536937476426651106830712908323770172306378725480595131493802842379458359187757054022063621072639579206077216469020762877584071537520360964965

Зашифроване повідомлення за допомогою відкритого ключа A: 2155752966089226377143256167718144692895367949826934624200842035293724549328152034045745361081908121258126818660188314312084705835464019368575133932217944574137386048899083199235869296183641894121574413287022441952295594498172830725082063802530139676942849133325389572621539908663307760203573339629364463856896688644701131882606542205948758559523238268469740208969606111628754917005735279497666748083526841028792662819941163942406390452831624035010431659997990826669176076424857844127683305079127805593498

Розшифроване повідомлення за допомогою секретного ключа A: 8227455934535141042140333525152174500659826452337044678455581855176808598831003736497384857496959585982815780845127965586268397456021517873063015599185506095916922667713165184200826862376056807498020647381219237166620675933371573819084336775094502445732011602194692859297748187588516783061189381554558055133976808428770284950930247456277157768329112101671198117416536937476426651106830712908323770172306378725480595131493802842379458359187757054022063621072639579206077216469020762877584071537520360964965

Повідомлення з цифровим підписом: (8227455934535141042140333525152174500659826452337044678455581855176808598831003736497384857496959585982815780845127965586268397456021517873063015599185506095916922667713165184200826862376056807498020647381219237166620675933371573819084336775094502445732011602194692859297748187588516783061189381554558055133976808428770284950930247456277157768329112101671198117416536937476426651106830712908323770172306378725480595131493802842379458359187757054022063621072639579206077216469020762877584071537520360964965

Підпис підтверджено.

```
174 #check_task
175
176 pubkey_serv = (int('B147F36F358E32B82562545E92A9D82F5C86A1F02F908C93CD928BAD171647B9', 16), int('10001', 16))
177 message = 'KittyKitty'
178
179 ciphertext_serv = (int('8D0207343313143C514681B7BCA9561458FCAE5CAB04B7777555FF8353C2D95E', 16))
180
181 def Encrypt(message, pubkey):
182     # Конвертуємо повідомлення у числове представлення
183     m_int = int.from_bytes(message.encode('utf-8'), 'big')
184     # Шифруємо повідомлення використовуючи відкритий ключ
185     c_int = pow(m_int, pubkey[1], pubkey[0])
186     return c_int
187
188 ciphertext_our = Encrypt(message, pubkey_serv)
189
190 print(f" ciphertext encrypted by server: {ciphertext_serv}\nciphertext encrypted by us: {ciphertext_our}")
191
192 # Приклад виведення розшифрованого повідомлення у шістнадцятковому форматі (для сервера для розшифровки)
193 #print(hex(15276783273893125296850988844401314747835178068421855344631264836079154485))
194
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

Підпис підтверджено.

k = 3019434326298823064033093953267670902232760868798077798516461393200547548773691516576657971969127898963884113302105924557417407245963723760211588068147938194070940293695697037379225561194379476690303130694080858734648519324432617493194197308181334235642201774819920808583509360120521626831719103386821389592391063296582950671914383508811237648527069200063972983072448324750850157402524129184244995781388468445067720547797196271994660645622802346074488706096436742086370619649611992940941330745835798811371401

Підпис = 1500091579601589134875946297743715584882091113605309489892881552835972463092897745834903933366339284774522454615287767968880947345906475626097112881597005216095424259561232825523283218987502443076765589067268920821832847803206772263121574545705395115780571467134136616868417524730110681107647284082652793474163519488290613765104132100630512504447378348234380507996624355189492774737351645807462216797534001126046794393503265772334053434032004740099000426006865289860967064141262301409905706465585448

Зашифрований підпис = 430208704847314678209936747392784660448603521494648771865717219570623580712076146402941164757384041002683066574485247707138804293502887602468153426850908487475176015453416380082198435798934969213489663105571007146146935760723612678145573310110649423330746913314968257951200065351577182360825524735120047386023796880817998629241528985548180967442639455006168606224580067532663560533213816194182559773492259661397125783491427141904262010233085826418204445600064561782626940771988448108360707841876683424653

Зашифрований ключ = 256656436310748122065820696766248714028257595778654631479599563340275094648474605160525237140261433739920514573092787587832010411025966235460752172787590527663585245588351938353424337329237941451745392343785781515302867735987744210828201914638092793576179950329844688139083600848641807803551493932335738051398792766580659395477467737690575961117276790043381338497458745824501219849151817967529440070872918024688524571694265380678183312884475779560937174546961488755625151017430207127673249593715781418634

Розшифрований ключ = 113934659957940490972766928934568975240247630802172729407156799471607214555043726770831309966443693011031237446080510423293713363083080593434081093074791160550661094073717603720169643069446874840656580408431160030143500805109003910870122633416655031594444680678021013212023775880891621755329808047016549282774843909570809150632235608004930762771873101242193939378798836453983678793759695958076218351704251647742906855198551489364521225076782716051922433127189266979774838706314425173394400173681466

Розшифрований підпис = 1500091579601589134875946297743715584882091113605309489892881552835972463092897745834903933663392847745224546152877679688809473459064756260971128815970052160954242595612328255232832189875024438767558090672689208218328478032067722631215745457053951157805714671341366168684175247301106811076472844035262729347416351794882906137651041321006305125044473783482343805079966243551894927747373516458074622167975340011260467943935032657793308534340230047400990004260068652898609670641412623014099052784656585448

Підпис не підтверджено.

PS C:\Users\Support\Documents>cd .\fb-14_khashcha_lab4> python -u "c:\Users\Support\Documents>cd .\fb-14_khashcha_lab4\1..py"

ciphertext encrypted by server: 63779695063890547294201203523209522894327922914962929363536071045805448026462

ciphertext encrypted by us: 63779695063890547294201203523209522894327922914962929363536071045805448026462

PS C:\Users\Support\Documents>cd .\fb-14_khashcha_lab4> |

Ciphertext

8D0207343313143C514681B7BCA9561458FCAE5CAB04B7777555FF8353C2D9E

Decrypt

Message

KittyKitty

Message

KittyKitty

Sign

Signature

1ACFD7926878FC613A99166C69190373A008EE772BD6218EB3EC2C24B7642661

Verify

Message

KittyKitty

Text

Signature

1ACFD7926878FC613A99166C69190373A008EE772BD6218EB3EC2C24B7642661

Modulus

B147F36F350E32B82562545E92A9D82F5C86A1F02F908C93CD928BAD171647B9

Public exponent

10001

Verification

true

```
91 signed = (message, int("1ACFD7926878FC613A99166C69190373A008EE772BD6218EB3EC2C24B7642661", 16))
92
93
94 def Verify(signed, pubkey):
95     # Розбиваємо підпис на повідомлення та цифровий підпис
96     message, signature = signed
97     # Конвертуємо повідомлення у числове представлення
98     m_int = int.from_bytes(message.encode('utf-8'), 'big')
99     # Верифікуємо цифровий підпис
100    verified_signature = pow(signature, pubkey[1], pubkey[0])
101    # Якщо числове представлення повідомлення відповідає верифікованому підпису, підпис дійсний
102    return m_int == verified_signature
103
104 verified = Verify(signed, pubkey_serv)
105
106 print(verified)
107
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
S C:\Users\Support\Documents\study\fb-14_khashcha_lab4> python -u "c:\Users\Support\Documents\study\fb-14_khashcha_lab4\1.py"
iphertext encrypted by server: 63779695063890547294201203523209522894327922914962929363536071045805448026462
iphertext encrypted by us: 63779695063890547294201203523209522894327922914962929363536071045805448026462
true
S C:\Users\Support\Documents\study\fb-14_khashcha_lab4>
```

Під час лабораторної роботи ознайомився з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. Крім того, ми на практиці ознайомились з системою захисту інформації на основі криптосхеми RSA, організували з використанням цієї системи засекречений зв'язок й електронний підпис, вивчивши протокол розсилання ключів.