

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

КРИПТОГРАФІЯ

Лабораторна робота №4

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

Виконали:
Студенти 3 курсу
Снігур А.Ю. та
Носова Є. О.

Київ – 2021

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.

Порядок виконання:

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.
2. 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 $pq \leq p_1q_1$; p і q – прості числа для побудови ключів абонента А, $1 < p < q_1$ – абонента В.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , (d_1, n_1) та секретні d і d_1 .
4. 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 M і знайти криптограму для абонентів А і В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$.

Хід роботи:

Було використано функцію `inverse_of_e` для знаходження оберненого та `gcd = e * v + u * mod`. Також написано ймовірнісний тест Міллера-Рабіна (`miller_rabin`). `e_to_power` - Схема Горнера швидкого піднесення до степеня. `prime_check` - ймовірнісний тест Ферма. `generate_prime` - генерація простих чисел вказаної довжини в бітах. `generate_keys` - генерація ключів вказаної довжини в бітах. `to_decrypt` - Функція розшифрування. `to_encrypt` - Функція шифрування. `to_sign` - Функція цифрового підпису. `to_verify` - Функція перевірки цифрового підпису. `to_send` - Функція відправлення (формує повідомлення що буде відправлене). `to_receive` - Функція отримання (оброблює отримане повідомлення, розшифровуючи його та перевіряючи його піддліність)

Кандидати, які не підійшли:

invalid_keys.txt

```
1 41743221557630164802339798129965332285431130494829028613139691799293588765330523568781805677913509390911063041093834671172153763
2 43887813137637925998107510556825728979359607801200699227588635086869952453794119040554311631587412014289794137771208128932921053
3 37169286389979149101568293896736074479926818322170370338781017983088260065833165988089695701073495148270636509892004312920552257
4 36791832581132848733441340901113051874305271100387738101206051007472684339174693729480422210977033558017490184848966791328787477
5 43082842802551939933786797838551820787964757812430119445771950166188995153322891698075501699984804826464619603807846619704289386
6 4921739151661705302876374079237817374498479440374109716419708802470331264886039682652129741067185988429566255189970039077744266
7 42122893852916897565468377922505445390186369821404200696027206743166847821315145385797031682613883439708210610117649313774717175
8 45572701001274628547617789722495512364501421730117696754719867847017836588790022656542171792225293922523585981827475109282957152
9 48114924210341099052425411725776075577501127599646145010748199142983893121737994758026141728138840835640556246829299684571397736
10 45729824424673317527219385851549781311029927224315149966952472277507604267969941642915859149073666789937810041412653104139094561
11 4531299448166864131311314767091543863868296524965483397541276548410111590439777929587949186788490126782391183728047322575340166
12 500681705826211370574294804879750329329206806712033163400694390789597232897619301203516446084992144649313442457752273232984833764
13 46315119623860056022908814055852314080057537499540083280308902591463125774180677077851753591272591961310038743378502682097177796
14 3867937271586726284021924342751714934662531846140352957493084995083033658913983730325575906048894969171244727406692950905545122
15 51650206787278249731174700658192711086605410525833076719057615491327898798267214091643203898532561455502905845377757028665695821
16 37009663203534391349592875123785973686966507455488706697508035367965194915229201029817318698819244340648873258836145616750871700
17 3665413324479266720086895656584734483191548652330228091574065609738543703707060901904118579914823570354685884640922647609152410
18 48309779602001725153743650211850119617110121113780052226537686526069061026676238912314480043346111090045559177687280868638234903
19 42332797323594343192960156987049493563165991152176461816206565731665639439905896706746748257419462364124389058280804832671881382
20 4350077998275558914421914681390278257261583768060427569137928504557446126425114049592227892784841667271735255268111924049221283
21 42111048618181196295930875142329348703649063809749219321783339558656028105089851059898144152642701394022199925103207505056798926
22 42193633504079313409572982281627071187772400141967347678055429785580533350314253025668693053126714182184352834219155436849958373
23 5430421770632065233692756345426968023821664752306064451726655949366216675665465741734556341845806426665014856347466890871728683
24 5326877399919825439943883156860699237237582434345088069389788257391611675578878968505181995754299888677568671183309503628360786
25 36282894417888748671142180440062134951223349435752869142078372784686705221462358308141716944899126414063108673629093667932319440
26 55921484446396998557111792160645850147601456423220260788007115972394421527786217744716267454984964363967566444018489136013999149
27 59390467815602703412353132739184203825446939666953274710692855148685799536680367698505851967729641425097853807633916401911793422
28 57802395742097634227092501845429418105489736928843170254588583513395916616890339752900683058920719364579135992880347886983501959
29 6115362786872808980370574559397270373141166643466656671833878193843373254819005875403425492539506248088149361534559573114776504
30 5851578249026895018663407390714930269160112535322297164522489447086140574311241783518438561031366026777176770818232829620966654
```

Параметри криптосистеми RSA для абонентів А і В:

pA =

25292632601440005876166030221947800494842325759320264833674289049941180085870958322
566261647995316717553118495666392370498638774903812589393367561689154637

qA =

13899778693615818385512706137213134498699838105275193052240016412577498314010201356
301155567234491901983570705428623324605123068881716273186086019759298991

pB =

13739744107654235715504886449008199686988852901602331699979508032366768279225911418
005970213346255865096988062358853454396868848897211690814211505070821143

qB =

14892766283207785351883509611602637653527200631262014903539763807292542974280724916
990121552226741328903761995139328655101529056088931390431360038193678487

A

N =

35156199573894862296931220446351047161989878557146802234867706734026932852877621597
53528380269069964247996176269200501631931400804059657769043637529532173485943973635
50378502993385931957396665709481250731092947762958313467891579445585349533424324049
254084166298341922975463019759742794260894557425474517071267

e = 65537

d =

61480568734670341453702292984974800726851396637542075531961912641512836630732322371
99625977121902262881469120683172398676101406017261659473428617380406218751325453302
73904231152966836110936909640298543189421768443384702493085165782364559180784514729
03313702487913133485617286193324695043682477066937248568393

B

N =

20462279778637584145020386636438905713055001327286590019587232213442169672927090904
60084305290706122739043743958015333542954527770648284549650908554077214419609177624
47651294063628514864231424192520617961688071697116187667703248409554229190194705742
153634653352244725916958929077285251373653335792900823850641

e = 65537

d =

15570653105278793983736922372998584431848465999233749550281753368087660429816348374
39071124782146182171843561822882107569573558446713001060333716978070870940489750159
60074147493688183676652317819634916670040115019440890415772903639295594602436999347
48053306293042215919460672761921805738817202708911151692685

Чисельні значення ВТ та ШТ та цифровий підпис А та В:

open text Alice wants to send: 23238184

Encrypted text with Bob's public key:

34342800315877574336510295680424784242247219615855724896907947208648724646645382384
44333196853427531922078086276634173491651991092331423904830561988128044788099530930
84901389710915884822273964359244759947045689388059677689115396488604050107767910879
908439390993693506068751896160597916652139449662852307072117

The text Bob received after decryption with his private key: 23238184

ВТ , що а надсилає б 98375224

ШТ ключем В

83577507772823599894831482758475192704524428589179374473416581757512001992613510402
73741281728237038840816420702871346213904477641711121471647050907312987074121121873
62202870037892785033420024731037941902746544609976949670111071746479061230043539052
75839885224003638357599446787363540266251021763599937705385

ВТ, що отримав В 98375224

signature is:

5fb2f7f8de8ff1095fd2c0431c86d91ba9d9009fb75279adc50dc5ca13fd49b57348e2724239e8118ef6078f
75410a13ac1cb8cc2061406cfc43c033f5d3198c9e5fdb93a54458217e8fde3b85854425463daffd324c0be
2a3490cff2e2711a71d848dbf58358a5658d9e985e939aa8c5fa7341cbd982e056f239ddbfb78d295c

Signature is valid

Get server key

Key size

1024

Modulus

D340B105FED577C21F3D87B5EE0FCC4EA40F5FD71149D843191C623091403C6014ECDBA2F4EC44DCE151

Public exponent

10001

BT A 13888218

key

9fa86040d6340a944fd1afb97a22579f573dec3787c2a355ec9b5ccc354c3e583e7ac65e670bde762f40514410b40ace981e5ba4f402d9a3737ac82523b2d0c4833bb43170322dfc3b89c2c4fe232c2764546238f423438b7e962dc4fd1950d238302759045c4bf79520d06d5d1d6cd2c81d0875b12815828215a92844ce994a

signature

27168dd27bcf9805abfc096442f5a50c8f57b25c6c5df644943c1abdf7c48a3208f737965cd13cb734347167cf0b82f39fc0de511e92ef8930f4f10f4a39f7c6d7ee57c2de3364825b329ad5f1efe7d7019204d544ca46ac2ef11c5535002cd789498699e1aabb0f0424b09f9abbf533d6065fddacbab6c9e690feff6dbe23

modulus

1f4a41206f397eb83165a028dd3486750a029619659a0f14fd67d326347bb12f4b8ca5dcd8bc879f42ee4f3adff5aa10d759934f346e60244a826fb490e767b443503033fdfe1f967d131999895ceeaba4e923594f8b1c7b8e135642fd49d2aaeb0709f5ba72a29f09f817cdfd7b5cc185dccda2fbefc85e0bc2b81c390ff5a3

publicExponent 10001

Receive key

Clear

Key

568ed64feb3a5dcd9701f272b1bd31b870348a3bc7d30869216042c90d06647e243718c015fdc3560900379b6beca

Signature

3794c185a7a7127a0da3dd072483a0437ae4ce4bf95d3e955c63c515cb857f1eb9236b8406edcaa4d4330e913228t

Modulus

1aa774e29f690e8405c28c934d93d5596df17bf51903fb599a77cf9173d44d9d28b4a24f32ee3127424c0807b6ee8d

Public exponent

10001

Receive

Key

79D242

Verification

true

✓

Hexadecimal to Decimal converter

From

To

Hexadecimal

Decimal

Enter hex number

79D242

16

= Convert

× Reset

↔ Swap

Decimal number

7983682

10

Висновок:

В ході лабораторної роботи була створена тестова модель криптосистеми RSA, тести на псевдопрості числа, алгоритм Горнера для пошуку великих степенів за модулем. Протестована робота з готовим тестовим середовищем, посилання на яке надане вище. Згенеровані тестові випадки з можливою підміною повідомлення. Покращили навички програмування на мові python, ознайомились з модулем requests та удосконалили навички роботи з сервісом контролю версій.