Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №4

Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем
Варіант 4

Виконали:

Студенти 3 курсу

Загородній Я.М, Венгер П.Ю.

Перевірив:

Київ – 2024

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.

Постановка задачі:

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 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента A, 1 p і q1 – абонента B.
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 A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. 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 A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.
5. 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.

Значення обраних p, q, p1 , q1

p =
8735476654653670812586053004343769227826788946778894755919534418641044507567 7

q =
7096942854533694777490950692931487680143600629420710188496088704162576873603 7

p1 =
1098441109888057849895100663116709156148277068110543485602815877225900593180 3

q1 =
6189272965445772864091145807638515562786459537241344109442827642429382846968 9

Першій 20 кандидатів, інші наведені у файлі **numbers.csv**

1	6340889164393720093389547484835877929909183637676856098745911097512440751335 7
2	9970836809851812055295731201787556512770297162450729772687727220262647180134 1
3	1017866791730788569718888093938257394935194663993844486038192021391882222738 87
4	7813435170140375886072551885032676040569175474966318252638845167836431736780 7
5	1044241332821667931045079609213836335696530113614641592844450372992531610696 06
6	9664148082751543615465874732819539681380282618205630547260501701776544530088 5
7	9319339356299625285025593766839787219137890310841507668407126357233632674970 1
8	1026191284182219932224053679338102124412200766409473749891658569177607800327 67
9	1015180293571329392728025578329582753106727452107462814981432085701090611809 87
10	8429519171057995925015414962443671339696459534235897698930960099729181619098 8
11	8168748411863577614402362606924828484133264279304658965872320555695600573193 8
12	6181524358697084180853694308283104071207821871752755467100218361665518650765 5
13	6608527981741987573256431487413213622769192491304712233062864373415994325120 3
14	7650489021556154188649954232951506695842542569253769670397741943781110579703 4
15	6415066313496865906918793835217789379863480707321778710720927310200875987243 7
16	7025635520215928971777492772281714783346710522763735410151828076036438666380 3
17	6451722085835806280224051146146168501308784492159428148784816846891285188007 3
18	5864386688650974430290264493574145145954531183030207749548587157971270068711 3
19	6689462338365157264465422745421462012850462055273232245064844721800263128578 6
20	8458801336759349627432754515740518975498783062951439617129661542568093480699 3

Параметри криптосистеми

Відкритий ключ абонента A (e, n):

e =
209071740546228084636333331819817989103830884999480249810770882011399255416681599124822318060523966083659585980364788691781364493251104938154617804408281 3,

n =
619951786251902731877337473024863199220851097216220805351103428508452449150699240388060678240310123579836083600324882963894186102403353392885800710207204 9

Секретний ключ абонента A (d):

d =
488911208777162550234952358952283809207194196489492087750160718660324427773825085113057532785115659963665570809352364039089252070941172088899893629721573

Відкритий ключ абонента B (e1, n1):

e1 =
537801773598625789425969738667484073861887900755153175362599979846473970556511829489898310775448458428791240165975781126197425465147154958967186736165314 3

n1 =
679855186556440586630203118943133619794166366623881582679935637381783199987060988226334553773886888237835683510068020751240807310349456149096204898661926 7

Секретний ключ абонента B (d1):

d1 =
671360831864538495520915195540266879650376397968450580931163192460524843311759640734823194079201327444701344154732266368683622722606456610292781444058295

Результати роботи:

Випадкове повідомлення k:
421212992269247787140906551717106946607245667126666003761814238278710233428107844598452243242908489326360394224407144788441153531988268702526036904219153 4

Зашифроване повідомлення:
850124687929945285026952277711881845013525663610290968609733682036741279941152758588070030467049900146237976866168108794108245425347883672677966955802585

Зашифроване підписане повідомлення:
472824198432174381351844382503329602334530639546915050605192621331795526308025365475759446891930802072807723309120491533900075357210830469730252111233477

Перевірка підпису успішна

Отриманий ключ:
421212992269247787140906551717106946607245667126666003761814238278710233428107844598452243242908489326360394224407144788441153531988268702526036904219153 4

Кроки конфіденційного розсилання ключів з підтвердженням справжності:

1. Абонент A (відправник) шифрує відкрите повідомлення (k) відкритим ключем абонента B => k1.
2. Абонент A (відправник) підписує відкрите повідомлення (k) своїм приватним ключем => s.
3. Абонент A (відправник) шифрує підписане повідомлення (s) відкритим ключем абонента B => s1.
4. Абонент A (відправник) передає k1 та s1 абоненту B (отримувач).
5. Абонент B (отримувач) розшифровує k1 і отримує відкритий текст.
6. Абонент B (отримувач) розшифровує s1 і отримує підписаний текст.
7. Абонент B (отримувач) перевіряє підпис відкритим ключем абонента A (відправник).

Перевірка на зовнішніх ресурсах:

Відкритий ключ:

Encryption

Clear

Modulus: 96DE2528537D4E7493B62B6DEA0D36DA78260109DAF13AE94F99A4FDC95BEB8C3F547F40DAA235B5FC33

Public exponent: 85D323921F3DE23FAACFFB4B64CA9CA2856296F0C26ED498C04B224110F7D24C57003437AFEDCBF1DAB6

Message: 2 Bytes

Encrypt

Ciphertext: 5D23D29F0C3F9F3178327C5EA54347A67C6A9B12ACD95099237BCD23D2F954D8223B7FDD2FED9AD1A8ED

```
t = 
 4878134088213678933867295438683034659964434471896246561594220447222018947750912285520166076778902024365462306432249670130336555500458906847917038696135665
t_en = encrypt(t, private_key_A)
print(t_en)
```

[12] < 10 ms

2

Send key

Clear

Modulus: 96DE2528537D4E7493B62B6DEA0D36DA78260109DAF13AE94F99A4FDC95BEB8C3F547F40DAA235B5FC33

Public exponent: 85D323921F3DE23FAACFFB4B64CA9CA2856296F0C26ED498C04B224110F7D24C57003437AFEDCBF1DAB6

Send

Key: 33D46F604B9EC8C2DE95382BF7AF9E272A52944666D8BECF597E888E3D704DFC50F8184056315CC858DD

Signature: 9237E21AD01ABDCB35AEF882098E9F56C08B7A5E37EC53D2AE232A3FEDBFBDEFB97FC14F1FBE1696708

```
server_key = (65537, 828340328116846790627933750263107293423290548942492122589229322527379527995 67)
en_mes = 
 271454816981468056987708293566431444124476614357657236683695801457406573993292266370209266404773786896307936810739179327901850331565204334919937760748756 4
sig_mes = 
 765807343584731428515709957270292340266827800200176455174208405435129721404841022573832231669010187051412576009739336832608985016764632679860660637487346 1
receive_key(en_mes, sig_mes, private_key_A, server_key)
```

[13] < 10 ms

Перевірка підпису успішна

12727984711805633016

Висновки

Ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практично ознайомилися з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.