

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

з дисципліни

Криптографія

**З теми: « Вивчення криптосистеми RSA та алгоритму електронного підпису;
ознайомлення з методами генерації параметрів для асиметричних криптосистем»**

Варіант 18

Виконав студент групи ФБ-91

Свищо Максим Іванович

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.

Завдання:

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 A, $1 < p$ і q_1 – 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) , (e, n_1) та секретні d і d_1 .

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 і B, перевірити правильність розшифрування. Скласти для A і B 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 $0 < k < n$.

Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція `Encrypt()`, яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: `GenerateKeyPair()`, `Encrypt()`, `Decrypt()`, `Sign()`, `Verify()`, `SendKey()`, `ReceiveKey()`.

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою <http://asymcryptwebservice.appspot.com/?section=rsa>.

Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально

Хід роботи:

Кандидати на ключ, що не підійшли:

```
177086735393654972090336069577824622260159968641781427379952702616765184161395
111437288231813205550491116404080002339871950786701108697065248707336395161697
78415561994634894184861085960726813642079490363495091872027913354796871489791
210741895031491664234095441072332389307007921407229550461009699228104805681425
92657577673479944203887164962970921151278209385717995092199770589841056909247
346694896539013195576434029588218574738783284279494961558252690999500766420103
78624432672505399960790204274266054223910364678306087701387466538332442669717
287544971343889017447136205178001619263732999672357015208430556182109678886091
110933826073106049568425562278868848482708685254129819425466324155571953676607
439330125908473276812423969227583024881149545531271611080050078429843561121139
440530271540860033987608954315717430881356153621203594898764937404408789127519
259527358988444532978723934632632352355311160245891186139809963553410801645333
318577833247525412274887440071129080933865556765477262563262959603362348819725
173207394537565077001607375540446357281580704127813797198730602079094767940999
145562699169540105836910922678476623439387002277127345704062545246674332848679
217350934895099874594214639183394316085074694567988249239380357050660188543703
278166016206695902624371546583789840273934693685947706309764358987843834826429
288569754950226742884051144260889227577220192283836764687636452767266756081535
84158602824268220128248284165250791087297750190055840644816889885023180942675
172548398235401360862988506438030326484134602608503205780296141630086985572043
130591172970734842885189498248073093895332726929582885432515305083820984931085
109988272316630498671360101879892415966439273712145519058961416795898861839039
437222500345125904463532730345279504493419365763338915820122572279797665033113
275874268288536271306875986043254691756504052219889335732848997450394728235447
75902757841696850893781503786564575268203298024987385880714294798047949415805
451520848255362301141065179903290390808939997843523415525813237172224807602273
256705643102805237221886551270108496916347610716674552643315456591161842133193
322233897718390366328719137050692133966444338650404451398894179173933790557289
64104388508679383978710055679531587069198376877107670824183756370388180630613
211280708428696734160861910413235103426753209614463763513261326546603482706653
```

Абонент А:

P =

39066030369282479486940956968425103353375189682424050508724117593007881585920
1

Q =

28190498086565219484827122334157491142041907295658102118156721936825958756798
9

N =

11012908543749564927295098681445539510302827655400846964068117593073501522935
88926471719976699802485847392655675399441798540085319914150131269469510387167
89

E =

28794724804082479379767795310126883569224445670380202118809714094454721840834
36969511648605111840874790352454724126983039306033644769357925349019048992269
9

D =

39346154362508720079750405453439867159979795407436555867912636616650791353806
13327503219737908514616767873592778314847452117148136711886190927952929582569
9

Абонент В:

P =

32647250271496030923065694278067640208595728082341298407218400424764704092325
3

Q =

41245298099844199175790252134436033181050046815520648115357717879928035287555
7

N =

13465455695880732598881817299908420678672563430216930461976070859718988756726
54228373333424165879770216910332046609046797493613068547425679871630346966269
21

E =

65096832897326821394456468728698464843512796960896914820578677050181719281694
1770949105658483235385082390414133444617006595806045580677012467116826689171

D =

80421462714851702901474725204549493192156305179676581533344217060620769716117
02396998486749905040001586087470410104563983389484954006166543971751777357167
5

Відкритий текст:

30989142154015669727308245949717188504213808755944038314118553529807938597643

ШТ по ключу Б:

52211167354374419418385820097839803795289845446769523985997620110529854079217
81500935786440971210706083421243252884777122693518264318198581537606755910814
4

Підпис Б:

63580611191303342501885885998182737858873230710075636886607732210844721949155
16120334517921348929967042444806424585501731079132396106869144897357043696792
2

ШТ по ключу А:

10671018729195319575610356434622887927139243463124680004392383365147541628415
96076820251964359003287575315440708756057953435479987633447931493366444654695
36

Підпис А:

12464932612078866609704062205804818495748743483388886615783316190511314034657
54622159589847648557554981100191504591968560825136191109427441426928899586487
2

Перевірка роботи на сайті <https://www.dcode.fr/chiffre-rsa>

Найдите инструмент

ИСКАТЬ НА DCODE ПО КЛЮЧЕВЫМ СЛОВАМ:

Введите, например, "ничья"

ПРОСМОТРИТЕ ПОЛНЫЙ СПИСОК ИНСТРУМЕНТОВ

Полученные результаты

Дэшифрование с C, D, N

30989142154015669727308245949717188504213808755944038314118553529807938597643

Шифр RSA - dCode

Категория (и): Современная криптография, арифметика

Делиться

dCode и другие

dCode бесплатен, а его инструменты очень полезны в играх, математике, головоломках, тайниках и повседневных задачах! Предложение? проблема? идея? Напишите в dCode!

ШИФР RSA

Криптография · Современная криптография · Шифр RSA

РАСШИФРОВКА RSA

Укажите известные числа, остальные оставьте пустыми.

★ ЗНАЧЕНИЕ ЗАШИФРОВАННОГО СООБЩЕНИЯ (ЦЕЛОЕ ЧИСЛО) C = 106710187291953195756103564346228879271392434631241

★ ОТКРЫТЫЙ КЛЮЧ E (ОБЫЧНО E = 65537) E = 287947248040824793797677953101268835692244456703801

★ ЗНАЧЕНИЕ ОТКРЫТОГО КЛЮЧА (ЦЕЛОЕ ЧИСЛО) N = 110129085437495649272950986814455395103028276554001

★ ЗНАЧЕНИЕ ЗАКРЫТОГО КЛЮЧА (ЦЕЛОЕ ЧИСЛО) D = 393461543625087200797504054534398671599797954074361

★ МНОЖИТЕЛЬ 1 (ПРОСТОЕ ЧИСЛО) P = 390660303692824794869409569684251033533751896824241

★ МНОЖИТЕЛЬ 2 (ПРОСТОЕ ЧИСЛО) Q = 281904980865652194848271223341574911420419072956581

★ ПРОМЕЖУТОЧНОЕ ЗНАЧЕНИЕ PHI (ЦЕЛОЕ ЧИСЛО) Φ = 110129085437495649272950986814455395103028276554001

★ ОТОБРАЖАТЬ ☐ ОЧИСТИТЬ ТЕКСТ (СТРОКА СИМВОЛОВ) ☐ РАСЧЕТНЫЕ ЗНАЧЕНИЯ (C, D, E, N, P, Q, ...)

☒ ОБЫЧНЫЙ ТЕКСТ (ЦЕЛОЕ ЧИСЛО) ☐ ОЧИСТИТЬ ТЕКСТ (ШЕСТНАДЦАТЕРИЧНЫЙ)

РАССЧИТАТЬ / РАСШИФРОВАТЬ

Результат работы програми:

```
30989142154015669727308245949717188504213808755944038314118553529807938597643
Message was generated
Message was received
30989142154015669727308245949717188504213808755944038314118553529807938597643 Verified from A to B
Message was generated
Message was received
30989142154015669727308245949717188504213808755944038314118553529807938597643 Verified from B to A
```

Key =

27076536834292835781303590380329432802681705828946792144447706955751489432154

N, e =

(14622575559290140988104147538060668929186441860470507296117262975349712008790
20785569260464546923723120860096272771095555082778675051448469096126746811871
3,

11476608098021895401599626510714037481140200232640228952164437730692055826115
63440798609202544794414671195586821918158547568852900175637375696486043266667)

Message was generated

K, s =

(29686929837638623639783111494219697689317427567719155624875492592842408649665

284028097617315585467659577483819625855800369348033034181403220736566706246005743,
5978825210405189445019246495713429214579441610555569220429094418933121986709918118259954002846383244116792032226917546617347615113127656285705347679378548520)

Get server key

Clear

Key size

524

Get key

Modulus

91075D1A5C37BDCD6F6657225B26284C7C41CAB8101EFC32A6A767412B79DCA2EEC45E987FAA9BFE3B8f

Public exponent

10001

Receive key

Clear

Key

8A627025EE3B1A8FCF51ABEB3A50C18EC28EE6DD7B106FE80005EE6D93B9575F79ADB4D51A9B8569DE4f

Signature

1BDEBD0DFC1158EC5CC7A14FBEE4C2B28173B87C1DEF0ACA5359FB7534C172ECE218022DA4D5EEB6B8

Modulus

11731A915A5934E8468F50DF4BD3A8C0B2964C1F20762F25E533D63CA3DFA3FC31D247F5037F6FA178B384

Public exponent

15E9A631026BD4D5DC0B2E22CD2AD172AF3EFFAD8086B7802CD7981A980F4C19C67B6F14A85CED81F1A0

Receive

Key

3BDCC6D9A69692F89ED629F137CC739AA426CFBC72C30C415950F67D910E6A5A

Verification

true

✓