

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

Лабораторна робота No4  
з дисципліни Криптографія на тему:

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

Виконав :Єльський Іван ФБ-91

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 роботи:

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 ць  
p1q1 ; p і q – прості числа для побудови ключів абонента А, 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 А 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 А 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 А и B, перевірити правильність розшифрування. Скласти для А 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 :**

**Ті кандинати що пройшли відбір крипто системою**

**p=4429540880077795634198658644001995631132676320702670240224036104419289056559**

**q=66995302051973629214396153293087487168194982240797623777449789950098155081747**

**p1=69092879725250473477623603915575304837558176810318876972115760746934658775773**

**q1=5932159964588744632859589796823845338722068068318309026694491367015374223127**

**n,e,d for abonent A**

296758429212377017298594030822641713114600735986487235840061652754450268914412371815751178086730803753452281332836959215222677398551774527360171151528573,

114654654035202228129675883652316475816740203972734885458945461097299587023692129927497583942125607463377415861174929163819245039334167160489089318597281,

271837027004504057417243579671277375209114837756041732540679741766251487846100248017085742856654468354653949850353259732013587254236167604802100371409549

**n1,e1,d1 for abonent B**

409870014944276240743056978569781165752313251819050771041705439343471104478165220026402954265028961710816434817736114171095618122959858876999342763902171,

364475464272014554853046196740887093974681317810570779256408135796910587314065729632291867124545724401330700943585693406652522174321420971586822420152867,

179489429269562739844909125394909525085506547166839458988611501276458558923676697084472516456310197145080234572676590071042581272101482883680126193761947

**Робота програми**

**Msg:**

272371971802954464552888454867079238062960633383433867027360788537697266829758581935190711132479638384122049874036713580542688206166288183095917122439844

**Encrypt msg :**

204897127047506629961869301701371938117349686106971830197086217133817918810876209799527955868762548946107449263447824282180818855286784248395474197398430

**Decrypt msg:**

272371971802954464552888454867079238062960633383433867027360788537697266829758581935190711132479638384122049874036713580542688206166288183095917122439844

**Як можна побачити , то розшифровка пройшла успішно .**

generated a secret value k: **231984728457147448449737494358848638858250825165902255704224283927608092070275650869103867971126216228924483782964686143799678420466915617802405520968623**

**created msg k1,s1.**

21554534553027136599340705118946647581232501577720742781351050617480323928377561124432731417409701052544947541333237844430348846588344738351564332535762,

341380253979207810983989419776841516771064275785311573656883087816724629592154489627347952995115479296355035634288740867962274306859173170485780208720240,

**Recived(km,sm):**

29489808350635420401812871606843538899107817866493828240013537165146101914372694185461610253153250551049780588781449717655346965857478241145764085556426,

178638837439499440362845112000708517323450822199540101642429721826415699829132991887400421364099119156035096641501782778139191154066880266187685476279961

Изображение выглядит как текст

Автоматически созданное описание

**Робота с сайтом**

**Изображение выглядит как текст

Автоматически созданное описание**

**Изображение выглядит как текст

Автоматически созданное описание**