НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

Криптографія

Лабораторна робота №4

Підготував: Літвінчук В.С. ФБ-81
Перевірив: Чорний О.М.

Київ 2020

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 до 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 p_1, q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \le p_1 q_1$; p і q – прості числа для побудови ключів абонента A, p_1 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_1, 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 и 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 $0 < k < n$.

Хід роботи

Умовні позначення:

P, Q - прості числа
(E,N) - відкритий ключ
(D,P,Q) - приватний ключ

ABONENT A:

P= 599431867180041453314284638271754062066680308983750186593995028106809669901 09

Q =792487387569744358656034662989044684575298564547338895872903574212850487456 41

E=255049215475281620735131051473633522646221900605536194039617199263653365583 48979969601554813381081224184865350402458380651132776418977839719233469781117 49

D=156074042850551593763488555061931121562758059715045970460616950715286869539941358114426816981985147875633764270055372304102550820194823468041579631592730 9

N=475042194447565034613201993960508935985753910930096533553946740172174432920273293853601947480223040812508411849866654832548110161450084528645249770386486 9

ABONENT B:

P=100199055397358537970979418957648066963831499616726259618484283710029398477 90

Q =664491887603179015549466578511696568559552779516126511177288806133857328884 53

E=416847768513105402206885456789408067191567924265884630767887901385889602938786677214160883006615973633538171847734146721434660071297737662572668033759203

D=213563536045847054010945531607607018268165552816299341573113284043972255816413065810849994660389174175816800153510477314332855390106644792203967393022907

N=665814594570462773054624540157971405285792664190735042098594485995878843767692729036129581342870121533831817149689319676067290743020695383864696028168477 7

Зашифрування повідомлення відкритим ключем A і розшифрування повідомлення приватний ключем B.

MESSAGE=3020969709205018453143176723953798578018543578867469518525401659842698306285 7

ENCRYPTED MESSAGE WITH A PUB KEY = 325837666934971511192438205681852478874677346076033999923873258358697482881529574071315140128655562671766201798151247532233758750101859195316290904358457 4

DECRYPTED MESSAGE WITH A PRIV KEY =
30209697092050184531431767239537985780185435788674695185254016598426983062857

A підписує відкрите повідомлення, B перевіряє підпис:

MESSAGE =
30209697092050184531431767239537985780185435788674695185254016598426983062857

SIGNATURE =
35185454057925730962524182150979689906812851192753246271256812986056655173445199
69781580843787082058058715041185208986301169619843610998567148462270170015

VERIFIED: True

SendKey, ReceiveKey від A до B:

SHARED KEY =
36934010087216160322200738519437864146093161181925913282762430743487442482291

ENCRYPTED MESSAGE =
31622378441692243993260742452038453640242963781997316704437197065992886638246371
77741268187313155777108540190297218521652479158145698265522413343686576462

SIGNATURE =
31887861968926785877024562170654120188960203308746347049912391765318337636689741
47088576758282118765023585795294335496394069107691587345350421381048803609

KEY =
36934010087216160322200738519437864146093161181925913282762430743487442482291

SendKey, ReceiveKey від A до сайту:

SERVER E = 65537
SERVER N =
97408194638743503252153855057149938977156009457373466025512022910674354178941

SHARED KEY =
54867441096918995461856293111551368342034521321009610689170398833037226633243

ENCRYPTED MESSAGE =
15044228053383816777094756161259795177159167490501955725070781306435036899397
SIGNATURE =
73283378713302510983163333736765560434305849513947815629679461720580001237965

http://asymcryptwebservice.appspot.com/rsa/receiveKey?key=2142bb384790eb8ec5546abaae6b254
87a5e92dbeeef5a797d1e958d8c91e845&signature=a204ec26aa55e64838a63b8431ddd4ced85487
d549926bcaa795698ed4d20bcd&modulus=5ab3942b3415025d16f860d06578913db554527c560e86
ff4eb277dfff62226ef4ed668a870a30c3c2ff904c54716ec200b871f889aec4680ffca689ae3d8a25&pub
licExponent=30b28bc46370a4b8e5b987bcdfdfac26bd899e1faf1c59211499fd69bb5e613916add8e3e
bd9e85c3c48dd2831830c9c417ab3040df22555013922a7e8060105
{"key":"794DDF03E44796D40E6F530CB5E58D8077C5CFE9A34C8C0335AA2EF4239D681B","verified":true}

Висновок

В результаті виконання лабораторної роботи я ознайомився з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практично ознайомився з системою захисту інформації на основі криптосхеми RSA.