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

Виконали:
Студенти ФБ-01
Сотнікова П.О.
Струкало В.В.

Київ – 2022

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 p_1, q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1 q_1$; 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* 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.

---------Ключі для абонента А---------

p = 110905688587148640964539180244740580996780567156440521708985649796175934165547

q: 732267647337568362777206216369942373262009440807610451189267737662091832712219

e = 394390186515538447851371794561313512945165221524705445603980135332791631644511173621925949566769771892885960888710728624139523659617122036636371886910428 7

n = 812126476580643414773933675387715556497444669819889389202888552622164397830016478292736696810356038607282427693035152733439065362541048314559430654649179 3

d = 605769243439231523534154312333205345843872091895941662731960500008774594539990515853789585303091610200517411436022240162844504746197897559929807448707119 9

---------Ключі для абонента В---------

p1 = 107409076332632481733418240267154605919339001932537525256296703531298224822271

q1 = 105540634573358042959003671926395040098543492996728083605411385388001181046557

e1 = 515267833396369350621827520460667451967746457007640674423895505707702060615380722946430917712531951393382279038160929325342075983625042196382836014017145 1

n1 = 113360220750842848132507790984502773437136354627414046743286007987764594977606746725853814780301858842395515000574491337884368940934522758863145551014709 47

d1 = 110652886113278036017300016622322499656831307204977155717343251912543074195146952486403982324157766859859602114149454771759294840156059968881847583322170 51

Повідомлення:

546084941911332542041910104596875379375477478022535815106600325547572670412902226043178671981956316693224188764175080847806815323515672545858800887099531

Шифрування:

722571470566952926851481077459002885597074225101898912495175273294279059238520731465160646542771222955385127594747239125092256724841348628466289161737016 5

Розшифрування:

546084941911332542041910104596875379375477478022535815106600325547572670412902226043178671981956316693224188764175080847806815323515672545858800887099531

Ф-ція Ейлера:

812126476580643414773933675387715556497444669819889389202888552622164397829998065047404606262631812627094254211202854582315345205858257072203192142905 5028

Перевірка тексту: True

Перевірка ключа: True

Висновок:

У даній лабораторній роботі ми ознайомлювалися з тестами перевірки протоколу та методами генерації ключів для асиметричної криптосистеми типу RSA. Також ознайомлювалися з системою захисту інформації на основі криптосистеми RSA.