КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

Виконали: ФБ-04 Ковальчук Єгор

ФБ-04 Омелянович Олександр

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

Мета та основні завдання 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 і рекомендації щодо 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 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. 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:

Ми зробили функцію пошуку випадкового числа, використовуючи тест Міллера-Рабіна. Зробили функції для герерації двух пар ключей, функції шифрування та дешифрування, підпису та верифікації повідомлення.

Результати:

Message = 3408372540834758034

Public e = 65537

Public n =
54912145176268115686038443394129778855240989240263477989017011321444592473976
77816263712116112244667414259201814114589644537618869268184686928193355675 37

Public e1 = 65537

Public n1 =
27097695312065102560979229548779725187364925319976602554058784685691377322972
96193831896046905145383401146664110016309670842499587803228618014999878686749

Encrypted from A =
21489036711332795864235639252236472370307591860234056669456725966974412673082
78478432877069337696239922904862226777084696670311485471245895650245589 4152

Encrypted from B =
81946516344757787464877232956623935897930129942598954216970615508566346153779
37161177740454878740664835785715579101911832386722052362324658912066041970 30

Decrypted from A = 3408372540834758034

Decrypted from B = 3408372540834758034

Sign from A =
84813288065387084937179901208365030673514791855780605641278063022849243109849
95600740752973406292112940753330880844106868249348019125767148874776314163 7

Sign from B =
71344510957774383312220995069220370122855946378580256456347065675388359917791
36614093656197122292870460588124918403373038770791254126573444369122574265 52

Verify Message sign from A = True

Verify Message sign from B = True

Is key okay? - True

Висновки:

Ми ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA, ознайомилися з системою захисту інформації на основі криптосхеми RSA, вивчили протоколу розсилання ключів.