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**

Роботу виконали:  
Касаб О.Р.  
Косигін О.С.  
Групи ФБ-06

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 і довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб ; *p* і *q* – прості числа для побудови ключів абонента *А*, і – абонента *B*. q p, 1 1 , q p 1 1 q p pq  1 p 1 q

3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ та відкритий ключ . За допомогою цієї функції побудувати схеми RSA для абонентів *А* і *B* – тобто, створити та зберегти для подальшого використання відкриті ключі , та секретні і . ) ,, (qpd) ,(en) ,(ne) , ( 1 1 n e d 1 d

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 . nk   0

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:**

1. Під час виконання був обранний тест Міллера, який був рекомендований у методичці для реалізації

Також були використані функції вбудовані у пайтон функції для реалізації псевдовипадкових числе

1. значення вибраних чисел p, q, p1 , q1:  
   p: 191772136514096483425832293639303549677550378395525470432119184961129579142549  
   q: 139904671983757115225113079900297343072858493355519498589637325770155831560029  
   p1: 226033581442392560027697793424882139296899596245901831433657557892460176128157  
   q1: 148394336250698434992550284706657293624827564811621342322804467548691337471861  
   із зазначенням кандидатів, що не пройшли тест перевірки простоти у протокол ми їх не додали тому що їх багато і вони не несуть у собі смислового навантаження  
   і параметрів криптосистеми RSA для абонентів А і B  
   e\_A: 65537  
   n\_A: 26829817854628959173612149599172780717312103182079805197030616737304749193915711524654029446181117793577655069807866334810378609801114799231529630841573921  
   d\_A: 20169135545478202108829360121800591842773019629698121101699915998547279834850985229165292963848824239902225564292552547770242217931591741088630423796370577  
   e\_B: 65537  
   n\_B: 33542103288512031320019327290057528401483038300733740974362855345909554514023653290928903079328157356360375801253580830506075122755809261027098843917290177  
   d\_B: 7540409352726669781006832002752911575736600748961810973576574268142964533852708660584771301068283702585139763941037437929446637695384040888222268065116913

3 та 4 пункти, приклади роботи кода та його обробка по вимогам звіту:  
Зображення, що містить текст

Автоматично згенерований опис

Перевірка сайт у порівнянні з кодом: Зображення, що містить текст

Автоматично згенерований опис Зображення, що містить текст

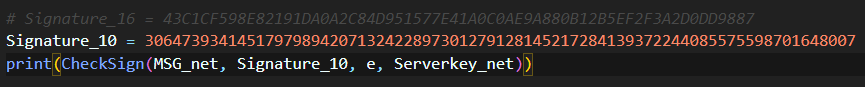
Автоматично згенерований опис Зображення, що містить текст

Автоматично згенерований опис  Зображення, що містить текст

Автоматично згенерований опис

Зображення, що містить текст

Автоматично згенерований опис Зображення, що містить текст

Автоматично згенерований опис  

Робимо висновок що код працює так само як на сайті

**Висновки:** Під час виконання лабораторної роботи нами було оброблена інформація стосовно RSA криптосистем, а також пов'язаних з ним тестами на простоту текста(наприклад тест Міллера-Рабіна), організувати зв'язок за технікою RSA та обмін даними. Ще у живу зіткнулися з методами реалізації і роботи з електронним підписом, з шифруванням - розшифруванням інформації з потенційним захистом від втручання 3-й особи у лінію зв'язку