Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Лабораторні роботи № 4

з предмету «Криптографія»

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

Виконали:

Студенти 3 курсу ФТІ

Групи ФБ-84

Асєєв В.Д

Кравченко В.В

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:

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:

Під час виконання лабораторної роботи ми стикнулись з наступними проблемами:
- Необхідність використовувати функцію pow, вбудовану у пайтон, оскільки ми при використанні звичайних операцій програма некоректно реагувала на великі числа ключів.

1. Робота виключно з локальними функціями

Примітка: числа, які було відкинуто під час тестів, додаються до файлу log.txt, де їх можна переглядати.

Таблиці значень елементів ключів для кожного з учасників (як приклад):

Aseyev		Balentin
Open Key		
n	5338219236653169344274049928011851036177069552515991021812222014233771054915690077502163848805769455068166733710807925465822787140511509103347992688560831	6474333039089595770013496998762051427750229407165609379793614252234380949070307147942277625944537672532803269740791464835379503137172934747629579685234019
e	4396155916926015439996028618965912470784677558037453060840016633205520913513728989279991828343087781531678276486339157122635959025782183747368236553327731558632709010881781968086738736724637852295008639872399542014304805421535676126978424778415718918323135480095394471032913357261998435119085359988176235741
Secret Key		
p	7344760682205174539658959201880014282041000235660111032951863304516133774731	8382661776971167039042615755779789838497941327862338521723814647509103399677 9
q	7268064226498982844715214791674910626560587720443033731429874279292341213432 1	7723481170236250667610764104980704378617266865882980527840405717758248257956 1
d	3519919513049835228117369881483715846249419578516394074196397804551162293177770768627013763629590940325393462591527279511800863454293920427646168449442374	4638992733579952931164036767883629859645673152858352869349350330525535551396892514615729075801924789761379088342587174709716068983678566559573874351852091

Приклад шифрування/дешифрування

Aseyev		Balentin
PT	93947273919	44026582591
CT	5132640010433531989127452487713063513363915762515652593803959073601667076488815597101205429102973932416109619743158907476512141829124049044205744571565763	2424028535031519631998981174380408921359801176894580657950606565010014891416229648860331597598998575957699699926443269092764549020521505607077347011949095

2. Робота з допомогою сайту

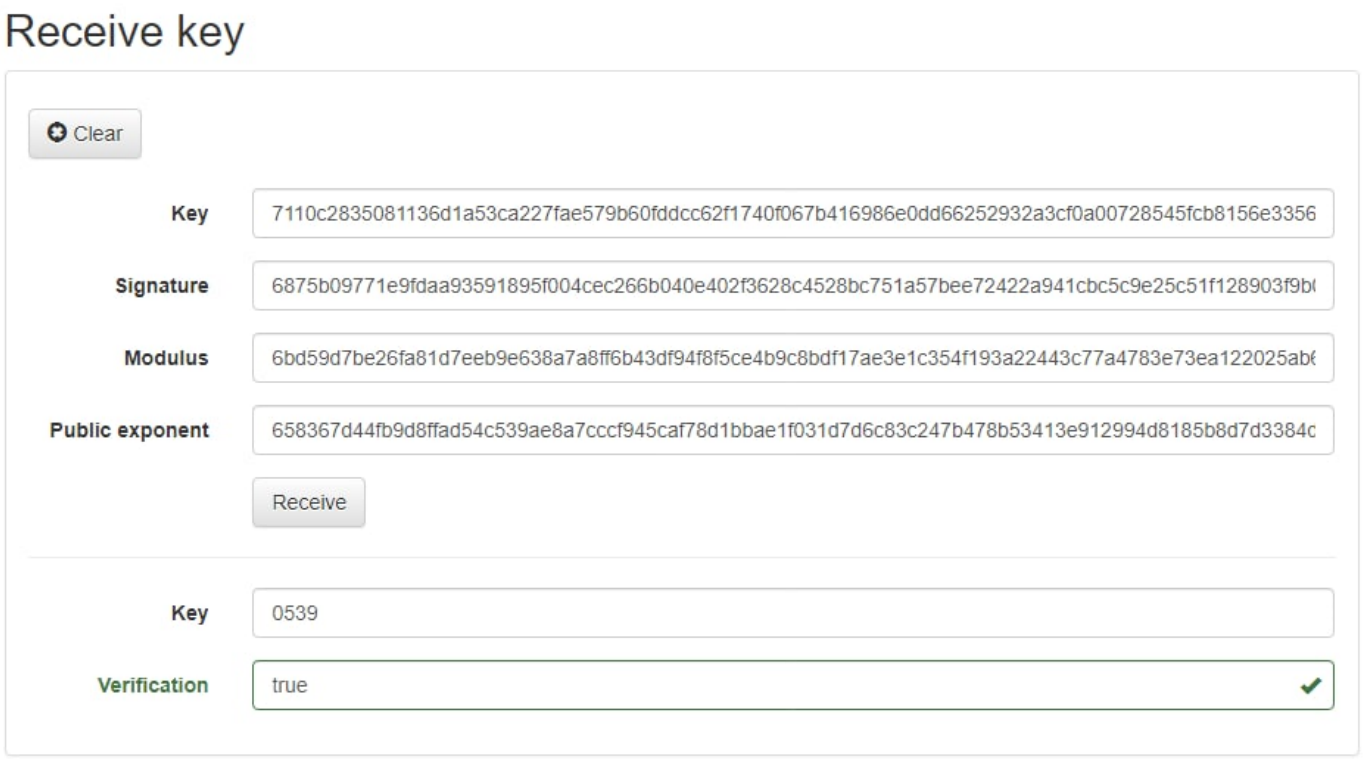
За допомогою сайту http://asymcryptwebservice.appspot.com було перевірено створені функції.

Я згенерував 512-бітний ключ на сайті та за його допомогою передав сайту таємне повідомлення

Me		Asymcryptwebservice
Open Key		
n	0x6bd59d7be26fa81d7eeb9e638a7a8ff6b43df94f8f5ce4b9c8bdf17ae3e1c354f193a22443c77a4783e73ea122025ab6662e503b89b8654f5e690559e3cc1345	0x942B79BB398C49BE8D550D99B6D7E6848777E3BD171280FDF6A2F6EC1ACB8780317741D77FB31920E258FF1D0CA5CFA9474B90261E352D42EC10CF2F2B6164F9
e	0x658367d44fb9d8ffad54c539ae8a7cccf945caf78d1bbae1f031d7d6c83c247b478b53413e912994d8185b8d7d3384d75368b6e863ea2e63434645b992550927	0x10001
Secret Key		
p	0x9d75ecdbbf9506ba18207da5bd677f55d209b0783e523838799fe6b4aa84f145	???
q	0xaf514b344f0216166803aaf56d70da9fe8aed9d2eb78b3fd5770184b5a3fba01	???

d	501422099550689629961397364634260816565842498646025566335074672113948068351031834406427242478428607414653928596162415967876815573712293170702018337941467 9	??

Sent Data	
k 1	0x7110c2835081136d1a53ca227fae579b60fddcc62f1740f067b416986e0dd66252932a3cf0a00728545fcb8156e3356a694835d778cdbea9476370ba5904bcee
s 1	0x6875b09771e9fdaa93591895f004cec266b040e402f3628c4528bc751a57bee72422a941cbc5c9e25c51f128903f9b0024875382897394c1dd78d9f3f37d371b



Висновки:

В результаті виконання лабораторної роботи ми ознайомились 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.