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:

студент гр.ФБ-01 Заріцький О.В.

студент гр.ФБ-01 Свірщук Я.Ю.

Київ – 2023

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.

Постановка задачі

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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 $p1$, $q1$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \le p1q1$; p і q – прості числа для побудови ключів абонента A, $p1$ 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), ($e1$, $n1$) 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

Кандидатів, що не пройшли перевірку на прості числа дуже багато, тому тут вставлю лише частину

```
Можливе просте число:
 651083877314814086912764464305114366136301646971973597061378058712941822735 31
_____________________________________

Можливе просте число:
 818285065292489118228168123250625860179349876182501953369042107852878064013 88
_____________________________________

Можливе просте число:
 359640009872744411112451031699954678600968058522585113653827959250555200066 2
_____________________________________

Можливе просте число:
 817259332848559855698339525178529607321378834854981558411943972292155390135 98
_____________________________________

Можливе просте число:
 495721361610930043170691371611547592173256215545805912065126424205886089495 05
_____________________________________

Можливе просте число:
 108335278008539186020971683966842744268702423381807540871868736694480251580 209
_____________________________________

Можливе просте число:
 108052342530586542276114344019985980549878476613958174294045243117386872280 589
_____________________________________

Можливе просте число:
 174763266921991401933431572633983588070003039753604187272111983857204684511 56
_____________________________________
```

```
p =  362070786157541445344388819323898438178506913058795631580093828912442424205 19
_____________________________________

q =  380506941736943948366071958393135060879853606298351286648327953865009529889 51
_____________________________________

p1 =  947867837395709351593618458549571849970569016850580457179765145836885617996 83
_____________________________________

q1 =  105784403081385925490020146930828150680668864833046312737733162521965124447559
_____________________________________

n =
137770447533097114187658385626891612987825595124810858465510574610247241344352397976258858098765408397
720277022470114539735768459816150033326262010268556 9
_____________________________________

e = e1 =  65537
_____________________________________

n1 =
100269633378949289708521760809695388815076602681887153545161333801576963696006730560987445666060498462
435796472482909211298565860632096153602692861963237 97
_____________________________________
```

p =
362070786157541445344388819323898438178506913058795631580093828912442424205 19

_____

q =
380506941736943948366071958393135060879853606298351286648327953865009529889 51

_____

p1 =
947867837395709351593618458549571849970569016850580457179765145836885617996 83

_____

q1 =
105784403081385925490020146930828150680668864833046312737733162521965124447559

_____

n =
137770447533097114187658385626891612987825595124810858465510574610247241344352397976258858098765408397720277022470114539735768459816150033326262010268556 9

_____

e = e1 = 65537

---

n1 =
10026963337894928970852176080969538881507660268188715354516133380157696369600673
05609874456660604984624357964724829092112985658606320961536026928619632379 7

Секретний ключ абонента A:
78936788453359119852092289550784748580082260355778380691516579590380760676871899
93548218170412595644158816632001550859197185554722220518748139532289884 73

Відкритий ключ абонента A:
[13777044753309711418765838562689161298782559512481085846551057461024724134435 23
97976258858098765408397720277022470114539735768459816150033326262010268556 9,
65537]

Секретний ключ абонента B:
93790211108173235847106229780977870899519750638647577500121764571223446732265462
90951229704206975285098527020201825138504407824671022840932439644782835849

Відкритий ключ абонента B:
[10026963337894928970852176080969538881507660268188715354516133380157696369600 67
30560987445666060498462435796472482909211298565860632096153602692861963237 97,
65537]

Відкритий текст:
55067251624883258327617799179594763063136699588000132336647395297415544680918975
98613441595371489628938969451556283404611429035541670133407424540605715 11

```
Зашифрований текст:
966608968122175013834732333052365506521870730781266182153418504510810967633191873500378531255666601313406771400998080662103251296913460917040252313179284 3
```

У цій лабораторній ми використовували як k значення відкритого тексту(випадкове число).

Висновок

У ході виконання лабораторної роботи, реалізували перевірку числа на простоту за тестом Міллера-Рабіна. Також реалізували криптосистему RSA з цифровим підписом. Автоматизували перевірку змістовності розшифрованого тексту.