КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

ФБ-23 Невмержицька Дар'я

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 p1 , q1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ 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:

Генеруються числа довжиною 256 біт (можна й більше), які проходять перевірку спочатку діленням на набір простих чисел, а потім тестом Міллера-Рабіна. Якщо число проходить перевірку, то воно повертається як просте. Якщо перевірка не пройдена, виводиться повідомлення, що число не є простим. Коли дві пари простих чисел згенеровано, проводиться перевірка на умову pq <=

p1q1. Якщо умова не виконується, генеруються нові пари простих чисел і процес повторюється, поки не буде отримано дві пари простих чисел, що відповідають цій умові.

```
Генерація простих чисел для абонентів A і B:
Перевірка числа: 151940301884317792207136946779355859960564874676997261608277394
942398173175917
Число не є простим числом
Перевірка числа: 168724513786536750582308152895100514792175809534132070101369513
709426279661111
Число не є простим числом
Перевірка числа: 128349067488034964202047031187843922536419804826131167708202892
946840604475536
Число не є простим числом
Перевірка числа: 174167028874516051120335258811942053994398775885892206572014405
488143880407931
Число не є простим числом
Перевірка числа: 201736659578977108877146837425695963442667492803768936109017985
384081609579139
Число не є простим числом
Перевірка числа: 146640579424224899872124846065128264100241021148079432773062725
740299261444339
Число не є простим числом
Перевірка числа: 118833143622391869049574936920072661371179305345543213391968287
106290694927428
Число не є простим числом
Перевірка числа: 133611873649222106364912845898269173332798836293659660627461004
756849504376795
Число не є простим числом
Перевірка числа: 200792265842665482548570973493580864762425945478091031966317488
142758566603107
Число не є простим числом
Перевірка числа: 137877421519276905960332222902146129548838709196522061471215160
482699177380536
Число не є простим числом
Перевірка числа: 194831886524439859329754609401878618411735411821126325442450964
392551780845662
Число не є простим числом
Перевірка числа: 171867514089329364662597695586063138805808612512564484432466168
383822881298938
Число не є простим числом
```

…

```
Перевірка числа: 188766738838312566479454871984121239153123219940218053573790537
274876488615130
Число не є простим числом
Перевірка числа: 200317540153525435883612673984137000133792928152306185212444878
443924548402333
Число не є простим числом
Перевірка числа: 119641314851820870671347193072508269641216615139684004615469934
402321147838611
Число не є простим числом
Перевірка числа: 142338123391140468610912557684752800284067949562168620445561310
087505647363970
Число не є простим числом
Перевірка числа: 163145599901279773335892116751756596668388829376800832155475793
802972442334088
Число не є простим числом
Перевірка числа: 216014983298841878954782541903230180563275242512350442033568506
690587057633496
Число не є простим числом
Перевірка числа: 145054225104002876000968997023849201558134763192408206811287976
021583179711929
Число не є простим числом
Перевірка числа: 221056727712431612221571816609595150638265872097286398295799165
683892880000010
Число не є простим числом
Перевірка числа: 225131622077157961405469875947537355329304980167560625724893810
717662493033157
Число не є простим числом
Перевірка числа: 143151425985435565184466066860506312488137533447405339212908199
052701635017420
Число не є простим числом
Перевірка числа: 149300313348984648982918699452304160241064231276161879303946528
891677613362528
Число не є простим числом
Перевірка числа: 209945637263496154202309799108344662050451855303635589176203650
410877551744397
Число є простим числом
```

```
Пара простих чисел для абонента A: p=124898071918461136529259716163211965537081560075148098784597262311314548793627, q=200249168260618488157721529364625942408768042565392485412534745048723250516451

Пара простих чисел для абонента B: p=168137005645343581799508837263428700763635564266262078693401742832496101582389, q=209945637263496154202309799108344662050451855303635589176203650410877551744397
```

Тепер на основі простих чисел генеруємо ключі для RSA. Для абонентів A та B на основі їх пар простих чисел обчислюємо значення n = p * q, φ(n) функцію Ейлера φ (n), обираємо публічний експонент e=65537 (стандартне значення), а потім обчислюємо приватний ключ d = e^(-1)modφ(n). В результаті отримуємо публічний ключ у вигляді пари (n,e) та приватний ключ у вигляді (d,p,q).

```
Генерація ключів для абонентів A і B:

Ключі абонента A: (250107350190267531075223814242893142509902943820134414395036989062962839028042058610227458423139499981345705953707571491897190207777693775647967667674577777, 65537)
Секретний ключ: (4975280413248268615633448077093241831181782319274749165308294896644409314446102092948766694923171978442443969498797181938702445126929846732873073768371173, 1248980719184611365292597161632119655370815600751480987845972623113145487936272300249168260618488157721529364625942408768042565392485412534745048723250516451)

Ключі абонента B: (3529963079778770873139957477394292546844755976960020578922772800869009666467419355676701510006682660942426774812695848004154829898869611435081757896462443 3, 65537)
Секретний ключ: (2320165549606334347488850699547378515157616437486150517382201827520842583468100882499000566504433539356362676059234148430023256504411130658798032360329977 7, 1681370056453435817995088372634287007636355642662620786934017428324961015823892, 2099456372634961542023097991083446620504518553036355891762036504108775517443 97)
```

Тепер переходимо до шифрування, розшифрування та створення і перевірки цифрового підпису. Спочатку генеруємо повідомлення, потім це повідомлення шифрується за допомогою публічного ключа. Далі повідомлення розшифровується за допомогою приватного ключа. Порівнюємо отримане розшифроване повідомлення з оригінальним для перевірки коректності. Після цього генерується цифровий підпис повідомлення, і функція Verify перевіряє його дійсність. Усі ці кроки можна побачити в коді нижче, щоб впевнитись у правильності роботи всіх функцій при взаємодії між абонентами A та B.

```
Перевірка шифрування, розшифрування та підпису для абонента A
Повідомлення: 7665053379417750082843436969247193236391463990413953460212342053474704333074923869969448427199956706899162141160181857357622757521181211060995711423494819
Зашифроване повідомлення: 2029542478573992133719771391772164369292113054416345097915148516154012819076035034687397086637315907360631747488436061317416879454303463127672110402814940
Розшифроване повідомлення: 7665053379417750082843436969247193236391463990413953460212342053474704333074923869969448427199956706899162141160181857357622757521181211060995711423494819
Повідомлення розшифровано правильно
Цифровий підпис: 3968274949176614575011240590927377214168738175298829247212636428784117900206765458314920852052620581959618674336906793820640034932444796785283552962667954
Підпис дійсний

Перевірка шифрування, розшифрування та підпису для абонента B
Повідомлення: 1484587263568176852572887584301170223955948471642998875429902248391536099427348878445240486645142885136065139662829361662871151668354676701387410604
Зашифроване повідомлення: 2657251245802503122190936992604219520300144753293260110332702500929176472512879621683031896419604246949188120835534328156991739207125210453635168643701021 0
Розшифроване повідомлення: 1484587263568176852572887584301170223955948471642998875429902248391536099427348878445240486645142885136065139662829361662871151668354676612968057038741060 4
Повідомлення розшифровано правильно
Цифровий підпис: 2217779059486154760118635923072286818685895569549704910688376622524180173447091236628446542886286354284438374850110603614280748179735782225772640881294728
Підпис дійсний
```

Тепер переходимо до роботи протоколу конфіденційного розсилання ключів із підтвердженням справжності через відкритий канал за допомогою алгоритму RSA. Спочатку генерується секретний ключ 0<k<n. Потім за допомогою функції SendKey ми отримуємо зашифрований ключ і підпис. Відправник A шифрує ключ за допомогою публічного ключа отримувача B, створює підпис своїм приватним ключем і шифрує цей підпис публічним ключем отримувача. Потім він повертає зашифрований ключ і підпис. Функція ReceiveKey розшифровує ключ та підпис, перевіряє підпис і, після успішної верифікації, повертає ключ. Отримувач B розшифровує ключ і підпис своїм приватним ключем, верифікує підпис за допомогою публічного ключа відправника і, якщо підпис дійсний, отримує ключ.

```
Перевірка протоколу розсилання ключів:
Ключ: 114900199653117887038543684151109449790017691121699775183647534635850941626648694940142222048383831736465551105723829591300299433582422245199742132851419211
Зашифрований ключ: 26122661241527630996588551921860559141694691164930856550994599496988593883168311503083556385059425934098388152029859747623121691316816413638809850798999488
Зашифрований підпис: 82435588466134604079927307065785422969548912479906055653660255013118382409044740258127071710185991726630314857238309951844843224251862079242459279694802381149001996531178870385436841511094497900176911216997751836475346358509416266486949401422220483838317364655511057238295913002994335824222451997421328514192113285141921
Ключ передано успішно
```

Перевірка правильності шифрування і розшифрування:

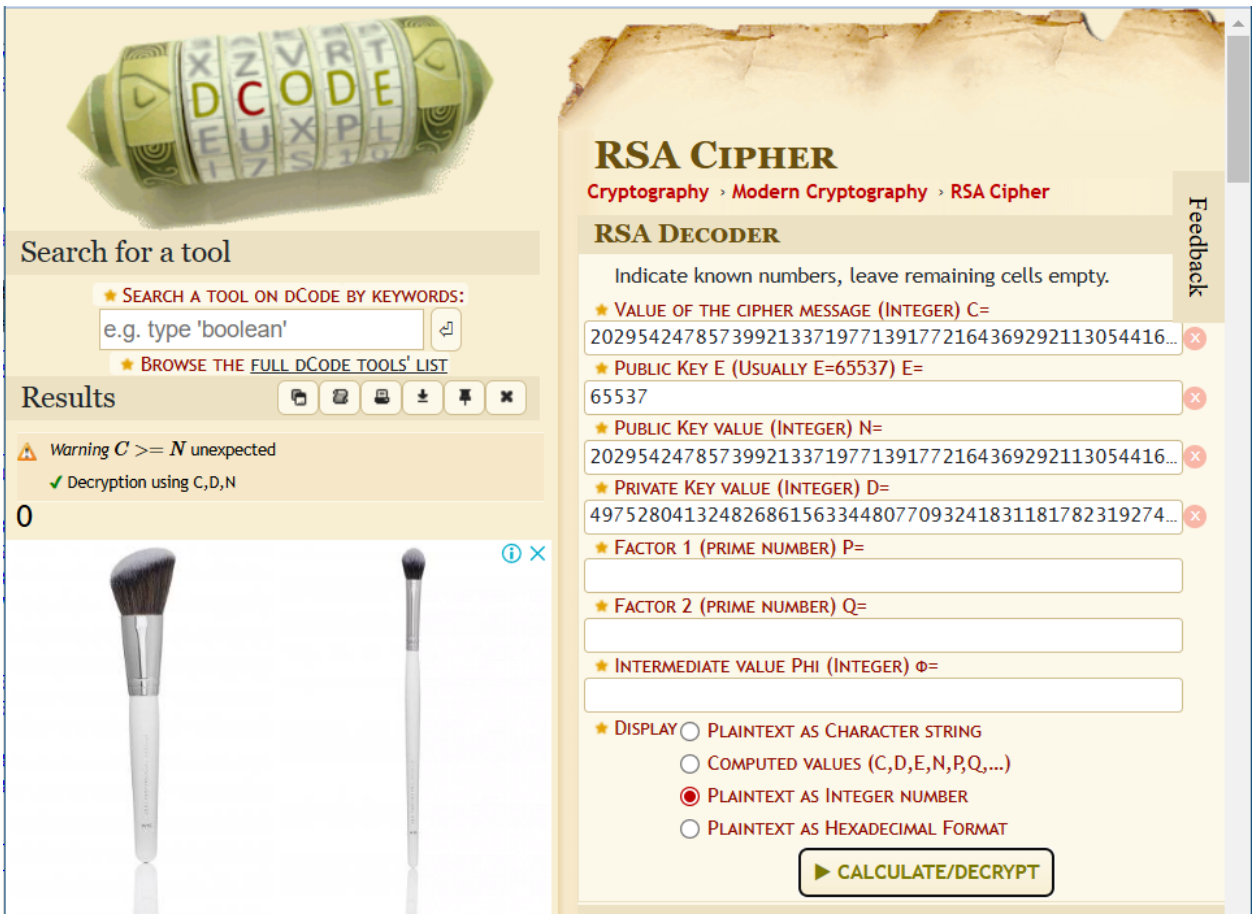
Було згенеровано такі ключі для абонентів:

```
Генерація ключів для абонентів A і B:

Ключі абонента A: (25010735019026753107522381424289314250990294382013441439503698906296283902804205861022745842313949998134570595370757149189719020777769377564796766767457777, 65537)
Секретний ключ: (49752804132482686156334480770932418311817823192747491653082948966444093144461020929487666949231719784424439694987971819387024451269298467328730737683711731485487936272000249168260618488157721529364625942408768042565392485412534745048723250516451)

Ключі абонента B: (35299630797787708731399574773942925468447559769600205789227728008690096664674193556767015100066826609424267748126958480041548298988696114350817578964624433, 65537)
Секретний ключ: (23201655496063343474888506995473785151576164374861505173822018275208425834681008824990005665044335393563626760592341484300232565044111306587980323603299777, 16813700564534358179950883726342870076363556426626207869340174283249610158238920994563726349615420230979910834466205045185530363558917620365041087755174439 7)
```

Отримано такий вивід:

```
Перевірка шифрування, розшифрування та підпису для абонента A
Повідомлення: 766505337941775008284343696924719323639146399041395346021234205347
470433307492386996944842719995670689916214116018185735762275752118121106099571142
3494819
Зашифроване повідомлення: 202954247857399213371977139177216436929211305441634509
791514851615401281907603503468739708663731590736063174748843606131741687945430346
31276721104028149 40
Розшифроване повідомлення: 766505337941775008284343696924719323639146399041395346
021234205347470433307492386996944842719995670689916214116018185735762275752118121
1106099571142349481 9
Повідомлення розшифровано правильно
Цифровий підпис: 396827494917661457501124059092737721416873817529882924721263642
878411790020676545831492085205262058195961867433690679382064003493244479678528355
2962667954
Підпис дійсний

Перевірка шифрування, розшифрування та підпису для абонента B
Повідомлення: 148458726356817685257288758430117022395594847164299887542990224839
153609942734887844524048664514288513606513966282936166287115166835467661296805703
87410604
Зашифроване повідомлення: 265725124580250312219093699260421952030014475329326011
033270250092917647251287962168303189641960424694918812083553432815699173920712521
045363516864370102 10
Розшифроване повідомлення: 148458726356817685257288758430117022395594847164299887
542990224839153609942734887844524048664514288513606513966282936166287115166835467
6766129680570387410604
Повідомлення розшифровано правильно
Цифровий підпис: 221777905948615476011863592307228681868589556954970491068837662
225241801734470912366284465428862863542844383748501106036142807481797357822257726
40881294728
Підпис дійсний
```

Введемо всі необхідні дані на сайті і перевіримо, чи все працює коректно:



Як видно, повідомлення, зашифроване абонентом А, правильно розшифровується його приватним ключем, що підтверджує правильність роботи наших функцій. Така ж перевірка виконується і для

абонента B:

Висновок: Під час виконання четвертої лабораторної роботи я отримала глибоке розуміння роботи алгоритму RSA. Ми навчилися генерувати та перевіряти прості числа за допомогою ділення на прості числа і тесту Міллера-Рабіна, а також створювати публічні та приватні ключі на основі пар простих чисел. Крім того, ми освоїли процеси шифрування, розшифрування, підпису та перевірки підпису. Наприкінці ми застосували набуті знання для реалізації протоколу конфіденційного розсилання ключів з підтвердженням справжності через відкритий канал за допомогою RSA.