Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

**Криптографія**

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №5

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

Виконали:
Студенти 3 курсу
групи ФБ-92
Сидоренко Андрій
Варгіч Дмитро

Перевірила:
Селюх П.В.

**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, $p_1$, $q_1$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1 q_1$; p і q – прості числа для побудови ключів абонента A, $p_1$, $q_1$ – 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 (e,n) . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n), ($e_1$,$n_1$) та секретні d і $d_1$ .

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

**p:**120285844595584002425090794706901296062364656381664634403954242288707557920371590946683818493031577921122094015347099647364801 17

**q:**744903943395392754928888190207583671521808884080862991402300606022669226917039952850864757935508504656864553055331685481515129 83

**p1:**421267151052349053088718060057885621799991747716180222097950315593981055996363421283605603303785664350187544806579382190047090 47

**q1:**735048993279565791692074420366968433103841043384216509534447174455554686343562902725728029534567891505198464846546441929950608 73

Непідходящі значення для p та q:

NOT APPROPRIATE:
737359204451164363999881729073725225029747456833841780210463009033350716625221663779852921249263472409178944303385479655806052 17

NOT APPROPRIATE:
413460312239074672412809398098689728282261811504162536230197436353333099642474337222031483343671511964548843113881893128215266 72

NOT APPROPRIATE:
622942629277041602318168281401393941277865165196027342766042421476462463544611827735112668788284922160825108220353313831512351 95

NOT APPROPRIATE:
277639007710374073078611285742983180531647050647034388259547603999102484244704615499230037043246110732184391876701105349867201 87

NOT APPROPRIATE:
977057053031657063077678688460325145318247030352559802704126662802621754815865636968884036604265651717080363186706815006951058 90

NOT APPROPRIATE:
218565424951230831127440360813333334324000642635409446358028945064289724155444867667681087053254603753779002617661831010188861 50

NOT APPROPRIATE:
755877895911583547473561041272210834129452035979889438952044038889535555858302487180100405941298660679082898321261140866699447528

NOT APPROPRIATE:
778915959907218600964681442195049506266572245856510710671485641115188110552718763825828166719056499159334463606958188581635695 18

NOT APPROPRIATE:
563421060463703719334862503460020516903661086467057540139856595249909633485413113248528069905776478994328917593756010019789995 66

NOT APPROPRIATE:
187363649177208846560097779596491154546036973366080747108920622343875637117796504421754696876845294167790369489968201471074245 82

NOT APPROPRIATE:
909583756890786324562700281355455766998223967931367440925511100065891169083299830769357471990567974064037977664401060567272947 93

NOT APPROPRIATE:
951896487631622600629263464357132309566620410135131378109212240499500896714911304557370980573137602791809581111645518258596391 36

NOT APPROPRIATE:
646065496577421959855322026202228318930616345112925705619367299795371752933501939675227388618425347995779437087912088755377340 82

NOT APPROPRIATE:
400627455512269139270817682800558791533867121179417577053045414506335784666952218983760469589342956839263029499119116668037422 29

NOT APPROPRIATE:
880459585914343779364832047211278751805658319382886553410213882711640555209495850018606404642936426639484671227406133597033485 83

NOT APPROPRIATE:
454664176149975568412888705514461206265740279398689111231457250193580857553115664684783384973657696781349667384664116634989236 84

NOT APPROPRIATE:
511972784901917283655676580818910768648700273577760130519197741580495492521485284736806392103788749974843670654714277463473910 48

NOT APPROPRIATE:
339278630516555175083929352203761910583064524281854360413616255778257018260459434018925127704363872460754653911074275514283447 44

NOT APPROPRIATE:
237740936330390493049521876204281816338252073983465792040640654361123833814375858916236243759532701615044008941341482896538690 45

NOT APPROPRIATE:
584836464675588306933112503808120582163186529440442454756163380010124834876260052915927955254071533499155810094801080352322411 83

NOT APPROPRIATE:
529971860793705005069186622847993848563614238041317439580048658900586393005828417331109774279466887794148223612647049201307790 92

NOT APPROPRIATE:
816947006787022315611348951994084251755779334678436977915645164845027878474673866089478353705768721321304288777316262158987730851

NOT APPROPRIATE:
767459709751860654857749535668880925063663472003002260460638965895659421828203531672970520249275475714036942354780182908651262831

NOT APPROPRIATE:
910919541576317307192284753477878303422120782130156824083387256566893201443665455815590916478896078891954212920847125605979802081

NOT APPROPRIATE:
484389228596027172956520430985618596072307541420459779569604220859142239684490172558856880898704447308114622304282673703033395451

NOT APPROPRIATE:
811648530921678315702606877694274579745772953884971731215654815952293035837778837441035814435251338987547999654348950063822571171

Параметри криптосистеми RSA для абонентів A і B:

```
Сторона A:
n = 89601399973895915267767770561356316026727391531183984242800094820715556076749026208865725201985334375820797457801927869973465634594022201819695555077802041847330629926408809027446859011
e = 65537
d = 60130295440009708247122912508338986147847741076536960968347513165233240334643009666558350255651781301759821814608730932721825642882669938378260020643593255551030114359409717405559223291
p = 120285844595584002425090794706901296062364656381664634403954242288707557920371590964736480117
q = 744903943395392754928888190207583671521808884080862991402300606022669226917039952548151512983

Сторона B:
n = 309651995282779946355180414525509412543054494660989161046821037748812200437631004002261713107740970517158877536712976119379209329011092400962931231080659217238801731764851295999418818031
e = 65537
d = 145596018045361613240381532166616911782874166546811434726304076754041960365680446769896313370758596281469442534017276329926277641204437262583182028480067520993289767041272646889487128913
p = 421267151052349053088718060057885621799991747716180222097950315593981055996363421219004709047
q = 735048993279565791692074420366968433103841043384216509534447174455554686343562902192995060873
```

Шифрування:

```
Шифрування:
A side: Original text of a sender (text to send): наутилуспомпилиус
A side: Plaintext converted to number (M): 384817812515347884506873334463387412221672
765476108424194574193345912619075847726 4
A side: Encrypted message (C): 972101475026799259171948015299877976097489286790470190
348209030699525031906563800141844216515957944377928354332443846088147664514557154477 9
520415531285783267812347382566227062541599204431367701643389362332922791423584362306 8
581918804179677022023245258364 9
```

Розшифрування:

```
Розшифрування:
B side: M gained by an addressee: 384817812515347884506873334463387412221672765476108
424194574193345912619075847726 4
B side: Decrypted message (Obtained text from a sender): наутилуспомпилиус
```

Цифровий підпис:

```
Підписання відкритого повідомлення:
M =  384817812515347884506873334463387412221672765476108424194574193345912619075847726
4
S = 777142980881896647406197606995317116845896051754928521513327979166971441420407954
705501352810818652227283741537549202970850689131748601538563569862923606113717407788 9
486677491477305030203239814396979368585078140364985533330618574129581036334762023744 2
1493
```

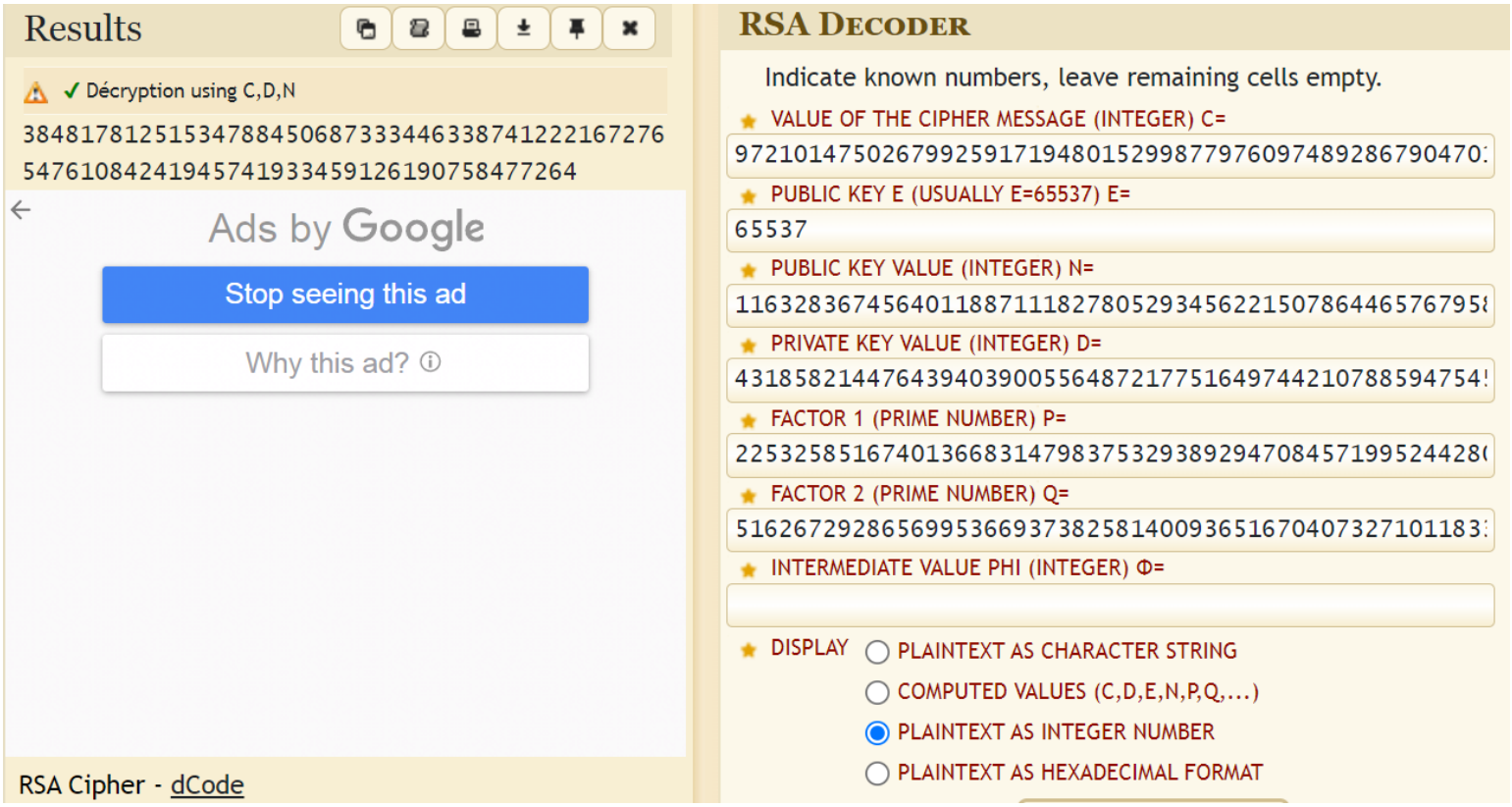
```
Перевірка підпису:
M = 384817812515347884506873334463387412221672765476108424194574193345912619075847726
4
```

Розсилання ключів по відкритих каналах зв'язку з підтвердженням справжності відправника:

```
Ключ надіслано
k = 71465701467801470 86
```

```
Перевірка відправника:
k = 71465701467801470 86
```

Перевірка на сайті:




## Висновки

Під час виконання лабораторної роботи ми ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; системою захисту інформації на основі криптосхеми RSA, організацією використання цієї системи засекреченого зв'язку й електронного підпису, протоколом розсилання ключів. Найбільші труднощі виникли при реалізації теста Міллера-Рабіна, адже слід було взяти до уваги багато чинників, завдяки яким визначається чи є число сильно псевдопростим. У ході виконання комп'ютерного практикуму було створено програму, що переводить текст російського алфавіту (без "Ъ" та "Ё") у число (M), над яким проводяться подальші операції. Протоколи роботи кожного учасника (відправника та приймаючого) реалізовані у вигляді окремих процедур.