**Національний технічний університет України “Київський політехнічний інститут”**

# КРИПТОГРАФІЯ

## КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1

**Експериментальна оцінка ентропії на символ джерела відкритого тексту**

**Варіант 5**

Виконали студенти групи ФБ - 01:

Пітель Богдан та Ширий Віталій

## 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 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq $\leq$ 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 $0 < k < n$.

**main.py** – код нашої програми.

Виконання програми у VS Code:

```
№2


Числа для абонента A:
p: 652761953741158972765682641723396387809216186200273098946435209383975545878887
q: 59656558582394019407241645134309269582015745275697925202861137827802580490683

Числа для абонента B:
p: 114874601569781278643355817071790027289992963547648524235208591950632798742903
q: 68799275883770717322575649791122412103260653882816695678613959510422684983499
```

```
№3


e:  19742105217296064114390260953909661294776742621649548565815364063725562874824932076858591171188834705640407946695378935806915654344652598160968370482198
3
n:  38941531733717425201453878715117941051668317375500028513965596537049993214083453990117638094931983210016511053128231635926062303162067856784226263081568
21
d :  14498061051409378526818854611747341026507393109191946327292044649695696494532551820740627268635863965680805792101223648768900329089811539305879836819695
59

e1:  34014902276661410248797451020700054117092659531023301555303245064485760799695023859104662240982200949462697643644697245126072261508273846506261179608855
99
n1:  79032894054376229107065391872556211991551637139636402376444797817722112785142453476931787703802892431224526014550544998262300158628315906167821424983575
97
d1:  38918755531324885514969418826683859393296637416701527886114501841877405078619525589257391926560431021744059828189668217952451433361923593178771275196908
31

Відкриті ключі [e,n] для абонента A:
e =  19742105217296064114390260953909661294776742621649548565815364063725562874824932076858591171188834705640407946695378935806915654344652598160968370482198
3
n =  38941531733717425201453878715117941051668317375500028513965596537049993214083453990117638094931983210016511053128231635926062303162067856784226263081568
21
Секретний ключ для абонента A:
d =  14498061051409378526818854611747341026507393109191946327292044649695696494532551820740627268635863965680805792101223648768900329089811539305879836819695
59
p =  65276195374115897276568264172339638780921618620027309894643520938397554587887
q =  59656558582394019407241645134309269582015745275697925202861137827802580490683

Відкриті ключі [e,n] для абонента B:
e1 =  34014902276661410248797451020700054117092659531023301555303245064485760799695023859104662240982200949462697643644697245126072261508273846506261179608855
99
n1 =  79032894054376229107065391872556211991551637139636402376444797817722112785142453476931787703802892431224526014550544998262300158628315906167821424983575
97
Секретний ключ для абонента B:
d1 =  38918755531324885514969418826683859393296637416701527886114501841877405078619525589257391926560431021744059828189668217952451433361923593178771275196908
31
p1 =  11487460156978127864335581707179002728999296354764852423520859195063279874290
3
q1 =  68799275883770717322575649791122412103260653882816695678613959510422684983499
```

```
№4


Початковий k =  9474709378132406436396498976013469476716053341756574997997879748477138022876763867229990661155513582026367365900200502323507328006889181903181368
8444261

Повідомлення:  32286674552080175491079975723784321666790350905638973834809626066126755019018966325340681486282227053753916932860367176893193462255282756134390883
49762338

Розшифрований k:  9474709378132406436396498976013469476716053341756574997997879748477138022876763867229990661155513582026367365900200502323507328006889181903181368
8444261

Ключ отримано

Шифрування:  9098206194131569078907024537246346456139832608800259621953486993257933247872184047338092369598592933051817744095660877975087703633384484852725847221
81343

Розшифрування: 32286674552080175491079975723784321666790350905638973834809626066126755019018966325340681486282227053753916932860367176893193462255282756134390883
49762338

Функція Ейлера: 38941531733717425201453878715117941051668317375500028513965596537049993214082204662578072995765145110923444564044602262287105050811092810196564261
73078252

Перевірка:  True
PS D:\lab4>
```