

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Фізико-технічний інститут

«Криптографія»

Комп'ютерний практикум №4

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

**Виконали:**

ФБ-21 Жиговець Олександр

ФБ-21 Альгішиєв Дмитро

### Варіант: 3

(В прикладах вказані значення на момент скріншотів, код писався походу і після кожного запуску значення змінюються)

- В функції `num_generator` генерується випадкове число в заданому інтервалі до тих пір, поки згенероване число не пройде тест Міллера-Рябіна.

- p = 78302540389693942474076813278372752384437637531297976548792235829579262390259  
q = 96880060186409533026208180366753145801105544418965076105975976547746881137739  
p1 = 76526143188604052757270825114355946474060600994704011527952168364951922341869  
q1 = 107119939379738677568589884199808458527975582492265400186448070546953987009831

- В функцію для генерації на вхід передається об'єкт `Pair` із значеннями `p`, `p1`, `q`, `q1`. В самій функції обчислюються потрібні значення, після чого повертається результат.

[illegible]

- В кодї є реалізовано 4 функції: Encrypt, Decrypt, Sign та Verify. Дві перші для шифрування/дешифрування, дві інші для роботи з цифровим підписом.

Зашифроване повідомлення: [848075747701943754200088474805070102013198181998664480433325160532433714705183754337404346043394093913915287519456200525347480536573562]

- Ключ  $k$  шифрується публічним ключем отримувача, потім підписується приватним ключем відправника. Ключ  $k$  дешифрується приватним ключем отримувача, після чого виконується функція *Verify*, що перевіряє підпис.

Підпис ділової: 6404368910E2A88574167B25157658917491066747742268122406779357873060810731858372498247544541461758120080813397553550682719770268936614886715856273006576752B7/

Перевірка за допомогою онлайн інструменту, було зашифровано повідомлення “Test1”, за допомогою онлайн інструменту спробували розшифрувати першу букву повідомлення, отримали T

**Search for a tool**

★ SEARCH A TOOL ON dCODE BY KEYWORDS:  
e.g. type 'caesar'

★ BROWSE THE [FULL dCODE TOOLS' LIST](#)

**Results**

✓ Decryption using C,D,N

**T**

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

Share

dCode and more

**RSA DECODER**

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C= 4116727544431457115027447458372981578807053590812...

★ PUBLIC KEY E (USUALLY E=65537) E= 65537

★ PUBLIC KEY VALUE (INTEGER) N= 9470759623333340091801309890912934756488299004509...

★ PRIVATE KEY VALUE (INTEGER) D= 8339389907126056884167264158945384117787307306593...

★ FACTOR 1 (PRIME NUMBER) P=

★ FACTOR 2 (PRIME NUMBER) Q=

★ INTERMEDIATE VALUE PHI (INTEGER) Φ=

**Search for a tool**

★ SEARCH A TOOL ON dCODE BY KEYWORDS:  
e.g. type 'caesar'

★ BROWSE THE [FULL dCODE TOOLS' LIST](#)

**Results**

✓ Decryption using C,D,N

**1**

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!  
A suggestion ? a feedback ? a bug ? an idea ? [Write to dCode!](#)

**RSA DECODER**

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C= 1308086884074906952327086886810334619412241270353...

★ PUBLIC KEY E (USUALLY E=65537) E= 65537

★ PUBLIC KEY VALUE (INTEGER) N= 9470759623333340091801309890912934756488299004509...

★ PRIVATE KEY VALUE (INTEGER) D= 8339389907126056884167264158945384117787307306593...

★ FACTOR 1 (PRIME NUMBER) P=

★ FACTOR 2 (PRIME NUMBER) Q=

★ INTERMEDIATE VALUE PHI (INTEGER) Φ=

★ DISPLAY ☒ PLAINTEXT AS CHARACTER STRING  
☐ COMPUTED VALUES (C,D,E,N,P,Q,...)  
☐ PLAINTEXT AS INTEGER NUMBER  
☐ PLAINTEXT AS HEXADECIMAL FORMAT

**CALCULATE/DECRYPT**

І останній символ повідомлення – отримали 1, як і початковому повідомленні

## **Висновки**

Під час виконання завдань у цій роботі ми навчились перевіряти числа на простоту за допомогою тесту Міллера-Рябіна. Попрацювали із криптосистемою RSA, навчились шифрувати, дешифрувати та перевіряти підпис.