НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра прикладної математики

Звіт

з лабораторної роботи № 4

із дисципліни «Криптографічні методи захисту інформації»

на тему

*Шифрування з відкритим ключем на основі алгоритму RSA*

|  |  |
| --- | --- |
| Виконав: | Керівник: |
| студент групи КМ-ХХ | *ст. викладач Бай Ю. П.* |
| *Іваненко І. І.* |  |

Київ — 20\_\_

ЗМІСТ

[Постановка задачі 2](#_Toc102990368)

[Основні теоретичні відомості з асиметричних криптосистем 3](#_Toc102990369)

[Математичне підґрунтя алгоритму RSA 3](#_Toc102990370)

[Опис алгоритму RSA 3](#_Toc102990371)

[Контрольний приклад 1 4](#_Toc102990372)

[Шифрування і розшифрування за алгоритмом RSA 5](#_Toc102990373)

[Контрольні питання 6](#_Toc102990374)

[Список літератури 7](#_Toc102990375)

[Додаток 1 8](#_Toc102990376)

[Додаток 2 9](#_Toc102990377)

***Мета роботи:*** розробити асиметричну криптосистему на основі алгоритму шифрування RSA.

# Постановка задачі

1. Скласти програму, яка дозволяє виконувати шифрування та розшифрування за алгоритмом RSA. Перевірити роботу програми на контрольних прикладах. Навести скріншоти детального покрокового виконання алгоритму.

1. *Контрольний приклад 1* ([RSA-encryption](https://brilliant.org/wiki/rsa-encryption/))

*p* = 11, *q* = 17, *e* = 3

*public key* {*e, n*}= {3*,* 187}

*private key* {*d, n*}= {107*,* 187}

*M* = 72

*C* = 183

*M’* = 72, *text* = *chr (72)* = {H}

*Контрольний приклад 2* ([RSA uk.wiki](https://uk.wikipedia.org/wiki/RSA))

*p* = 3557, *q* = 2579, *e* = 3

*public key* {*e, n*}= {3*,* 9173503}

*private key* {*d, n*}= {6111579*,* 9173503}

*M* = 1111111

*C* = 4051753

*M’* = 1111111

2. Виконати дії ОДЕРЖУВАЧА і розшифрувати задане повідомлення, користуючись алгоритмом RSA. Необхідні результати занести до [Таблиця RSA](https://docs.google.com/spreadsheets/d/1IeqT1byTw2PgTOQXvXaozfia_Dh4pSM5RaWOLqZCtEM/edit?usp=sharing).

УВАГА! Числа ***n*** в стовпчику *D* мають бути унікальними.

# Основні теоретичні відомості з асиметричних криптосистем

……

# Математичне підґрунтя алгоритму RSA

……

# Опис алгоритму RSA

# Контрольний приклад 1

[RSA-encryption](https://brilliant.org/wiki/rsa-encryption/)

Виконати приклад. Додати скріншот, що містить усі проміжні результати.

# Шифрування і розшифрування за алгоритмом RSA

*Таблиця 1.*

|  |  |  |
| --- | --- | --- |
| Крок | Опис кроку | Результат |
| 1 | Обрати два довільних простих числа *p* і *q*  *p ≠ q*; 1 < *p, q* < 200 |  |
| 2 | Обчислити добуток *n = p* ∙ *q.* Увага! ***n >* 90 та має бути унікальним** в стовпчику *D* в [Таблиця RSA](https://docs.google.com/spreadsheets/d/1IeqT1byTw2PgTOQXvXaozfia_Dh4pSM5RaWOLqZCtEM/edit?usp=sharing) |  |
| 3 | Обчислити функцію Ейлера *φ*(*n*) *=* (*p – 1*) ∙ (*q – 1*) |  |
| 4 | Обрати відкриту експоненту *e* : *1 < e < φ(n),  e –* взаємно просте з *φ(n)* |  |
| 5 | Обчислити секретну експоненту *d* таку, що *(e∙d) mod φ(n) = 1* |  |
| 6 | Зберегти закритий ключ {*d*, *n*} |  |
| 7 | Опублікувати відкритий ключ {*е*, *n*} |  |
| 8 | Одержати від відправника / викладача зашифроване повідомлення *C*. *Дії відправника:*  1) обрати текст для шифрування *M;* 2) символи тексту замінити цілими числами *mi* згідно з таблицею ASCII; 3) виконати шифрування за формулою ***ci = (mi)e mod n*** *.* |  |
| 9 | Розшифрувати задане повідомлення *C:*  1) обчислити ***mi = (ci)d mod n***; 2) поставити у відповідність знайденим цілим числам *mi* літери англійського алфавіту, записати одержане слово |  |

*В процесі шифрування використовується наступне перетворення літер англійської абетки в коди ASCII: ord(‘A’) = 65, chr(65) = ‘A’* .

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | B | C | D | … | Z |
| 🡫 | 🡫 | 🡫 | 🡫 |  |  |
| 65 | 66 | 67 | 68 | … | 90 |

# Контрольні питання

1. В чому полягає принципова відмінність асиметричних криптосистем від симетричних?
2. Що таке одностороння (однонаправлена) функція з секретом? Наведіть приклади односторонніх функцій.
3. Складність якої математичної задачі полягає в основі алгоритму RSA?
4. Як визначається і обчислюється функція Ейлера?
5. Як пов’язані між собою відкритий і закритий ключі в алгоритмі RSA?

# Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.
3. Гулак Г*.*М*.* Основи криптографічного захисту інформації: підручник / Г*.*М*.* Гулак*,* В*.*А*.* Мухачов*,* В.О. Хорошко, Ю.Є. Яремчук / – Вінниця: ВНТУ, 2011. – 199 с.
4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.
5. Саймон Сингх. Книга шифров. Пер. с англ. А. Галыгина. — М.: АСТ: Астрель, 2007. — 448 с.

# Додаток 1

Текст програми, що реалізує шифрування/розшифрування  
 за алгоритмом RSA

# Додаток 2

Скріншоти виконання кроків 1-9 *Таблиці 1.*