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:
студент групи КМ-ХХ
Іваненко І. І.

Керівник:
ст. викладач Бай Ю. П.

Київ — 20__

ЗМІСТ

Постановка задачі 2
Основні теоретичні відомості з асиметричних криптосистем 3
Математичне підґрунтя алгоритму RSA 3
Опис алгоритму RSA 3
Контрольний приклад 1 4
Шифрування і розшифрування за алгоритмом RSA 5
Контрольні питання 6
Список літератури 7
Додаток 1 8
Додаток 2 9

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)

   $p = 11, \quad q = 17, \quad e = 3$

   public key $\{e, n\} = \{3, 187\}$

   private key $\{d, n\} = \{107, 187\}$

   $M = 72$

   $C = 183$

   $M' = 72, \quad text = chr\ (72) = \{H\}$

   Контрольний приклад 2 (RSA uk.wiki)

   $p = 3557, \quad q = 2579, \quad e = 3$

   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.

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

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 $p \neq q$; $1 < p, q < 200$	
2	Обчислити добуток $n = p \cdot q$. Увага! **$n > 90$ та має бути унікальним** в стовпчику D в Таблиця RSA	
3	Обчислити функцію Ейлера $\varphi(n) = (p - 1) \cdot (q - 1)$	
4	Обрати відкриту експоненту e : $1 < e < \varphi(n)$, e – взаємно просте з $\varphi(n)$	
5	Обчислити секретну експоненту d таку, що $(e \cdot d) \bmod \varphi(n) = 1$	
6	Зберегти закритий ключ $\{d, n\}$	
7	Опублікувати відкритий ключ $\{e, n\}$	
8	Одержати від відправника / викладача зашифроване повідомлення C. *Дії відправника:* 1) обрати текст для шифрування M; 2) символи тексту замінити цілими числами m_i згідно з таблицею ASCII; 3) виконати шифрування за формулою $\boldsymbol{c_i = (m_i)^e \bmod n}$.	
9	Розшифрувати задане повідомлення C: 1) обчислити $\boldsymbol{m_i = (c_i)^d \bmod n}$; 2) поставити у відповідність знайденим цілим числам m_i 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.*