

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Методичні вказівки
до виконання лабораторних робіт з дисципліни
"Сучасні стандарти інформаційної безпеки"
для студентів магістратури напрямку підготовки
121 „Інженерія програмного забезпечення”
за освітньою програмою
„Інженерія програмного забезпечення ”
усіх форм навчання

Методичні вказівки до виконання лабораторних робіт з дисципліни "Сучасні стандарти інформаційної безпеки" для студентів магістратури напряму підготовки 121 „Інженерія програмного забезпечення” за освітньою програмою „Інженерія програмного забезпечення” усіх форм навчання / Укл. Неласа Г.В., Г.Л. Козіна – Запоріжжя: ЗНТУ, 2016. – 52 с.

Укладачі: Г.В. Неласа, к.т.н., доцент
Г.Л. Козіна, доцент каф. захисту інформації, к.ф.-м.н.

Рецензент: Л.М. Карпуков, д.т.н., професор

Відповідальний
за випуск: Г.В. Неласа, к.т.н., доцент

Затверджено:
на засіданні кафедри
програмних засобів

протокол № 1
від 16.08.2016

ЗМІСТ

Лабораторна робота № 1 Базові шифри. Частотний крипто аналіз....	5
1.1 Теоретичні відомості.....	5
1.1.1 Шифр простої заміни.....	5
1.1.2 Квадрат Полібія.....	5
1.1.3 Шифр перестановки.....	6
1.1.4 Шифр Тритемія.....	7
1.1.5 Частотний крипто аналіз.....	8
1.2 Завдання на лабораторну роботу.....	9
1.3 Зміст звіту.....	10
1.4 Контрольні питання.....	10
 Лабораторна робота № 2 Режими шифрування блокових шифрів.....	11
2.1 Теоретичні відомості.....	11
2.1.1 Опис алгоритму шифрування RIJNDAEL.....	11
2.1.2 Режими шифрування.....	14
2.2 Завдання на лабораторну роботу.....	21
2.3 Зміст звіту.....	21
2.4 Контрольні питання.....	21
 Лабораторна робота № 3 Криптографія з відкритим ключем. Функція хешування.....	23
3.1 Теоретичні відомості.....	23
3.1.1 Асиметричні криптосистеми.....	23
3.1.2 Алгоритм RSA в схемі спрямованого шифрування.....	24
3.1.3 Цифровий підпис Эль-Гамала.....	25
3.2 Завдання на лабораторну роботу.....	26
3.3 Зміст звіту.....	27
3.4 Контрольні питання.....	28

Лабораторна робота № 4 Криптографічні перетворення на еліптичних кривих.....	29
4.1 Теоретичні відомості.....	29
4.1.1 Еліптичні криві над простим полем Галуа $GF(p)$	30
4.1.2 Алгоритм обчислення точок еліптичної кривої.....	33
4.1.3 Приклад додавання точок еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$	33
4.1.4 Алгоритм обчислення порядку точки еліптичної кривої.....	34
4.1.5 Алгоритм скалярного множення на еліптичній кривій.....	37
4.2 Завдання на лабораторну роботу.....	38
4.3 Зміст звіту.....	39
4.4 Контрольні питання.....	39
Лабораторна робота № 5 Стеганографічний захист.....	40
5.1 Теоретичні відомості.....	40
5.1.1 Стеганографічна система.....	41
5.1.2 LSB-метод (Least Significant Bits) приховування інформації.....	42
5.1.3 Формат BMP-файлу.....	43
5.2 Завдання на лабораторну роботу.....	45
5.3 Зміст звіту.....	45
5.4 Контрольні питання.....	45
6. Питання для самостійної роботи.....	46
Література.....	47
Додаток А Таблиця простих чисел.....	48
Додаток Б Підключення криптографічної бібліотеки Miracl.....	49

ЛАБОРАТОРНА РОБОТА № 1

БАЗОВІ ШИФРИ. ЧАСТОТНИЙ КРИПТОАНАЛІЗ

Мета роботи: ознайомитися з базовими шифрами. Розглянути методику частотного криптоаналізу.

Використовуване програмне забезпечення: середа розробки Microsoft Visual C++.

1.1 Теоретичні відомості

В криптографії здавна використовувались два види шифрів: заміна та перестановка. Історичним прикладом шифру заміни є шифр Цезаря. Його сутність така: в строку виписується алфавіт, після чого під ним виписується той же алфавіт з циклічним зсувом на 3 букви вліво.

**АБВГДЕЇЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЪЬЄЮЯ
ГДЕЇЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЪЬЄЮЯАБВ**

При зашифруванні буква відкритого тексту замінюється на букву, що знаходиться під нею в нижній строчці. Наприклад: РИМ – УЛП. Ключем в шифрі Цезаря є величина здвигу нижньої строки.

1.1.1 Шифр простої заміни

Подальший розвиток шифру Цезаря є очевидним: нижня строчка може бути записана з випадковим порядком букв. Такий шифр носить назву шифру простої заміни. Ключем такого шифру є порядок розташування букв в нижній строчці, так звана «таблиця заміни». Якщо в шифрі Цезаря існує тільки 33 варіанта ключів, то в шифрі простої заміни їх вже 33! (33 факторіал).

1.1.2 Квадрат Полібія

Одна з відомих модифікацій шифру простої заміни – квадрат Полібія. Візьмемо алфавіт з 32 букв. Виберемо ключ – будь-яке слово, в якому немає однакових букв. Запишемо його в перші клітинки квадрата розміром, наприклад, 4×8. В останні клітинки запишемо

алфавіт за винятком тих букв, що зустрічаються в ключі. Для зашифрування букви повідомлення замінюються на букви, що стоять *під* ними в квадраті Полібія. Наприклад:

Ключ – **«МОСКВА»**.

Повідомлення – **«НЕЛЬЗЯ ПОМОЧЬ ТОМУ, КТО НЕ ЖЕЛАЕТ СЛУШАТЬ СОВЕТОВ»**.

На рис. 1.1 представлено Квадрат Полібія для ключа **«МОСКВА»**.

М	О	С	К
В	А	Б	Г
Д	Е	Ж	З
И	Й	Л	Н
П	Р	Т	У
Ф	Х	Ц	Ч
Ш	Щ	Ы	Ъ
Ь	Э	Ю	Я

Рисунок 1.1 – Квадрат Полібія

Зашифроване повідомлення:

«УЙТМНКФАВАЪМЦАВЧГЦАУЙЛЙТЕЙЦБТЧЬЕЦМБАДЙЦАД».

Для розшифрування букви шифротексту замінюються на ті букви, що стоять *над* ними в квадраті Полібія.

1.1.3 Шифр перестановки

Оберемо ціле додатне число, наприклад, 5. Створимо випадкову підстановку:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Зашифруємо фразу:

«БАЖАЄШ БАГАТО ЗНАТИ, ТРЕБА МЕНШЕ СПАТИ».

Для цього доповнимо фразу до довжини кратної 5 випадковими символами та розіб'ємо на групи по 5 букв.

БАЖАЄ ШБАГА ТОЗНА ТИТРЕ БАМЕН ШЕСПА ТИВСЕ

Букви кожної групи переставимо згідно обраної підстановки. Отриманий текст запишемо без пропусків.

«ААБЄЖГЫШААНОТАЗРИТЕТЕАБНМПЕШАССИТЕВ»

При розшифруванні текст розбивається на групи по 5 букв і букви переставляються в зворотному порядку. Ключом шифру є степінь підстановки (тут 5) і порядок розташування чисел в нижньому рядку підстановки.

1.1.4 Шифр Тритемія

В XV столітті абат Тритемій (Германія) запропонував шифр на основі “таблиці Тритемія”. Для російського алфавіту вона має наступний вигляд:

А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А
В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В
Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г
Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д
Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Э	Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь
Ю	Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э
Я	А	Б	В	Г	Д	Е	Є	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ь	Э	Ю

Рисунок 1.2 – Таблица Тритемія для російського алфавіту

Тут перша строчка є одночасно і строчкою букв відкритого тексту. Перша буква тексту шифрується по першій строчці, друга – по другій і т.д. Після останньої строчки знову повертаємось до першої. Наприклад, слово **“КРИПТОГРАФИЯ”** зміниться на **“КСКТЦУИЧЗЭТЙ”**. Однак, в такому варіанті, в шифрі Тритемія був відсутній ключ. В подальшому удосконалення шифру пішли по двом шляхам:

- введення випадкового порядку розташування букв алфавіту;
- застосування більш складного порядку вибору строк таблиці при шифруванні (по ключу).

1.1.5 Частотний крипто аналіз

Частотний криптоаналіз базується на застосуванні статистики для аналізу текстової інформації. Текст складається із слів, слова із літер. Кількість літер в кожній мові обмежена. Важливими характеристиками тексту є повторюваність літер, пар літер (біграм) і, взагалі, m-грам, поєднання літер друг с другом, чередування голосних і приголосних і т.д. Всі ці характеристики є достатньо стійкими і можуть бути використані для аналізу шифртекстів. В табл. 1.1 та 1.2 приведені однобуквені ймовірності англійської та російської мов.

Таблиця 1.1 - Однобуквені ймовірності англійської мови

Літера	Ймовірність	Літера	Ймовірність
A	0.0856	N	0.0707
B	0.0139	O	0.0797
C	0.0279	P	0.0199
D	0.0378	Q	0.0012
E	0.1304	R	0.0677
F	0.0289	S	0.0607
G	0.0199	T	0.1045
H	0.0528	U	0.0249
I	0.0627	V	0.0092
J	0.0013	W	0.0149
K	0.0042	X	0.0017
L	0.0339	Y	0.0199
M	0.0249	Z	0.0008

Таблиця 1.2 - Однобуквені ймовірності російської мови

Літера	Ймовірність	Літера	Ймовірність	Літера	Ймовірність
А	0,062	К	0,028	Ф	0,002
Б	0,014	Л	0,035	Х	0,009
В	0,038	М	0,026	Ц	0,004
Г	0,013	Н	0,053	Ч	0,012
Д	0,025	О	0,090	Ш	0,006
Е	0,072	П	0,023	Щ	0,003
Ж	0,007	Р	0,040	Ы	0,016
З	0,016	С	0,045	Ь,Ъ	0,014
И	0,062	Т	0,053	Э	0,003
Й	0,010	У	0,021	Ю	0,006
				Я	0,018

Процес криптоанализу можна представити наступним чином. Криптоаналітик підраховує частоти букв в шифротексті. Далі він бере в шифротексті символ, що зустрічається найбільш часто, и припускає, що це пробіл. Потім бере наступний символ, що зустрічається найбільш часто, и припускає, що це Е (для англійської мови), и т.д. Шляхом проб і помилок такий метод може привести до рішення задачі. Крім того, при підставленні букв замість символів аналізованого шифротексту криптоаналітик враховує частоти появи сполучень із двох букв (діаграм), трьох букв (триграмм) і т.д.

1.2 Завдання на лабораторну роботу

1.2.1 Розробити програми шифрування та розшифрування наступними шифрами:

- шифр простої заміни;
- квадрат Полібія;
- шифр перестановки;
- шифр Тритемія з вибором строк по ключу;

1.2.2 Виконати частотний криптоаналіз отриманих зашифрованих текстів.

1.3 Зміст звіту

- 1.3.1 Титульний лист, тема і мета роботи.
- 1.3.2 Відповіді на контрольні питання.
- 1.3.3 Тексти програм.
- 1.3.4 Обране повідомлення для шифрування.
- 1.3.5 Обраний ключ.
- 1.3.6 Зашифроване повідомлення.
- 1.3.7 Розшифроване повідомлення.
- 1.3.8 Результати проведення частотного криптоаналізу.

1.4 Контрольні питання

- 1.4.1 Опишіть шифр Полібія.
- 1.4.2 Опишіть шифр простої заміни.
- 1.4.3 Опишіть шифр Тритемія.
- 1.4.4 Опишіть шифр перестановки.
- 1.4.5 Чи є шифр Полібія шифром простої заміни?
- 1.4.6 Як залежить стійкість шифру від довжини ключа?
- 1.4.7 Опишіть метод частотного криптоаналізу.
- 1.4.8 В яких випадках можна застосовувати метод частотного криптоаналізу?

ЛАБОРАТОРНА РОБОТА № 2

РЕЖИМИ ШИФРУВАННЯ БЛОКОВИХ ШИФРІВ

Мета роботи: ознайомитися з програмною реалізацією алгоритму симетричного блокового шифрування RIJNDAEL. Розробити програми його використання у різних режимах шифрування.

Використовуване програмне забезпечення: середа розробки Microsoft Visual C++. Криптографічна бібліотека Miracl.

2.1 Теоретичні відомості

2.1.1 Опис алгоритму шифрування RIJNDAEL

На цей час в Україні, як і в Росії діє міждержавний стандарт симетричного шифрування ГОСТ 28147-89. В 1997 році національний інститут стандартів і технологій США (NIST) об'явив про початок програми по прийняттю нового стандарту криптографічного захисту для закриття важливої інформації урядового рівня. Фіналістом конкурсу став RIJNDAEL, AES (Advanced Encryption Standart) Федеральний стандарт шифрування США затверджений міністерством торгівлі США як стандарт 4 грудня 2001 року. Місце розробки 1997 рік, Бельгія. Автори Йоан Дамен (Joan Daemen) Винсент Раймен (Vincent Rijnmen).

Алгоритм симетричного блокового шифрування RIJNDAEL становить особливий інтерес як новий американський стандарт криптографічного захисту – стандарт XXI в. для закриття важливої інформації урядового рівня, що прийшов на заміну існуючому з 1974р. алгоритму DES, найпоширенішому криптоалгоритму у світі. В алгоритмі RIJNDAEL не виявлено слабостей у захисті.

Його відрізняють:

- висока ефективність на будь-яких платформах;
- високий рівень захищеності;
- шифр добре підходить для реалізації в smart-картах через низькі вимоги до пам'яті;
- швидка процедура формування ключа;
- гарна підтримка паралелізму на рівні інструкцій;
- підтримка різних довжин ключа з кроком у 32 біта.

Параметри шифру RIJNDAEL наведені в табл. 2.1.

Таблиця 2.1 – Параметри шифру RIJNDAEL

розмір блока, біт	128, 192, 256
розмір ключа, біт	128, 192, 256
число раундів	10, 12, 14
розмір ключового елемента, біт	128, 192, 256 (дорівнює розміру блока)
число ключових елементів	11, 13, 15 (на 1 більше числа раундів)

Кількість раундів шифрування залежить від розмірів ключа та блока.

Таблиця 2.2 – Кількість раундів шифрування

Розмір ключа	128	192	256
Розмір блока			
128	10	12	14
192	12	12	14
256	14	14	14

Один раунд шифрування на псевдокодi виглядає наступним чином:

```
Round (State, RoundKey)
{
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State, RoundKey);
}
```

Останній раунд шифрування на псевдокодi виглядає так:

```
Round (State, RoundKey)
{
ByteSub(State);
ShiftRow(State);
AddRoundKey(State, RoundKey);
}
```

У цьому криптоалгоритмі деякі операції виконуються над байтами, що розглядаються як елементи поля $GF(2^8)$. Елементами $GF(2^8)$ є двійкові багаточлени степені $N < 8$, що можуть бути задані рядком своїх коефіцієнтів. При такому представленні елементів поля додавання в полі $GF(2^8)$ – це операція поразрядного XOR, а множення – це звичайна операція множення багаточленів з узяттям результату по модулю деякого незвідного двійкового багаточлена $\phi(x)$, з використанням операції XOR при приведенні подібних членів. У RIJNDAEL обраний незвідний поліном $\phi(x) = x^8 + x^4 + x^3 + x + 1$ показника 51.

Блок даних представляється у вигляді масиву значень.

Таблиця 2.3 – Представлення блоків даних

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

У процедурі ByteSub a_{ij} змінюється на a_{ij}^{-1} в полі Галуа $GF(2^8)$.

$$a_{ij} * a_{ij}^{-1} = 1 \pmod{(x^8 + x^4 + x^3 + x + 1)}$$

Афінне перетворення діє за правилом:

$$Y = C * x + C_1 \pmod{(x^8 + 1)}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

У процедурі ShiftRow останні три рядки стану циклічно зсовуються на різне число байтів ($C1$, $C2$, $C3$) у залежності від довжини блоку Nb .

Таблиця 2.4 – Зсув рядків

Nb	$C1$	$C2$	$C3$
4	1	2	3
6	1	2	3
8	1	3	4

У процедурі MixColumn стовбці стану розглядаються як багаточлени над $GF(2^8)$ і помножуються на багаточлен $g(x) = '03'x^3 + '01'x^2 + '01'x + '02'$ за модулем $(x^4 + 1)$:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

Загальне число бітів раундових ключів дорівнює довжині блоку, помноженої на число раундів, плюс 1 (наприклад, для довжини блоку 128 біт і 10 циклів буде потрібно 1408 біт циклового ключа). Ключ шифрування розширюється в розширений ключ. Раундові ключі беруться з розширеного ключа в такий спосіб: перший раундовий ключ містить перші Nb слів, другий – наступні Nb слів і т.д.

2.1.2 Режими шифрування

Під режимом шифрування розуміється такий алгоритм застосування блокового шифру, що при відправленні повідомлення дозволяє перетворювати відкритий текст у шифротекст і, після передачі цього шифротексту по відкритому каналу однозначно відновити первісний відкритий текст. Як видно з визначення, сам блоковий шифр тепер є тільки частиною іншого алгоритму – алгоритму режиму шифрування. Це обумовлено тим, що блоковий шифр працює тільки з окремим блоком даних, у той час як алгоритм

режиму шифрування має справу вже з цілим повідомленням, що може складатися з деякого числа n блоків. Більш того, повідомлення взагалі не зобов'язане складатися з блоків, у тім змісті, що це повідомлення не завжди можна розбити на ціле число n блоків. У цьому випадку в різних режимах шифрування приходиться доповнювати повідомлення різною кількістю біт.

Передбачено можливість функціонування блокових шифрів у наступних режимах шифрування:

- режим електронна кодова книга (ECB);
- режим зціплення блоків шифротексту (CBC);
- режим зворотного зв'язку по шифротексту (CFB);
- режим зворотного зв'язку по виходу (OFB);
- режим шифрування з лічильником (Counter).

На рисунках 2.1 – 2.5 приведені схеми шифрування в цих режимах. Використані наступні позначення:

P_i – i -й блок відкритого тексту;

E_k – функція зашифрування на ключі k ;

C_i – i -й блок зашифрованого тексту;

D_k – функція розшифрування на ключі k ;

S_i – i -те значення лічильнику;

S_0 – синхропосилка.

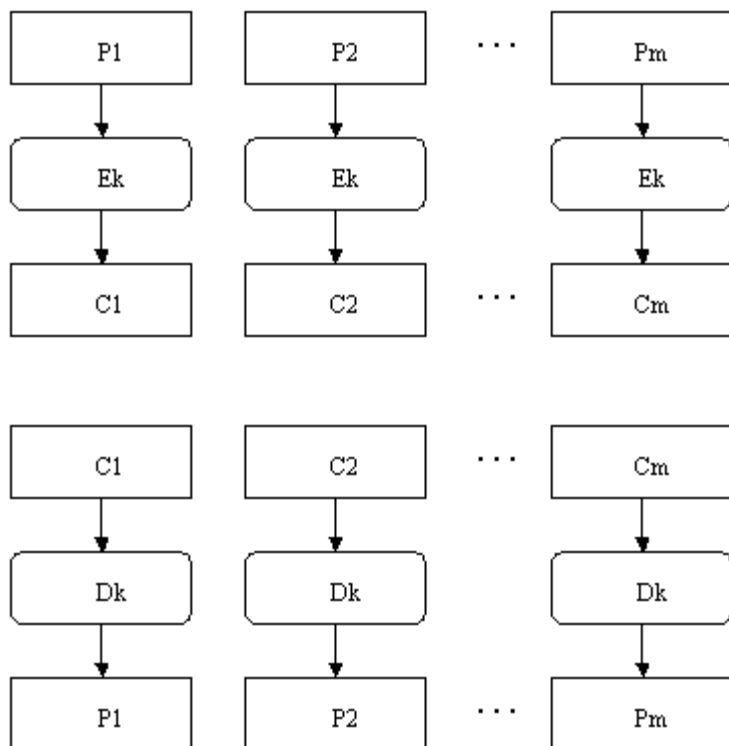


Рисунок 2.1 – Режим електронна кодова книга (ECB)

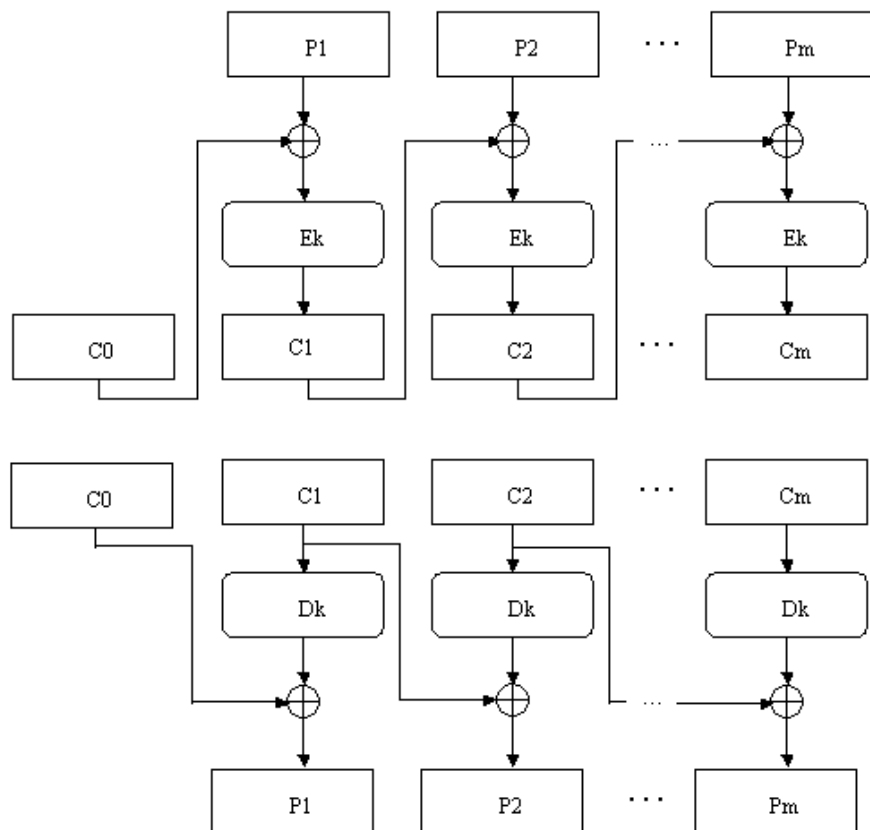


Рисунок 2.2 – Режим зв'язування блоків шифротексту (CBC)

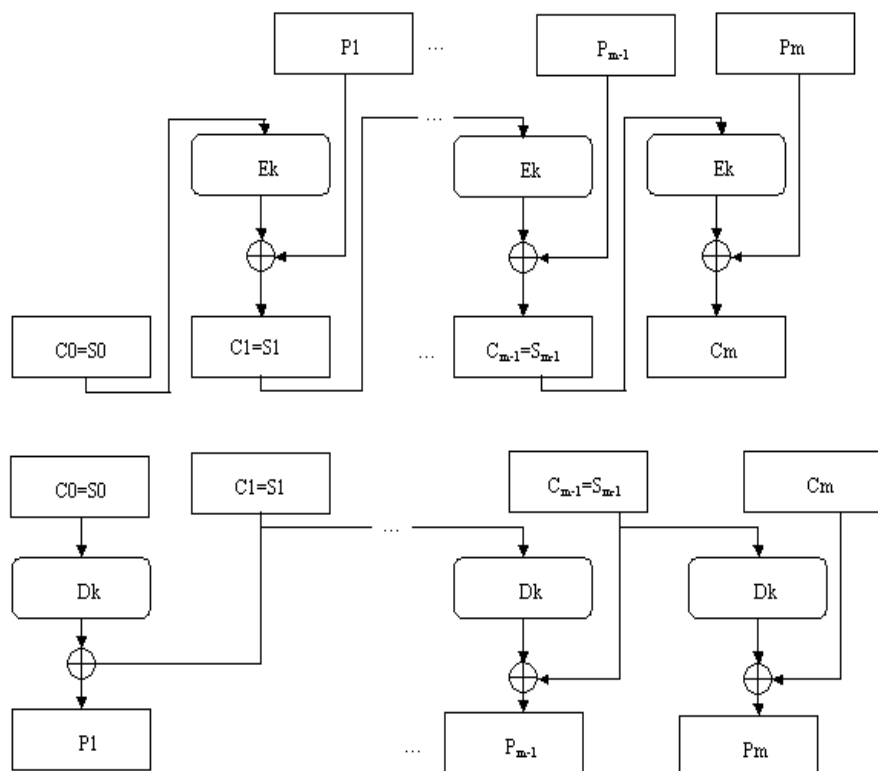


Рисунок 2.3 – Режим зворотного зв'язку по шифротексту (CFB)

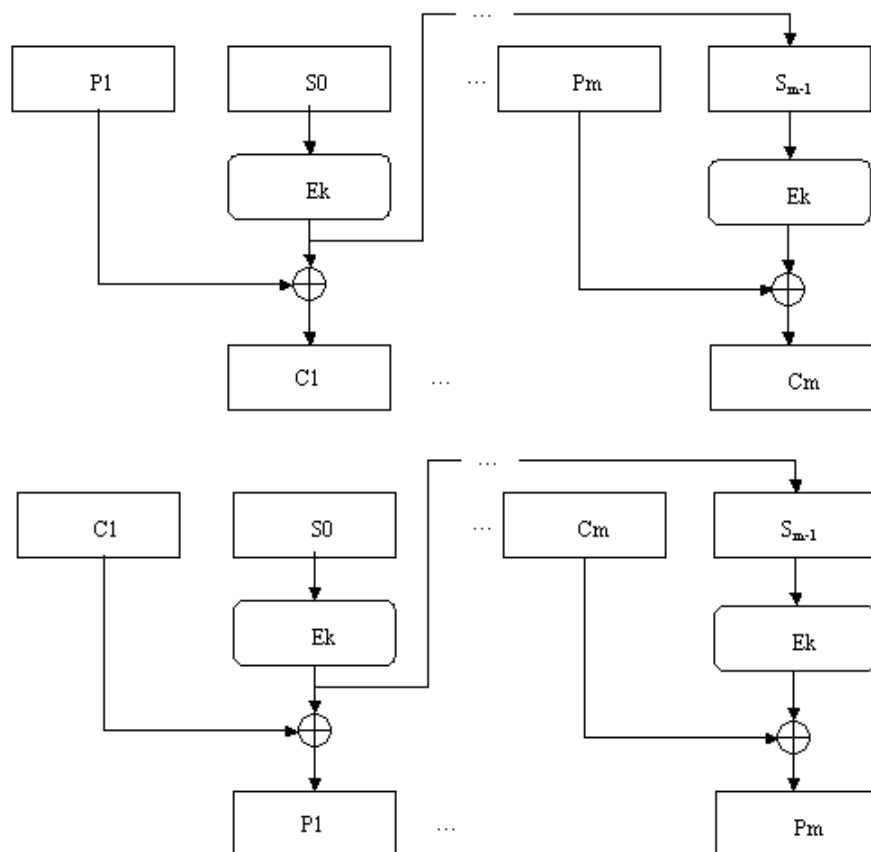


Рисунок 2.4 – Режим зворотного зв'язку по виходу (OFB)

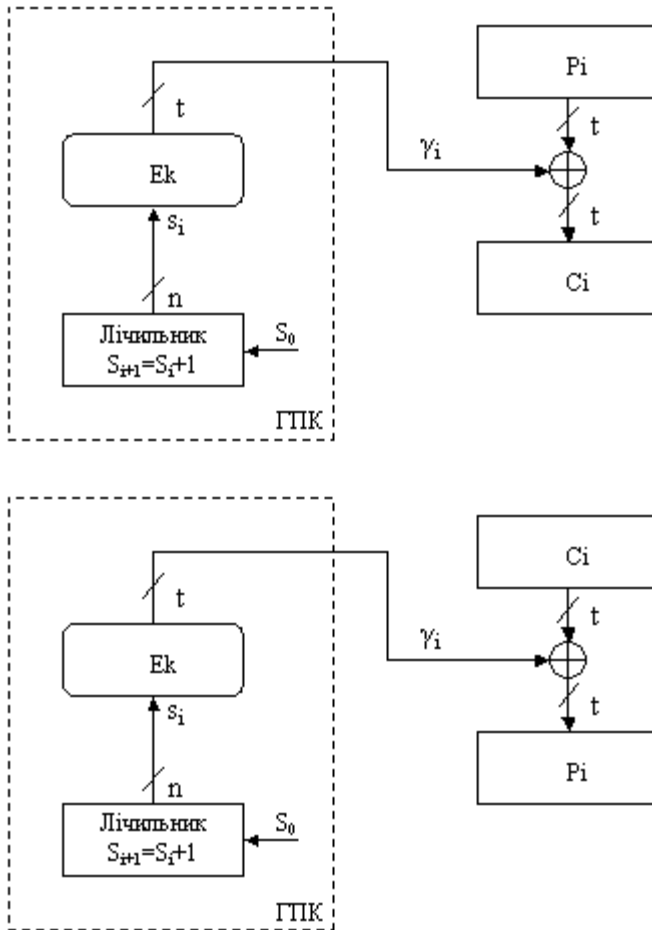


Рисунок 2.5 – Режим шифрування з лічильником (Counter)

Розглянуті режими шифрування представлені в документі *Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001 Edition*, що був виданий NIST США і має назву «Рекомендації для режимів шифрування з блоковим шифром».

2.2 Завдання на лабораторну роботу

2.2.1 Створити проект з підключенням бібліотеки MIRACL згідно додатку Б. Додати до проекту файл mraes.c з каталогу \miracl\source. Відкомпілювати та запустити програму. По тексту програми розібрати програмну реалізацію алгоритму симетричного шифрування AES (RIJNDAEL).

2.2.2 Розробити програму використання алгоритму RIJNDAEL в наступних режимах шифрування:

- режим електронна кодова книга (ECB);
- режим зіплення блоків шифротексту (CBC);
- режим зворотного зв'язку по шифротексту (CFB);
- режим зворотного зв'язку по виходу (OFB);
- режим шифрування з лічильником (Counter).

2.3 Зміст звіту

2.3.1 Титульний лист, тема і мета роботи.

2.3.2 Відповіді на контрольні питання.

2.3.3 Опис функцій бібліотеки MIRACL для реалізації AES.

2.3.4 Тексти програм.

2.3.5 Результати роботи програм.

2.3.6 Висновки.

2.4 Контрольні питання

2.4.1 З яких операцій складається один раунд алгоритму RIJNDAEL?

2.4.2 Поясніть роботу алгоритму в режимі електронна кодова книга (ECB).

2.4.3 Поясніть роботу алгоритму в режимі зіплення блоків шифротексту (CBC).

2.4.4 Поясніть роботу алгоритму в режимі зворотного зв'язку по шифротексту (CFB).

2.4.5 Поясніть роботу алгоритму в режимі зворотного зв'язку по виходу (OFB).

2.4.6 Поясніть роботу алгоритму в режимі шифрування з лічильником (Counter).

2.4.7 Чому шифри ГОСТ 28147-89 та RIJNDAEL називаються блоковими шифрами?

2.4.8 Якими можуть бути довжина ключа и блока в ГОСТ 28147-89 та в RIJNDAEL?

2.4.9 В чому полягає основний шаг криптосистем ГОСТ 28147-89 та RIJNDAEL?

2.4.10Перечисліть основні режими шифрування блокових шифрів.

2.4.11Які основні параметри шифрів ГОСТ 28147-89 та RIJNDAEL?

2.4.12В чому полягає режим простої заміни?

2.4.13В чому полягає режим гамування?

2.4.14В чому полягає гамування зі зворотним зв'язком?

2.4.15В чому полягає режим виробітки імітовставки?

ЛАБОРАТОРНА РОБОТА № 3

КРИПТОГРАФІЯ З ВІДКРИТИМ КЛЮЧЕМ.

ФУНКЦІЯ ГЕШУВАННЯ

Мета роботи: ознайомитися з найпростішою функцією гешування та схемами електронного цифрового підпису RSA та ElGamal.

Використовуване програмне забезпечення: пакети математичних обчислень MathCad і Maple.

3.1 Теоретичні відомості

3.1.1 Асиметричні криптосистеми

Ефективними системами криптографічного захисту даних є *асиметричні криптосистеми*. В таких системах для зашифрування даних використовується один ключ, а для розшифрування – інший. Причому ключі пов'язані між собою певним математичним співвідношенням, що робить можливим процес адекватного розшифрування. Концепція таких криптосистем ґрунтується на застосуванні односторонніх функцій з секретом, що дозволяє легко отримати відкритий ключ із секретного, але не навпаки.

Двухключова криптографія використовується в двох схемах: *цифрового підпису* і *спрямованого шифрування*. В першому випадку повідомлення підписується закритим ключем і будь-яка особа може упевнитися в його дійсності за допомогою відкритого ключа. В схемі спрямованого шифрування, навпаки, повідомлення зашифровується на відкритому ключі отримувача. Розшифрувати повідомлення має можливість тільки сам отримувач за допомогою свого секретного ключа.

В протоколах цифрового підпису застосовується так звана «геш-функція».

Геш-функцією називається перетворення H , що переводить повідомлення M довільної довжини у повідомлення $H(M)$ фіксованої довжини. Геш-функція повинна задовольняти таким вимогам:

- не вище чим поліноміальна складність обчислення значення геш-функції;

- не нижче чим експоненціальна складність визначення повідомлення M_i по відомому значенню $H(M_i)$;

- практична захищеність від колізій, коли можна знайти M_i та M_j , такі, що $H(M_i)=H(M_j)$, з імовірністю не вище чим P_k , де P_k завідомо задане значення.

3.1.2 Алгоритм RSA в схемі спрямованого шифрування

Алгоритм RSA запропонували у 1978 р. три автора Р.Райвест, А.Шамір, А.Адлеман. Стійкість алгоритму базується на складності факторизації великих чисел і трудності обчислення дискретних логарифмів.

Алгоритм RSA використовується в моделі взаємної недовіри. Її сутність полягає в тім, що кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Він також забезпечує цілісність і дійсність відкритих ключів. Таким чином, будь-хто може надіслати йому повідомлення, зашифроване на відомому відкритому ключі, яке може прочитати тільки сам користувач, бо тільки він володіє відповідним секретним ключем.

Алгоритм 3.1

1. Обираємо модуль перетворень $N=P*Q$, де P, Q – випадкові великі прості числа.

2. Обчислюємо $\varphi(N)=(P-1)(Q-1)$, де $\varphi(N)$ - функція Ейлера, що вказує кількість додатних цілих чисел в інтервалі від 1 до N , що взаємно прості з N .

3. Відкритий ключ e вибирається випадково так, щоб виконувались умови

$$1 < e \leq \varphi(N), \quad \text{НОД}(e, \varphi(N)) = 1$$

4. Обчислюємо закритий ключ d з умови

$$ed = 1 \bmod \varphi(N), \text{ або}$$

$$d = e^{-1} \bmod (P-1)(Q-1),$$

використовуючи розширений алгоритм Евкліда. Ключ d та модуль N повинні бути взаємно простими.

5. Зашифрування повідомлення M відбувається за формулою

$$C = M^e \bmod N$$

6. Розшифрування повідомлення відбувається за формулою

$$M = C^d \bmod N$$

3.1.3 Цифровий підпис Эль-Гамал

Цифровий підпис Эль-Гамал базується на великій обчислювальній складності задачі дискретного логарифмування.

Позначення:

p – велике просте число, модуль перетворень;

a – первісний корінь за модулем p ;

x – секретний ключ;

y – відкритий ключ $y = a^x \bmod p$;

M – повідомлення, що підписується ($M < p$);

$r, s = f(M, x)$ – підпис.

Алгоритм 3.2

Формування підпису Эль-Гамал

1. Згенерувати випадкове число k , що задовольняє умовам

$$0 < k < p-1 \text{ и } \text{НОД}(k, p-1) = 1$$

2. Обчислити $r = a^k \bmod p$
3. Обчислити s з рівняння

$$M = xr + ks \bmod (p-1)$$

З теорії чисел відомо, що таке рівняння має рішення для s , якщо $\text{НОД}(k, p-1) = 1$.

Перевірка підпису Эль-Гамал.

Якщо $(a^M) = a^{xr} a^{ks} = y^r r^s \bmod p$ підпис є дійсним.

3.2 Завдання на лабораторну роботу

3.2.1 Створіть геш-образ повідомлення

«ВЫДАТЬ_СТО_ГРН_ГЛБУХ_[ФАМИЛИЯ]»,

з використанням формули

$$H_i = (H_{i-1} + M_{i-1})^2 \bmod 33$$

і кодової таблиці. Значення $H_0 = 9$.

Таблиця 3.1 – Кодова таблиця

А	1	00001	И	9	01001	С	17	10001	Щ	25	11001
Б	2	00010	К	10	01010	Т	18	10010	Ъ	26	11010
В	3	00011	Л	11	01011	У	19	10011	Ы	27	11011
Г	4	00100	М	12	01100	Ф	20	10100	Ь	28	11100
Д	5	00101	Н	13	01101	Х	21	10101	Э	29	11101
Е	6	00110	О	14	01110	Ц	22	10110	Ю	30	11110
Ж	7	00111	П	15	01111	Ч	23	10111	Я	31	11111
З	8	01000	Р	16	10000	Ш	24	11000	_	32	00000

Геш-образ повідомлення представте в двійковому вигляді.

3.2.2 Використовуючи відкритий $e = 7$ і закритий $d = 3$ ключі та модуль $n = 33$ схеми RSA, зформуйте та перевірте цифровий підпис для повідомлення.

«ВЫДАТЬ_СТО_ГРН_ГЛБУХ_[ФАМИЛИЯ]»,

Геш-образ візьміть із завдання 3.2.1; цифровий підпис представте в двійковому виді.

Сформуйте та перевірте цифровий підпис зформованого геш-образа за допомогою схеми ElGamal.

3.2.3 Для заданого повідомлення в двійковому виді,

00101011	10001000	11100001	10111010	00000000
01101000	01000000	11000100	10101101	01101001
01110011	01000000	01001000	00110100	00000101
01001100	00001100	10101001	00111010	00011001

- відокремліть повідомлення і цифровий підпис, створений за допомогою алгоритму RSA (5 біт);
- повідомлення і цифровий підпис представте у десятковому виді;
- за допомогою відкритого ключа $e = 17$ і модуля $n = 33$ розшифруйте цифровий підпис;
- сформуєте геш-образ відокремленого повідомлення (см. завдання 3.2.1);
- перевірте коректність поставленого підпису, порівнявши результати двох попередніх пунктів;
- прочитайте повідомлення.

3.3 Зміст звіту

- 3.3.1 Титульний лист, тема і мета роботи.
- 3.3.2 Відповіді на контрольні питання.
- 3.3.3 Опис алгоритмів RSA та ElGamal.
- 3.3.4 Тексти програм
- 3.3.5 Результати розрахунків.

3.4 Контрольні питання

- 3.4.1 Поняття криптографії з відкритим ключем.
- 3.4.2 Поняття геш-функції. Її властивості.
- 3.4.3 Модель взаємної недовіри.
- 3.4.4 Загальна схема формування та перевірки цифрового підпису.
- 3.4.5 Загальна схема спрямованого шифрування.
- 3.4.6 Схема цифрового підпису RSA.
- 3.4.7 Доказати математично коректність алгоритму RSA.
- 3.4.8 Схема цифрового підпису ElGamal.
- 3.4.9 Доказати математично коректність алгоритму ElGamal.
- 3.4.10 Від чого захищає цифровий підпис? Яким чином?

ЛАБОРАТОРНА РОБОТА № 4

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ЕЛІПТИЧНИХ КРИВИХ

Мета роботи: ознайомитися з алгоритмами криптографічних перетворень на еліптичних кривих.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

4.1 Теоретичні відомості

На даний час на території України діють:

а) закон України "Про електронний цифровий підпис" – 2003, що визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису;

б) закон України "Про електронні документи та електронний документообіг" – 2003, що встановлює основні організаційно-правові положення електронного документообігу та використання електронних документів.

Сучасні світові стандарти цифрового підпису ґрунтуються на арифметиці еліптичних кривих. Наприклад:

ДСТУ 4145-2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. Київ:- Держстандарт України, 2003.

ГОСТ Р 34.10-2001. Государственный стандарт российской федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи. М.: Госстандарт России, 2001.

ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

Еліптична крива - це математичний об'єкт, що може бути визначений над будь-яким полем, зокрема над полем дійсних чисел або над скінченним полем Галуа.

У загальному випадку еліптична крива над полем K має вигляд

$$E: y^2 + axy + by = x^3 + cx^2 + dx + e,$$

де $a, b, c, d, e \in K$.

На рис.4.1 поданий приклад еліптичної кривої, визначеної рівнянням

$$y^2 = x^3 + x + 1,$$

над полем дійсних чисел R .

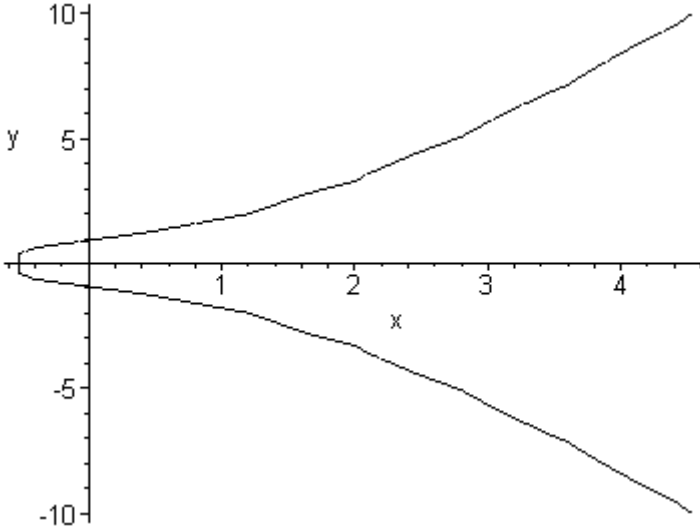


Рисунок 4.1 - Приклад еліптичної кривої $y^2 = x^3 + x + 1$ над R .

4.1.1 Еліптичні криві над простим полем Галуа $GF(p)$

У криптографії застосовуються еліптичні криві, визначені над скінченним полем Галуа $GF(q)$. У цьому випадку вони являють собою множину точок $E(GF(q))$, координати яких задовольняють рівнянню кривої.

Приклад. Дано еліптичну криву $y^2 = x^3 + x + 1 \pmod{5}$ над полем $GF(5)$. Цьому рівнянню задовольняють 8 скінченних точок із координатами з $GF(5)$. На рис.4.2 подано приклад цієї кривої.

$$L := [[2, 4], [0, 1], [0, 4], [2, 1], [3, 1], [3, 4], [4, 2], [4, 3]]$$

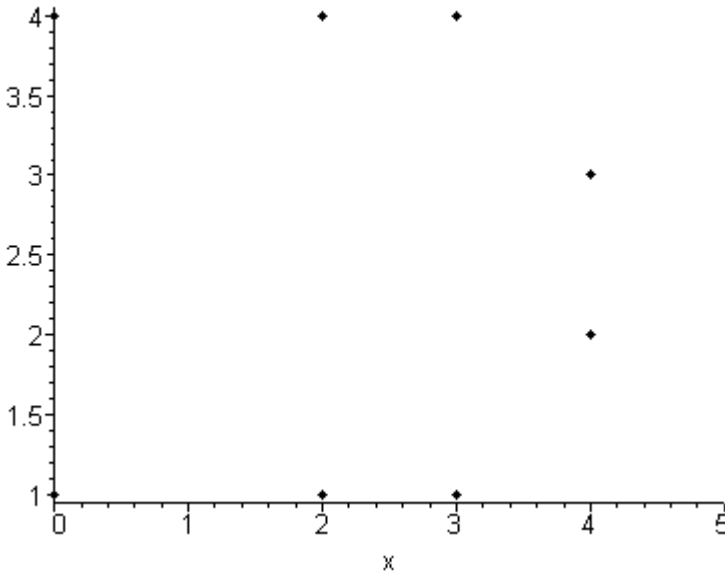


Рисунок 4.2 - Приклад еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$ над полем $GF(5)$

Розглянемо еліптичні криві над простим полем $GF(p)$:

$$y^2 = x^3 + ax + b \pmod{p}, \quad (4.1)$$

де p - просте число - модуль перетворень; параметри кривої $a, b \in GF(p)$ - невід'ємні і задовольняють умові гладкості кривої $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, змінні $x, y \in GF(p)$.

Крім точок (x, y) , що задовольняють рівнянню (4.1), у множину точок еліптичної кривої також включається нескінченно віддалена точка $\mathbf{O}$.

Наприклад, при $p = 2$ точками еліптичної кривої $y^2 = x^3 + x + 1 \pmod{2}$ є три точки - $(0,1)$, $(1,1)$ і $\mathbf{O}$.

Позначимо через $E_p(a,b)$ множину точок еліптичної кривої виду (4.1).

На множині $E_p(a,b)$ введемо операцію додавання $+$ за правилом: нехай $P_1=(x_1, y_1)$ і $P_2=(x_2, y_2)$ - точки еліптичної кривої, тоді

координати суми точок $P_3 = P_1 + P_2 = (x_3, y_3)$ визначаються за формулами

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$$

$$y_3 = (\lambda (x_1 - x_3) - y_1) \bmod p$$

$$\text{Якщо } P_1 \neq P_2, \text{ то } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}.$$

$$\text{Якщо } P_1 = P_2, \text{ то } \lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p}.$$

Вважаємо, що $P + \mathbf{O} = \mathbf{O} + P$.

Твердження. Множина точок еліптичної кривої $E_p(a,b)$ з операцією додавання $+$ утворює адитивну абелеву групу з нейтральним (нульовим) елементом $\mathbf{O}$, тобто виконуються умови групи:

а) якщо $P, Q \in E_p(a,b)$, то $P + Q \in E_p(a,b)$;

б) для будь-яких трьох точок кривої $P, Q, S \in E_p(a,b)$

$$P + (Q + S) = (P + Q) + S;$$

в) для будь-якої точки $P = (x, y) \in E_p(a,b)$ існує обернена точка $-P$, така, що $P + (-P) = \mathbf{O}$; точка $(-P)$ має координати $(x, -y)$.

Приклад. Знайдемо точки еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$. Можливі значення змінної $x \in \{0, 1, 2, 3, 4\}$. Задаючи значення x , знайдемо y :

$$x = 0 \quad y^2 = 1 \quad \Rightarrow \quad y = 1, y = -1 \text{ або } y = 4$$

$$x = 1 \quad y^2 = 3 \quad \Rightarrow \quad \text{розв'язків немає}$$

$$x = 2 \quad y^2 = 11 = 1 \quad \Rightarrow \quad y = 1, y = 4$$

$$x = 3 \quad y^2 = 31 = 1 \quad \Rightarrow \quad y = 1, y = 4$$

$$x = 4 \quad y^2 = 69 = 4 \quad \Rightarrow \quad y = 2, y = -2 \text{ або } y = 3$$

Таким чином, одержимо точки $(0,1)$, $(0,4)$, $(2,1)$, $(2,4)$, $(3, 1)$, $(3,4)$, $(4,2)$, $(4,3)$ і додаємо точку $\mathbf{O}$. Еліптична крива $E_5(1,1)$ містить 9 точок.

Визначення. Порядком групи точок еліптичної кривої $E_p(a,b)$ називається число елементів цієї групи. Позначення - $\# E_p(a,b)$.

Група точок еліптичної кривої $E_5(1,1)$ має порядок рівний 9.

4.1.2 Алгоритм обчислення точок еліптичної кривої

Нехай задана еліптична крива $y^2 = x^3 + ax + b \pmod{p}$. Для кожного значення x , $0 \leq x \leq p-1$:

а) обчислюємо $A = x^3 + ax + b \pmod{p}$;

б) вирішуємо порівняння $y^2 = A \pmod{p}$. Якщо порівняння має розв'язок, то є два значення y (крім випадку $y = 0$) – y_1, y_2 : $y_1^2 = A \pmod{p}$. У цьому випадку точки (x, y_1) і (x, y_2) належать еліптичній кривій.

4.1.3 Приклад додавання точок еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$.

Нехай $P_1 = (0,1)$, $P_2 = (4,2)$, $x_1 = 0$, $y_1 = 1$, $x_2 = 4$, $y_2 = 2$.

а) $P_1 + P_2 = (x_3, y_3)$.

Так як $P_1 \neq P_2$, то $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$,

$$\lambda = (2-1)/(4-0) = 1/4 \pmod{5} = 4.$$

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{p} = 16 - 0 - 4 = 12 \pmod{5} = 2.$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{p} = 4(0 - 2) - 1 = -9 \pmod{5} = 1.$$

Таким чином, $(0,1) + (4,2) = (2,1)$.

б) $2P_1 = (x_3, y_3)$

Так як $P_1 = P_2$, то $\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p}$,

$$\lambda = (3 \cdot 0 + 1)/(2 \cdot 1) = 1/2 \pmod{5} = 3.$$

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{p} = 9 - 0 - 0 = 9 \pmod{5} = 4.$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{p} = 3(0 - 4) - 1 = -13 \pmod{5} = 2.$$

Таким чином, $2 \cdot (0,1) = (4,2)$.

с) Аналогічно можна обчислити

$$3P_1 = 2P_1 + P_1 = (4,2) + (0,1) = (2,1)$$

$$4P_1 = 3P_1 + P_1 = (2,1) + (0,1) = (3,4)$$

$$5P_1 = 4P_1 + P_1 = (3,4) + (0,1) = (3,1)$$

$$6P_1 = 5P_1 + P_1 = (3,1) + (0,1) = (2,4)$$

$$7P_1 = 6P_1 + P_1 = (2,4) + (0,1) = (4,3)$$

$$8P_1 = 7P_1 + P_1 = (4,3) + (0,1) = (0,4)$$

$$9P_1 = 8P_1 + P_1 = (0,4) + (0,1) = \mathbf{O}$$

Визначення. Точка $P \in E_p(a,b)$ називається базовою точкою підгрупи точок еліптичної кривої $E_p(a,b)$, якщо будь-яка точка Q цієї підгрупи може бути подана у вигляді $Q = k \cdot P$, де $k=1,2,\dots,n$, де n - порядок підгрупи.

Для базової точки P має місце рівність $n \cdot P = \mathbf{O}$.

Приклад. Точка $P = (0,1)$ є базовою для групи точок еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$.

Твердження (теорема Хасе). Значення порядку групи точок еліптичної кривої над полем Галуа $\text{GF}(q)$ має верхню і нижню межі:

$$q+1-2\sqrt{q} \leq \#E_q(a,b) \leq q+1+2\sqrt{q}$$

Приклад. Нехай $Q = (2,4)$ - точка еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$.

Тоді $2 \cdot Q = (2,1)$, $3 \cdot Q = \mathbf{O}$.

Точка $Q = (2,4)$ породжує циклічну підгрупу порядку 3: $(2,4), (2,1), \mathbf{O}$.

Визначення. Порядком точки Q еліптичної кривої називається найменше число k , таке що $k \cdot Q = \mathbf{O}$.

Точка $Q = (2,4)$, що належить групі точок еліптичної кривої $y^2 = x^3 + x + 1 \pmod{5}$, має порядок, рівний 3.

4.1.4 Алгоритм обчислення порядку точки еліптичної кривої

Нехай задана еліптична крива $y^2 = x^3 + ax + b \pmod{p}$ над полем $\text{GF}(p)$, і точка P належить заданій кривій. Знайдемо порядок точки P . Для цього необхідно вирішити порівняння

$$x \cdot P = \mathbf{O}$$

(адитивний аналог задачі дискретного логарифмування).

Застосуємо алгоритм великих-малих кроків.

Нехай n - максимальна оцінка порядку групи точок еліптичної кривої, отримана по теоремі Хасе, P - точка еліптичної кривої.

Обчислимо $m := \lceil \sqrt{n} \rceil$, де $\lceil a \rceil$ - округлення з надлишком.

1. Будуємо таблицю пар (j, jP) для $j = 1, 2, \dots, m$.
2. Обчислюємо $\alpha := -mP$.
3. $\gamma := \mathbf{O}$.
4. Цикл по i від 0 до $m-1$
 - 4.1 перевіряємо, чи є γ другою компонентою у таблиці п.1
 - 4.2 якщо $\gamma = jP$, то вважаємо $x = m \cdot i + j$
 - 4.3 $\gamma := \gamma + \alpha$.

Приклад. Візьмемо еліптичну криву $y^2 = x^3 + x + 1$ над простим полем $\text{GF}(p)$, $p = 5$. По теоремі Хасе максимальна оцінка порядку групи точок кривої дорівнює $n = p + 1 + 2\sqrt{p} = 5 + 1 + 2\sqrt{5} \approx 10$. Звідси $m = 4$.

За допомогою алгоритму великих-малих кроків знайдемо порядок точки $P = (0,1)$.

Побудуємо таблицю

j	1	2	3	4
jP	(0,1)	(4,2)	(2,1)	(3,4)

Знайдемо $t := -mP = -4(0,1) = -(3,4) = (3, -4) = (3,1)$.

$\gamma := \mathbf{O}$.

$i = 0 \quad \gamma := \gamma + t = \mathbf{O} + (3,1) = (3,1)$.

$i = 1 \quad \gamma = \gamma + t = (3,1) + (3,1) = (0,1)$.

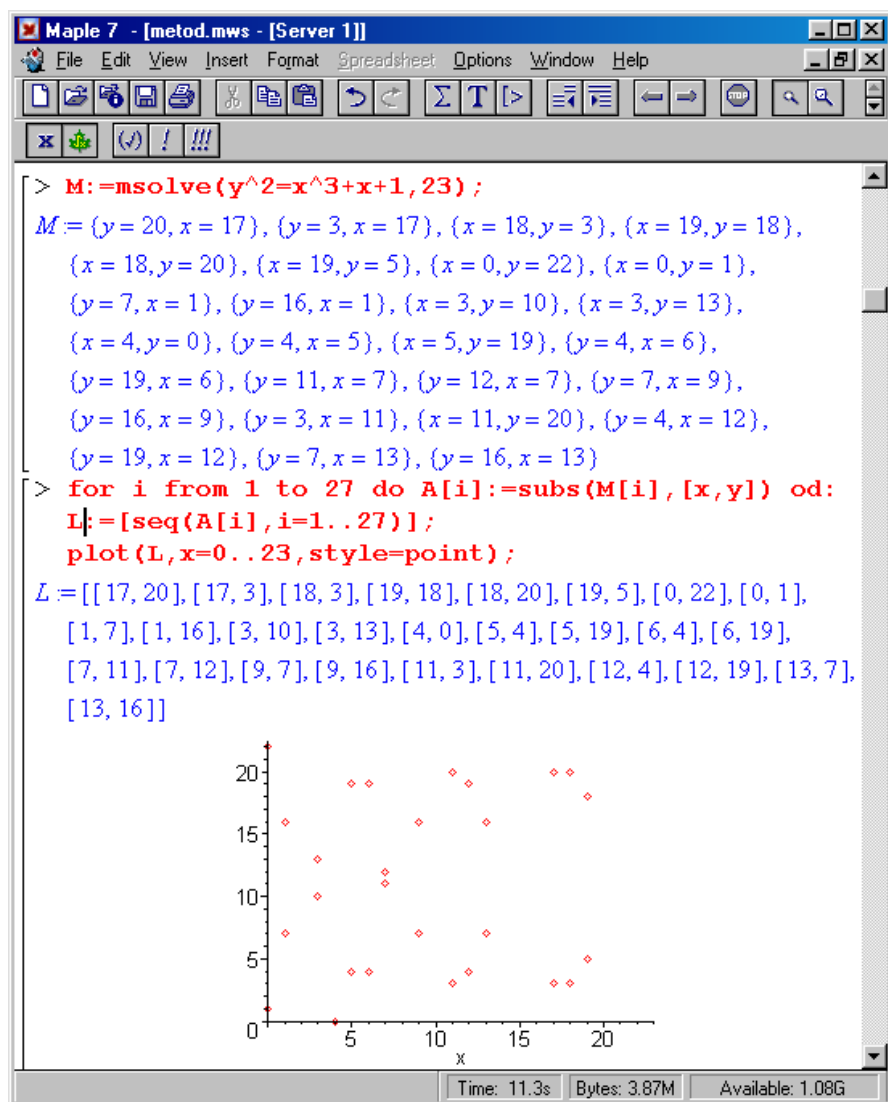
$i = 2 \quad j = 1 \Rightarrow x = m \cdot i + j = 4 \cdot 2 + 1 = 9$.

Порядок точки $P = (0,1)$ дорівнює 9.

На рис. 4.3 показаний приклад еліптичної кривої над полем $\text{GF}(23)$

$$y^2 = x^3 + x + 1 \pmod{23},$$

з параметрами $a = 1$, $b = 1$, $p = 23$, $4a^3 + 27b^2 = 8 \neq 0 \pmod{23}$. Точки кривої визначені як усі рішення рівняння $y^2 = x^3 + x + 1 \pmod{23}$, включаючи нескінченну точку. Отже, порядок групи точок дорівнює $27+1=28$.

Рисунок 4.3 - Приклад еліптичної кривої над полем $GF(23)$.

Наведемо протокол цифрового підпису на еліптичних кривих ГОСТ Р 34.10-2001.

Таблиця 4.1 – Протокол цифрового підпису ГОСТ Р 34.10-2001

Формування цифрового підпису	Перевірка цифрового підпису
Вхід: секретний ключ d , відкритий ключ $Q = d \times P$, загальносистемні параметри. Вихід: ЦП $\langle r, s \rangle$ для повідомлення M .	Вхід: відкритий ключ Q , загальносистемні параметри, ЦП $\langle r', s' \rangle$, для повідомлення M' . Вихід: Підпис дійсний чи ні.
$e = h(M) \bmod n$; - Обираємо $k \in 1, \dots, n-1$; $k \times P = (x, y)$; $r = \pi(x, y) \bmod n$; $s = (rd + ke) \bmod n$.	$e = h(M) \bmod n$; $w = e^{-1} \bmod n$; $z_1 = sw \bmod n$; $z_2 = -rw \bmod n$; $(x, y) = z_1 \times P + z_2 \times Q$; $v = \pi(x, y)$; $r' = v$

4.1.5 Алгоритм скалярного множення на еліптичній кривій

Для множення точки еліптичної кривої на велике ціле число застосовується наступний алгоритм:

Вихідні дані: число $d \neq 0$, точка P , еліптична крива $E = \langle a, b, p \rangle$.

Результат: точка $Q = d \times P$.

1. Якщо $d=1$, то $Q:=P$; закінчити роботу алгоритму.
2. $k:=l_d-2$; $Q:=P$, де l_d – довжина множника d в бітах;
3. Для i , що приймає значення від k до 0, виконати шаги 4-5.
4. $Q := Q+Q$.
5. Якщо i -й біт d дорівнює 1, то $Q := Q+P$.
6. Закінчити роботу алгоритму.

4.2 Завдання на лабораторну роботу

4.2.1 Дано еліптичну криву $y^2 = x^3 + ax + b \pmod{13}$.

Параметри a, b відповідають номеру варіанта (табл. 4.2). Необхідно:

- знайти всі точки, що належать заданій кривій і порядок кривої.

Використовувати пакет Maple;

- знайти базову точку;

- представити кожну точку як кратну базовій (знайти показник кратності).

Таблиця 4.2 – Варіанти завдань

Габарити 12		Варианти завдань		
1. a=1,b=1	11. a=2,b=1	21. a=2,b=11	31. a=3,b=11	41. a=4,b=10
2. a=1,b=2	12. a=2,b=2	22. a=2,b=12	32. a=3,b=12	42. a=4,b=12
3. a=1,b=4	13. a=2,b=3	23. a=3,b=1	33. a=4,b=1	43. a=5,b=1
4. a=1,b=5	14. a=2,b=4	24. a=3,b=2	34. a=4,b=3	44. a=5,b=2
5. a=1,b=6	15. a=2,b=5	25. a=3,b=4	35. a=4,b=4	45. a=5,b=3
6. a=1,b=7	16. a=2,b=6	26. a=3,b=5	36. a=4,b=5	46. a=5,b=4
7. a=1,b=8	17. a=2,b=7	27. a=3,b=6	37. a=4,b=6	47. a=5,b=5
8. a=1,b=9	18. a=2,b=8	28. a=3,b=7	38. a=4,b=7	48. a=5,b=6
9. a=1,b=11	19. a=2,b=9	29. a=3,b=8	39. a=4,b=8	49. a=5,b=7
10. a=1,b=12	20. a=2,b=11	30. a=3,b=9	40. a=4,b=9	50. a=5,b=8

4.2.2 Реалізувати в Maple алгоритм цифрового підпису ГОСТ Р 34.10. Для тестування використати наступні параметри (в шестнадцатерічній формі):

Модуль перетворень

[illegible]

Еліптична крива

$$y^2 = x^3 + ax + b \pmod{m}$$

```
a=7;
```

b=5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514COCE9DAE23B7E;

Базова точка $P(x, y)$;

 $P_X=2;$

Pv=8E2A8A0E65147D4BD6316030E16D19C85C97F0A9CA267122B96ABBCEA7E8FC8:

Порядок базової точки:

[illegible]

Секретный ключ

d=7A929ADE789BB9BE10ED359DD39A72C11B60961F49397EEE1D19CE9891EC3B28:

Результат множення (відкритий ключ) точка $Q(Q_x, Q_y)$

Qx=7F2B49E270DB6D90D8595BEC458B50C58585BA1D4E9B788F6689DBD8E56FD80B:

Qy=26F1B489D6701DD185C8413A977B3CBBAF64D1C593D26627DFFB101A87FF77DA.

4.3 Зміст звіту

- 4.3.1 Титульний лист, тема і мета роботи.
- 4.3.2 Відповіді на контрольні питання.
- 4.3.3 Тексти програм.
- 4.3.4 Результати обчислень.
- 4.3.5 Висновки.

4.4 Контрольні питання

- 4.4.1 Дати визначення еліптичної кривої.
- 4.4.2 Як визначити точку, обернену даній?
- 4.4.3 Які параметри еліптичної кривої необхідно знати для її застосування?
- 4.4.4 Дати визначення порядку групи точок еліптичної кривої?
- 4.4.5 Дати визначення порядку точки еліптичної кривої?
- 4.4.6 Як визначити базову точку?
- 4.4.7 У яких криптографічних алгоритмах застосовуються еліптичні криві?

ЛАБОРАТОРНА РОБОТА № 5 СТЕГАНОГРАФІЧНИЙ ЗАХИСТ

Мета роботи: ознайомитися з методами стеганографічного захисту інформації.

Використовуване програмне забезпечення: середовище розробки Visual C++.

5.1 Теоретичні відомості

У ряді систем необхідно забезпечити не тільки конфіденційність, цілісність і дійсність переданих команд, але й сховати сам факт передачі цієї інформації. Цим займається стеганографія.

Під стеганографією розуміється спосіб тайнопису, який більш давніший ніж сама криптографія. Основною метою криптографії є забезпечення конфіденційності, цілісності, спостережності та доступності за рахунок використання методів криптографічного захисту інформації.

Стеганографія - це наука про приховання однієї інформації серед іншої. Це метод організації зв'язку, що власне ховає саму наявність зв'язку.

На відміну від криптографії, де ворог точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в загальні послання так, щоб неможливо було запідозрити існування убудованого таємного послання.

Слово "стеганографія" у перекладі з грецького буквально означає "тайнопис" (steganos - секрет, таємниця; graphy - запис). До неї відноситься величезна множина секретних засобів зв'язку, таких як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні канали і засоби зв'язку на частотах, що плавають, і т.д.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не заміняє, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує імовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифроване, то воно має ще один, додатковий, рівень захисту.

В даний час у зв'язку з бурхливим розвитком обчислювальної техніки і нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості представлення інформації в комп'ютерних файлах, обчислювальних мережах і т.п. Це дає можливість говорити про становлення нового напрямку - комп'ютерної стеганографії.

5.1.1 Стеганографічна система

Стеганографічна система чи стегосистема (рис 5.1) - це сукупність засобів і методів, що використовуються для формування схованого каналу передачі інформації.



Рисунок 5.1 - Стеганографічна система

При побудові стегосистеми повинні враховуватися наступні положення:

- супротивник має повне представлення про стеганографічну систему і деталі її реалізації. Єдиною інформацією, що залишається невідомою потенційному супротивнику, є ключ, за допомогою якого тільки його власник може установити факт присутності і зміст схованого повідомлення;

- якщо супротивник якимсь образом довідається про факт існування схованого повідомлення, це не повинно дозволити йому витягти подібні повідомлення в інших даних доти, поки ключ зберігається в таємниці;

- потенційний супротивник повинний бути позбавлений яких-небудь технічних і інших переваг у розпізнаванні чи розкритті змісту таємних повідомлень.

Контейнер - будь-яка інформація, призначена для приховання таємних повідомлень.

Порожній контейнер - контейнер без убудованого повідомлення; заповнений контейнер чи стего - контейнер, що містить убудовану інформацію.

Убудоване (сховане) повідомлення - повідомлення, що вбудовується в контейнер.

Стеганографический канал чи просто *стегоканал* - канал передачі стего.

Стегоключ чи просто *ключ* - секретний ключ, необхідний для приховування інформації. У залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистемі може бути один чи декілька стегоключів.

5.1.2 LSB-метод (Least Significant Bits) приховування інформації

В даний час найбільш розповсюдженим є метод заміни найменших значущих бітів чи LSB-метод. Він полягає у використанні погіршності дискретизації, що завжди існує в оцифрованих зображеннях чи аудіо- і відеофайлах. Дана погіршність дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших бітів у більшості випадків не викликає значної трансформації зображення і не виявляється візуально.

Суть методу така. Цифрові картинки складаються з окремих крапок, так званих пікселів. Якщо зображення 8-бітове, це значить, що для опису одного пікселя картини приділяється один байт графічного файлу. Один байт, як відомо, складається з восьми біт, кожний з яких може дорівнювати нулю чи одиниці. Програма - стеганограф теж повинна записати файл-повідомлення нулями й одиницями, і вона розміщає ці біти поверх самих останніх восьми бітів кожного байта в графічному файлі. Якщо нуль чи одиниця файлу-повідомлення волею случая збігаються з нулем чи одиницею файлу-контейнера, то ніяких змін не відбувається. Якщо ж вони не збігаються, програма - стеганограф записує останній біт так, як їй потрібно.

Звичайно, після цього весь байт графічного файлу змінює свою значення, але оскільки змінюється тільки останній його біт – найменш значущий, то байт змінюється тільки на одиницю. Наприклад, якщо

спочатку байт дорівнює п'ятдесятьом, то після стеганографії він дорівнює п'ятдесят одному чи сорока дев'яти. Така зміна, звичайно, змінює колір одного пікселя, що відноситься до зміненого байта. Але тому що байт змінюється тільки на одиницю, то і відтінок пікселя змінюється незначно, і помітити його на око практично неможливо, особливо якщо мова йде про чорно-білу фотографію, оскільки градації сірого людина розрізняє набагато гірше кольорових відтінків.

В добавок до цього, графічний файл може бути не 8-ми, а 24-бітним, так зиваний true-color, у якому кожен піксель може мати 16 мільйонів відтінків. Крім того, якщо повідомлення, що ховає стеганограф, маленьке, те зовсім не обов'язково змінювати кожен байт картинки - цілком достатньо може виявитися кожного десятого, чи навіть кожного сотого байта.

5.1.3 Формат BMP-файлу

Файли формату BMP (скорочено від BitMaP – бітовий образ) зберігають зображення в True Color. Розглянемо формат файлу BMP для 24-розрядного рисунку. Файл BMP включає заголовок – 54 байти та бітовий образ зображення. Кожна точка зображення – піксель (picture element) – описується трьома байтами, що включають складові частини кольору - червона (Red), зелена (Green), синя (Blue) (див. рис. 5.2). Інтенсивність складових частин кольору змінюється в межах від 0 до 255. Шляхом варіації інтенсивності кожної складової частини можна змінювати колір від чорного, коли інтенсивність всіх складових частин дорівнює 0 (00 00 00), до білого, коли інтенсивність всіх складових частин максимальна і дорівнює 255 (FF FF FF). Наприклад, точка червоного кольору задається як (255,0,0) або (FF 00 00).

Зображення записується в файл по строкам. Першою сканується нижня строка (зліва направо). Скан - строки вирівняні по 32-бітній границі (4 байти). Тобто, якщо ширина зображення не кратна 4, то інформація по строку доповнюється нульовими байтами.



Рисунок 5.2 – Представлення кольору трьома складовими частинами RGB

Розмір заголовку 24-розрядного рисунку – 54 байти. В табл. 5.1 наведено призначення окремих байтів заголовку BMP - файлу.

Таблица 5.1 – Призначення байтів заголовку BMP - файлу.

1-2 байти :	тип файлу - BM (bit mapping)
3-6 байти :	розмір файлу
7-10 байти :	не використовуються
11-14 байти :	зсув даних бітового образу от заголовку в байтах - 54
15-18 байти :	число байт до начала бітового образу - 40
19-22 байти :	ширина бітового образу в пікселях
23-26 байти :	висота бітового образу в пікселях
27-28 байти :	число бітових площин пристрою - 1
29-30 байти :	число бітів на піксель - 24
31-34 байти :	тип стиску - 0 (без стиску)
35-38 байти :	розмір картинки в байтах
39-42 байти :	горизонтальне разрешение пристрою, піксель/м
43-46 байти :	вертикальне разрешение пристрою, піксель/м
47-50 байти :	кількість кольорів, що використовуються - 0 (всі кольори)
51-54 байти :	кількість "важливих" кольорів

Далі йдуть дані бітового образу картинки. Кожний піксел представляється трьома байтами – інтенсивностями **червоного**, **зеленого**, **синього**.

5.2 Завдання на лабораторну роботу

Реалізувати метод **LSB** в пакеті Visual C++. В якості контейнера застосувати файл формату **.bmp**. В якості повідомлення використати своє «Прізвище Ім'я Побатькові».

5.3 Зміст звіту

- 5.3.1 Титульний лист, тема і мета роботи.
- 5.3.2 Відповіді на контрольні питання.
- 5.3.3 Текст програми.
- 5.3.4 Результати роботи програми.
- 5.3.5 Висновки.

5.4 Контрольні питання

- 5.4.1 Чим відрізняється стеганографія від криптографії?
- 5.4.2 Що таке стегоконтейнер?
- 5.4.3 В чому сутність метода LSB?
- 5.4.4 Як використовуються цифрові водяні знаки?
- 5.4.5 Які недоліки стеганографічного захисту?
- 5.4.6 Що таке стеганографический метод захисту інформації?
- 5.4.7 Що таке контейнер?
- 5.4.8 Що може виступати як контейнер?
- 5.4.9 Вимоги, пропоновані до стего - повідомлень?
- 5.4.10 Що таке цифрові водяні знаки?
- 5.4.11 Які методи вбудовування повідомлень ви знаєте?
- 5.4.12 Що в даній програмі може бути використаний як ключ?

6. ПИТАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

- 6.1 Віртуальні приватні мережі.
- 6.2 Архітектура і конфігурація Firewall.
- 6.3 Захищені операційні системи.
- 6.4 Смарт-карти: архітектура, технології, галузі застосування.
- 6.5 Банківські технології.
- 6.6 Комп'ютерні віруси. Класифікація. Методи протидії.
- 6.7 Захищені бази даних.
- 6.8 Система безпеки Windows XP.
- 6.9 Безпека Internet - бізнесу.
- 6.10 Технічні засоби захисту інформації.

ЛІТЕРАТУРА

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
2. Петраков А.В. «Основы практической защиты информации» – М.: Радио и связь, 1999. – 368с.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.
4. Баричев С.Г., Гончаров В.В. Основы современной криптографии. М.: Горячая линия - Телеком, 2001 – 120с.
5. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации / Под ред. Ю.С. Ковтанька – К.:Изд-во Юниор, 2003. – 504с.
6. Жельников В. Криптография от папируса до компьютера. М.: АБФ, 1996 – 336с.
7. Журнал “Конфидент. Защита информации.” Спецвыпуск по стеганографии. – 2000, № 3.
8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Государственный комитет СССР по стандартам, 1989.
9. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 168 с.
10. Ростовцев А.Г. Алгебраические основы криптографии. – СПб.: НПО «Мир и семья, ООО «Интерлайн», 2000. – 354 с.
11. Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997.
12. Лидл Р., Нидеррайтер Х. Конечные поля. – М.: Мир, 1988.
13. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А.Садовниченко – М.: Высш.шк., 1999. – 109с.
14. Саломеа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318с.
15. Topics in cryptography
http://en.wikipedia.org/wiki/Topics_in_cryptography

Додаток А
Таблица прости́х чисел

1	2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61	67
71	73	79	83	89	97	101	103	107	109
113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199	211	223	227
229	233	239	241	251	257	263	269	271	277
281	283	293	307	311	313	317	331	337	347
349	353	359	367	373	379	383	389	397	401
409	419	421	431	433	439	443	449	457	461
463	467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593	599
601	607	613	617	619	631	641	643	647	653
659	661	673	677	683	691	701	709	719	727
733	739	743	751	757	761	769	773	787	797
809	811	821	823	827	829	839	853	857	859
863	877	881	883	887	907	911	919	929	937
941	947	953	967	971	977	983	991	997	1009
1013	1019	1021	1031	1033	1039	1049	1051	1061	1063
1069	1087	1091	1093	1097	1103	1109	1117	1123	1129
1151	1153	1163	1171	1181	1187	1193	1201	1213	1217
1223	1229	1231	1237	1249	1259	1277	1279	1283	1289
1291	1297	1301	1303	1307	1319	1321	1327	1361	1367
1373	1381	1399	1409	1423	1427	1429	1433	1439	1447
1451	1453	1459	1471	1481	1483	1487	1489	1493	1499
1511	1523	1531	1543	1549	1553	1559	1567	1571	1579
1583	1597	1601	1607	1609	1613	1619	1621	1627	1637
1657	1663	1667	1669	1693	1697	1699	1709	1721	1723
1733	1741	1747	1753	1759	1777	1783	1787	1789	1801
1811	1823	1831	1847	1861	1867	1871	1873	1877	1879

Додаток Б

Підключення криптографічної бібліотеки MIRACL

1. Створити новий проект «Консольное приложение Win32».
2. Підключити до компіляції каталог ...miracl/include.

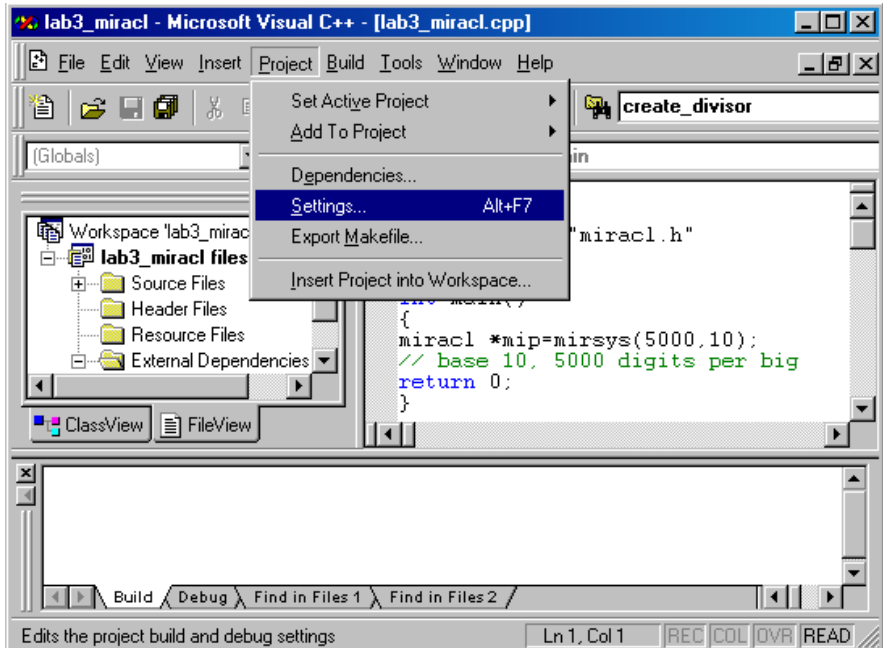


Рисунок Б.1 – Крок 1

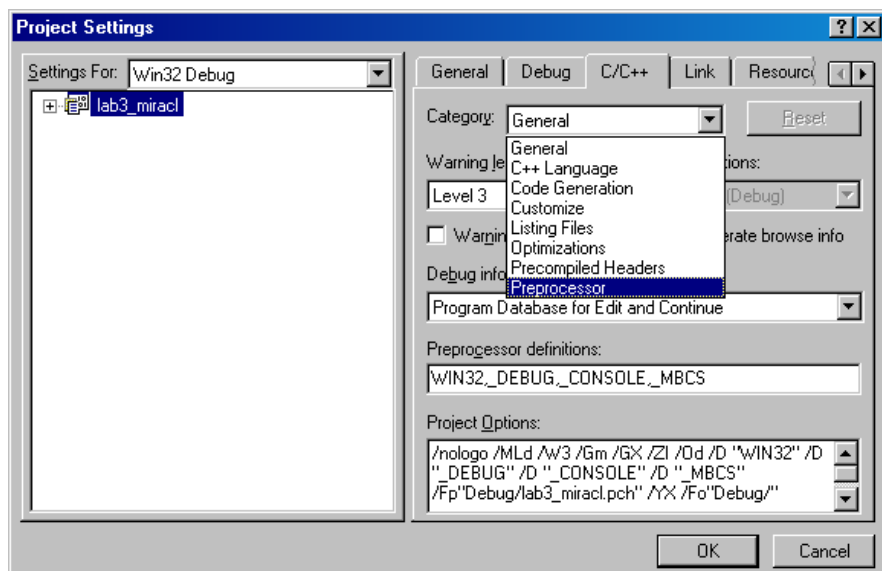


Рисунок Б.2 – Крок 2

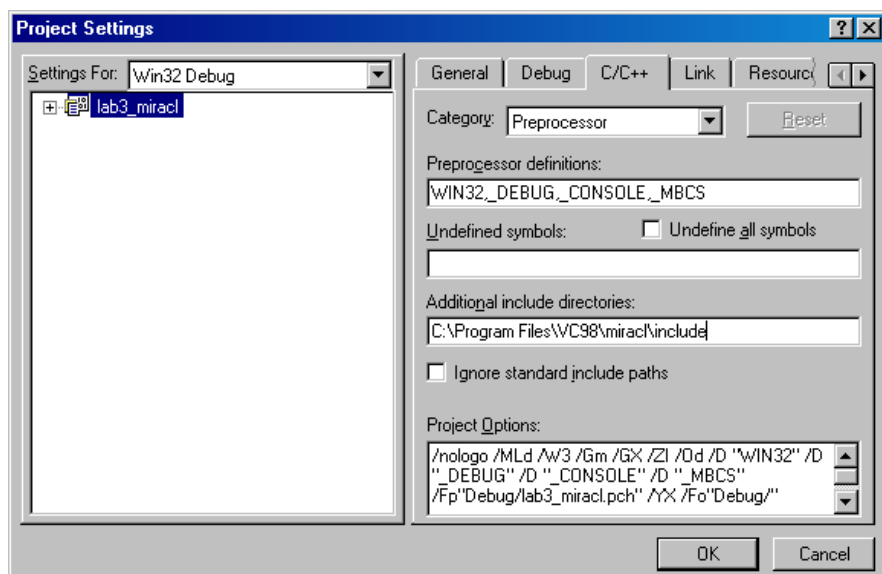


Рисунок Б.3 – Крок 3

3. Добавить до проекту файл ...miracl\lib\ms32.lib

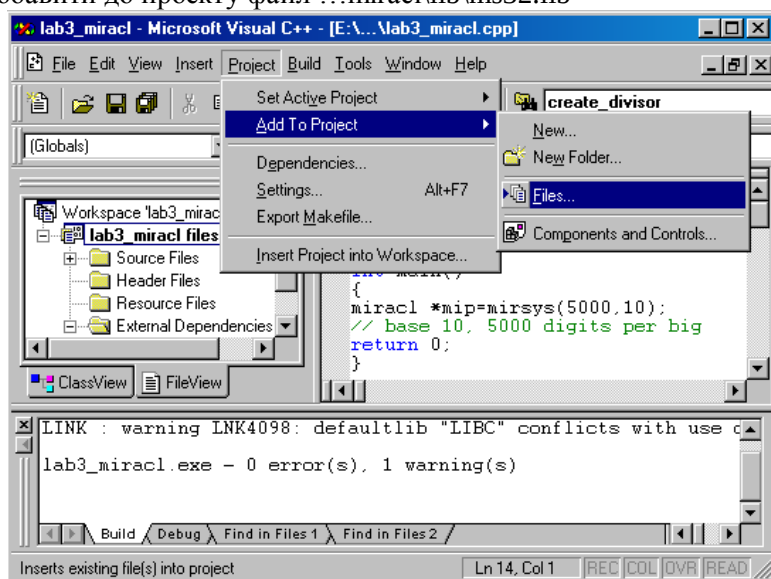


Рисунок Б.4 – Крок 4

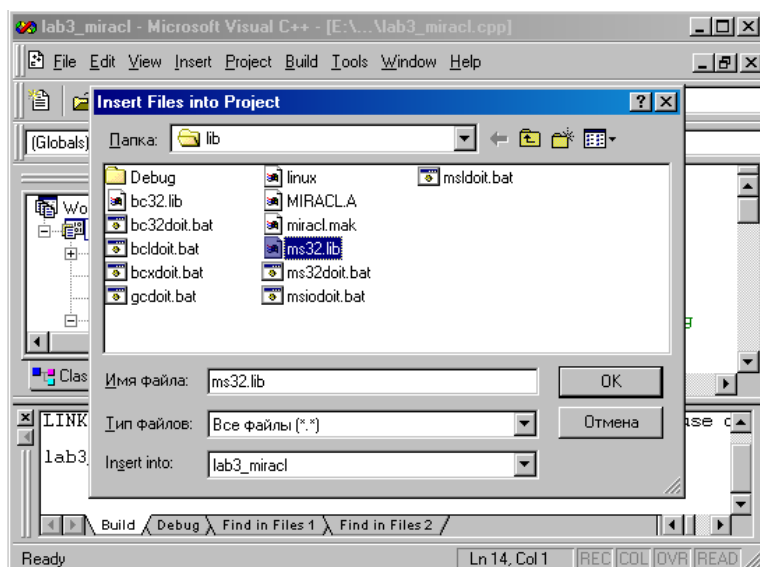


Рисунок Б.5 – Крок 5

4. Набрати програму у вікні коду.

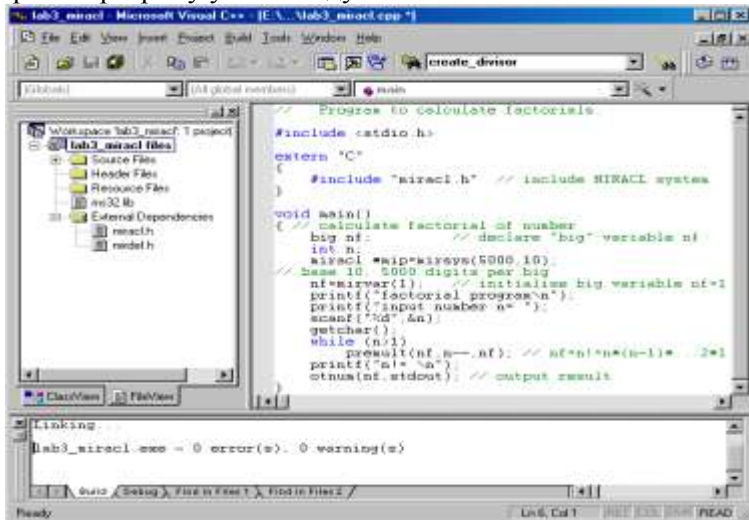


Рисунок Б.6 – Крок 6

5. Запустити проект на компіляцію та виконання.

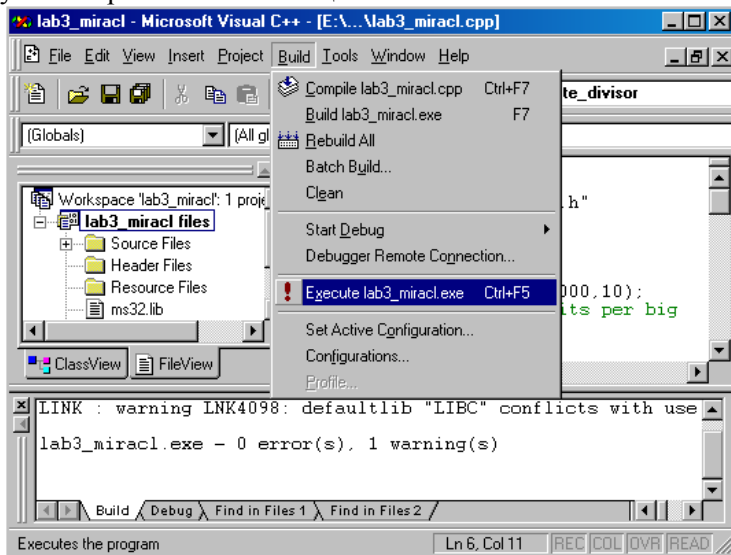


Рисунок Б.7 – Крок 7