

## Лабораторна робота № 11

Вивчення розповсюдження помилок в різних режимах роботи симетричних шифрів.

**Мета:** дослідити розповсюдження помилок в різних режимах роботи блокових симетричних шифрів.

**Обладнання:** персональний комп'ютер.

**Програмне забезпечення:** будь-яка мова програмування; криптобібліотека (фреймворк) з реалізованими основними симетричними блоковими шифрами в різних режимах роботи; програмне забезпечення “Файловый нож” або аналогічне ([http://sfg.dp.ua/page\\_soft.php?id=1613](http://sfg.dp.ua/page_soft.php?id=1613)); Нех-редактор (наприклад, WinHex).

**Література:**

1. Остапов С.Е. Основи криптографії / С.Е.Остапов, Л.О.Валь. – Чернівці : Книги-XXI, 2008. – 188 с.
2. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.
3. Кузнецов О.О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навчальний посібник / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. – Харків: Вид-во ХНЕУ, 2010. – 316 с.

### Теоретична частина

Про розповсюдження помилок в різних режимах роботи можна подивитися лекцію №7 “Режими роботи симетричних криптоалгоритмів” курсу “Криптографія та побудова систем безпеки” або у наведеній літературі.

### Завдання до лабораторної роботи

#### Спрощений варіант

1. Використовуючи програму Knife.exe, здійснити аналіз режимів шифрування ECB, CTS, CBC, CFB, OFB за поширенням помилок шифрування за варіантами табл.1.

Таблиця 1

Варіанти індивідуального завдання

Варіант	Шифр	Блоки для зміни
1	Blowfish Gost	0, 1, передостанній, останній
2	Des Gost	0, 1, передостанній, останній
3	square Gost	0, 1, передостанній, останній
4	Gost rijndael	0, 1, передостанній, останній
5	Gost twofish	0, 1, передостанній, останній
6	Gost Idea	0, 1, передостанній, останній
7	Gost Mars	0, 1, передостанній, останній
8	Gost rc6	0, 1, передостанній, останній
9	Cast 256 Gost	0, 1, передостанній, останній
10	RC5 Gost	0, 1, передостанній, останній

Варіант	Шифр	Блоки для зміни
11	Gost Q128	0, 1, передостанній, останній
12	Gost Skipjack	0, 1, передостанній, останній

2. Створіть текстовий файл, у якому повторюються перші чотири блоки відкритого тексту. Як відкритий текст оберіть своє прізвище, ім'я та по батькові.

**Приклад:** ПІБ – Петренко Іван Сергійович. При шифруванні алгоритмом Gost у режимі ECB довжина блоку перетворення дорівнює 64 бітам. Файл відкритого тексту має вигляд, представлений на рис. 1.

Програмою WinHex рекомендується скористатися для перегляду й редагування як файлів з відкритим текстом, так шифротекстів.

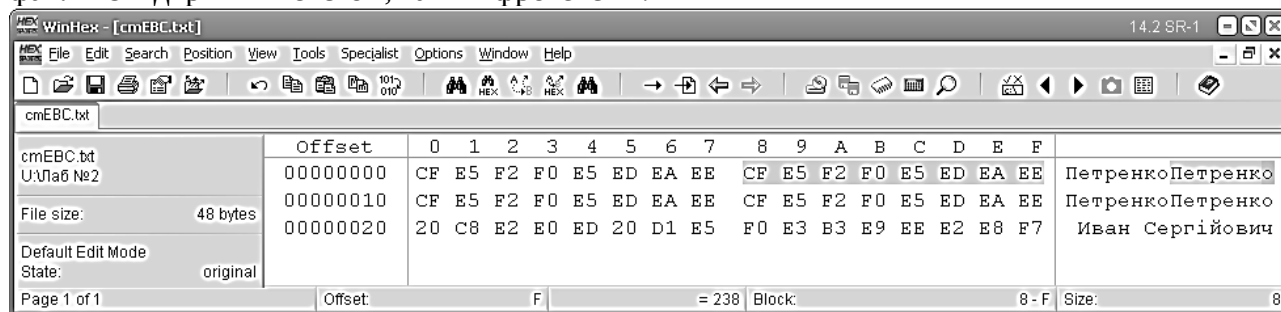


Рис. 1. Файл із відкритим текстом у режимі побайтового перегляду програми WinHex  
Інтерфейс програми knife.exe "АСе Файловый нож" представлений на рис. 2.

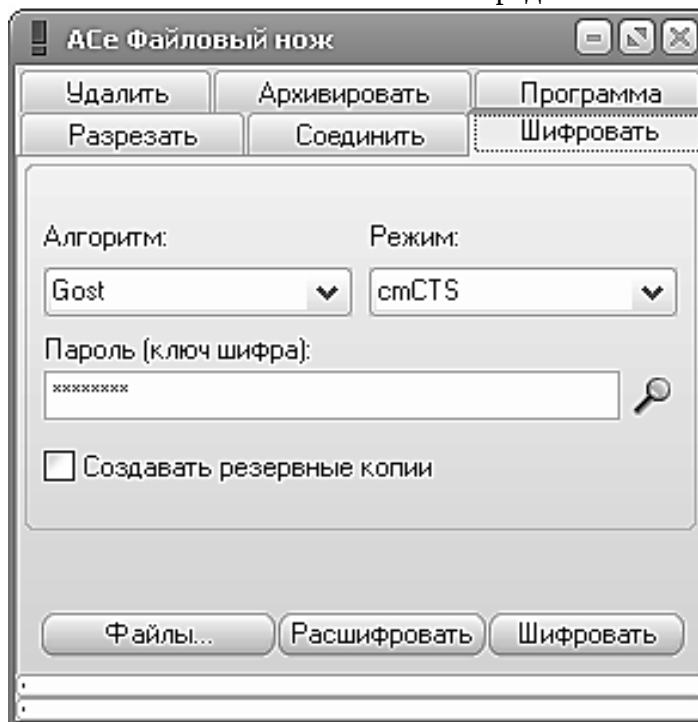


Рис. 2. "АСе файловый нож" – вікно шифрування

**Алгоритм** – вибір алгоритму шифрування;

**Режим** – вибір режиму шифрування;

**Пароль (ключ шифру)** – тут міститься будь-який текстовий рядок, на основі якого буде створений ключ шифрування;

**Створити резервну копію файлу** – залишити копію відкритого тексту до шифрування (розшифрування);

**Файли** – відкриває вікно зі списком файлів для шифрування;

**Розшифрувати** – запускає процедуру розшифрування файлів зі списку.

**Шифрувати** – запускає процедуру шифрування файлів зі списку. Необхідно пам'ятати, що при подвійному, потрійному і т. д. шифруванні, розшифрування необхідно робити також двічі, тричі й т. д. Оброблений файл буде перезаписано.

Для шифрування файлу необхідно натиснути кнопку "Файли", у результаті з'явиться вікно, показане на рис. 3, і додати необхідний файл у список.

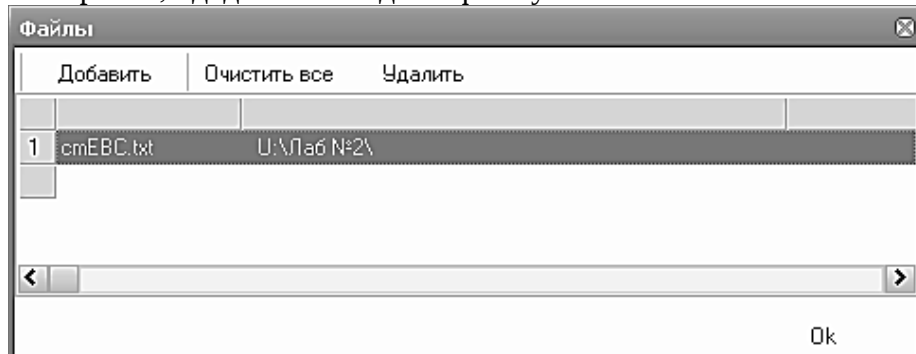



Рис. 3. Вікно додавання файлів

Далі необхідно ввести ключ шифрування. За замовчуванням в програмі використовується пароль «Password». Можна лишити його без зміни і використовувати для усіх шифрів та режимів роботи. Для перегляду ключа в текстовому вигляді натисніть на кнопку , дивись рис.4.

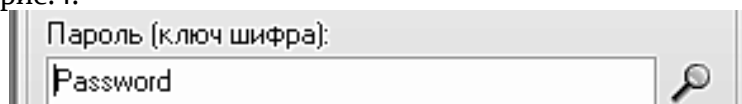


Рис 4. Подання пароля в текстовому вигляді

Для здійснення шифрування файлу натисніть однократно на кнопку "Шифрувати". Результат можна переглянути через програму WinHex (див. рис. 5).

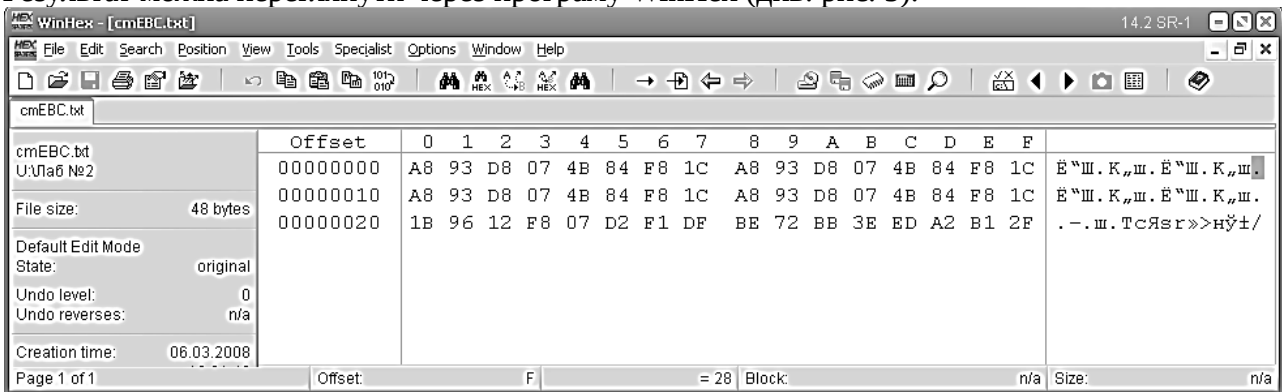


Рис. 5. Шифротекст, отриманий при використанні шифру GOST в режимі ECB з ключем "Password"

Проаналізуйте отриманий шифротекст, порівняйте його зі схемою використовуваного режиму. У режимі ECB зверніть увагу на блоки шифротексту, що повторюються, зробіть висновок. Розшифруйте отриманий шифротекст.

Для проведення аналізу поширення помилок внесемо зміни в один біт другого блоку шифротексту й збережемо зміни у файл. Це показано на рис. 6.

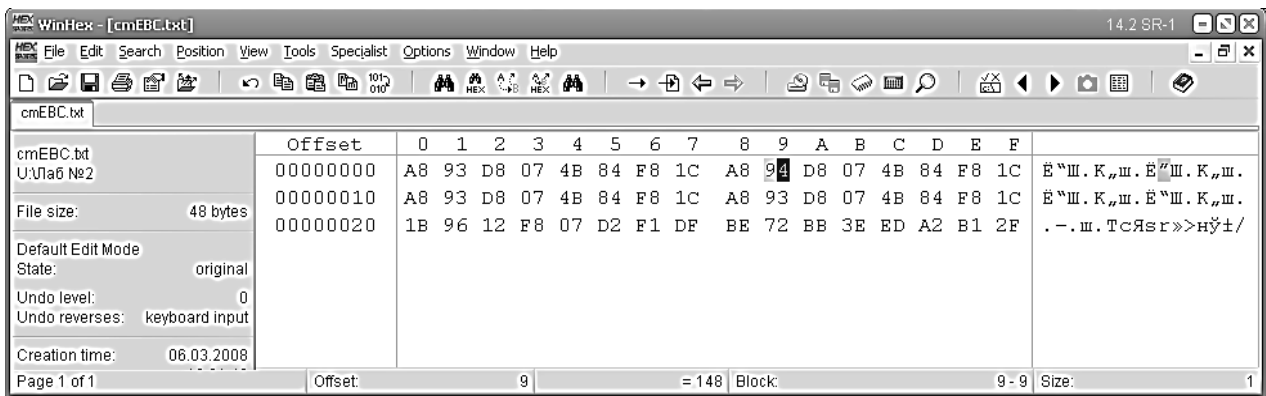


Рис. 6. Внесення помилки в другий байт другого блоку шифротексту

Тепер розшифруємо шифротекст із помилкою й проаналізуємо отриманий відкритий текст. Відкритий текст, що містить помилку, наведений на рис. 7.

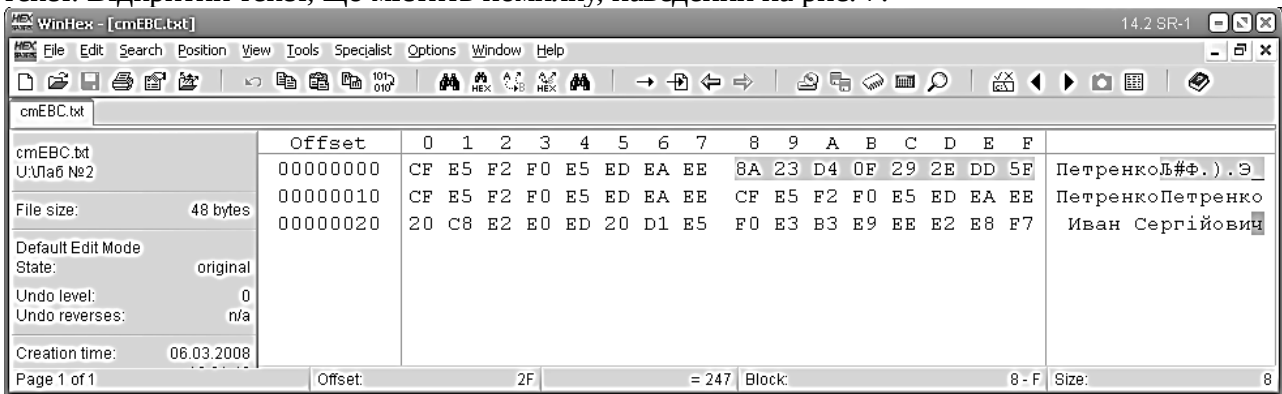


Рис. 7. Відкритий текст із помилкою

Проаналізуйте поширення помилки, порівняйте результати зі схемою режиму.

Виконайте ці кроки для всіх режимів шифрування й проаналізуйте результати. У звіт додайте скрін-шоти відкритого тексту, шифротексту, шифротексту з помилкою та відкритим текстом.

### Ускладнений варіант

1. За допомогою обраної криптобібліотеки розробіть систему шифрування для двох шифрів з Вашого завдання з використанням різних режимів шифрування (ECB, CTS, CBC, CFB, OFB) та проведіть дослідження розповсюдження помилки аналогічно тому, як це описано у спрощеному варіанті.

2. Складіть звіт з ЛР, який має містити:

- протокол Ваших дій;
- скрін-шоти відкритого тексту;
- скрін-шоти шифротексту;
- скрін-шоти тексту з помилкою та шифротексту;
- аналіз отриманих результатів.
- код програми.

3. Код має задовольняти вимоги до написання коду (наприклад, C++ Programming Style Guideline).

### Контрольні запитання

1. Охарактеризуйте алгоритми шифрування, використані у Вашому варіанті.
2. Охарактеризуйте режими роботи симетричних блокових шифрів та їх призначення.
3. Проаналізуйте результати розповсюдження помилки, отримані Вами у цій ЛР.
4. На Вашу думку, який режим роботи шифрів найменше поширює помилку?
5. Порівняйте між собою зашифровані тексти та визначте найстійкіший режим.