ВІЗУАЛІЗАЦІЯ ШИФРУВАННЯ ФАЙЛІВ БЛОЧНИМИ СИМЕТРИЧНИМИ АЛГОРИТМАМИ З ПОСИЛЕННЯМ КРИПТОСТІЙКОСТІ

Погромська Г.С.
кандидат педагогічних наук, доцент кафедри комп'ютерних наук та прикладної математики, Миколаївський національний університет імені В.О. Сухомлинського

Ключові слова: симетричні алгоритми шифрування, RC6, MARS, Rijndael, Serpent, Twofish, криптостійкість, ключ

Keywords: symmetric encryption algorithms, RC6, MARS, Rijndael, Serpent, Twofish, cryptometry, key

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Захист даних за допомогою шифрування – одне з можливих рішень проблеми їхньої безпеки. Зашифровані дані стають доступними тільки для того, хто знає, як їх розшифрувати, і тому викрадення зашифрованих даних є абсолютно безглуздим для несанкціонованих користувачів [2, 3].

Симетричні алгоритми шифрування можна розділити на потокові та блочні алгоритми шифрування. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Блочні алгоритми працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам, але деякі алгоритми відходять від цього правила [1].

Пропонована автором програма SymCript реалізує 5 алгоритмів – фіналістів конкурсу AES (Advanced Encryption Standard). Параметри алгоритмів надані у таблиці 1.

Програма працює з фіксованими параметрами: розмір ключа 128 біт, розмір блоку 128 біт.

Програма реалізує шифрування в двох режимах:

Таблиця 1
Параметри алгоритмів

Алгоритм	Розмір блока	Розмір ключа	Число раундів
RC6	змінний 128 AES)	8-256	змінне 20 AES)
MARS	128	128-1280	32
Rijndael	128, 192, 256	128, 192, 256	10, 12, 14
Serpent	128	1-256	32
Twofish	128	128, 192, 256	16

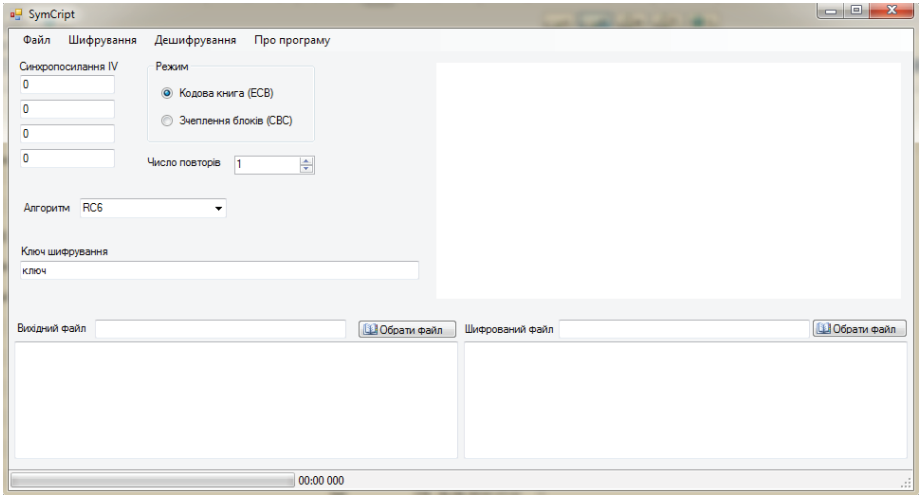

Рисунок 1 – Головне вікно програми SymCript

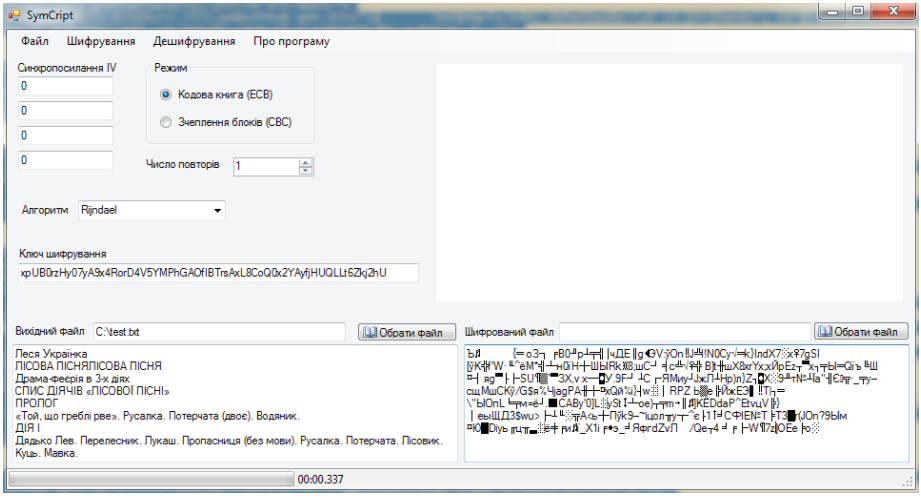

Рисунок 2 – Виконання шифрування

1. Шифрування в режимі кодової книги (ECB).

2. Шифрування в режимі зчеплення блоків шифротексту (CBC).

Програма має графічний інтерфейс, надає користувачу можливості:

1. Введення ключа, підбір ключа, вибору типу алгоритму, синхропосилання IV, вибору режиму роботи та числа повторів.

2. Вибору вхідного/ вихідного файлу.

3. Наочного відображення змісту вхідного/ вихідного файлу (в процесі шифрування/ дешифрування).

4. Відображення часу шифрування/ дешифрування у смузі прокручування (в мілісекундах).

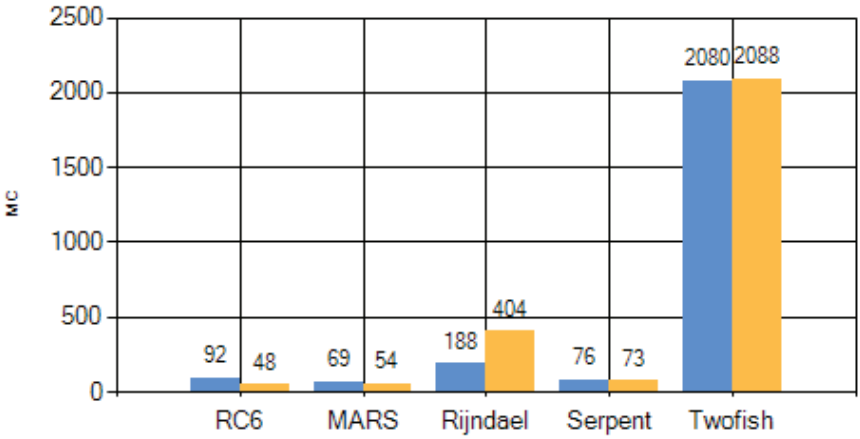

Рисунок 3 – Гістограма швидкості роботи алгоритмів

5. Візуалізації у вигляді гістограми порівняння показників роботи різних алгоритмів, тощо.

Програма SymCrypt дозволяє підсилити крипостійкість за допомогою завдання числа повторів обробки. Така схема виконана за зразком алгоритму Triple-DES. Реалізована схема EEE1 з однаковим ключем на кожному етапі обробки.

Програмний продукт SymCrypt працює в операційних системах Windows: Сімейство Windows 7 та Windows 10, сімейство Windows Server 2008 R2, сімейство Windows Vista, сімейство Windows Server 2008, ОС Microsoft Windows XP з пакетом оновлень 3 SP3). Запуск здійснюється виконанням програми SymCript.exe. Після запуску програми з'являється головне вікно (рис. 1).

Користувач може встановити необхідні параметри роботи алгоритмів:

– 4 числа вектора IV синхропосилання (гами). Крім того, користувач може згенерувати ці числа випадковим чином, обравши в головному меню пункт «Файл» – «Випадкове синхропосилання» (Ctrl+S). За замовчуванням ці числа встановлені рівними нулях.

– Обрати режим роботи – кодова книга або зчеплення блоків.

Ключ вводиться у вигляді рядка символів довільного розміру. Якщо заданий ключ коротше, ніж прийнятий в алгоритмі, він доповнюється нульовими символами. Користувач може згенерувати випадковий ключ, обравши в головному меню пункт «Файл» – «Випадковий ключ» (Ctrl+K).

Алгоритм шифрування/ дешифрування обирається в полі з вибором «Алгоритм». Поле «Число повторів» встановлює кількість циклів повної роботи алгоритму.

Користувач може зашифрувати заданий файл, обравши в головному меню пункт «Шифрування» – «Шифрувати» (Alt+E). Буде виконано шифрування і його результати відображатимуться в наступних елементах інтерфейсу (рис. 2).

Процес роботи відображається смугою прокрутки внизу вікна. Після смуги прокрутки в кінці роботи виводиться час, витрачений на операцію в секундах і мілісекундах. У текстових полях будуть відображені вміст вихідного і зашифрованого файлів.

Програма має функцію тестування всіх алгоритмів на предмет швидкості. Для цього користувач повинен обрати в головному меню «Файл» – «Тест швидкості алгоритмів». Програма виконує послідовне шифрування і дешифрування заданого файлу усіма 5-ма алгоритмами. Результати роботи відображаються в гістограмі (рис. 3).

Програма відображає час виконання шифрування (синій стовпчик) і дешифрування (помаранчевий стовпчик).

Таким чином, пропонований програмний продукт SymCript призначений для шифрування/ дешифрування файлів за допомогою 5 алгоритмів блочного симетричного шифрування (RC6, MARS, Rijndael, Serpent, Twofish). Програма дозволяє посилити крипостійкість за рахунок завдання числа повторів обробки. Така схема виконана за зразком алгоритму Triple-DES. Реалізована схема EEE1 з однаковим ключем на кожному етапі обробки.

Література:

1. Баранов В.М. Защита информации в системах и средствах иформатизации и святи. Уч. пособие. – Спб.: 1996. – 111 с.
2. Законодавство України. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» № 05/98 від 22 травня 1998 року [Електронний ресурс]. – Режим доступа: https://zakon.rada.gov.ua/laws/show/505/98 Дата звернення: 17.01.2019)
3. Погромська Г.С. Розробка програмного забезпечення моделювання атак типу SQl-ін'єкцій до баз даних // Zbiór artykułów naukowych Konferencji Miedzynarodowej NaukowoPraktycznej organizowanej dla pracowników naukowych uczelni, jednostek naukowo-badawczych «Obiecujące osiągnięci a naukowe Inżynieria i technologia» (30.09.2017) – Warszawa: Wydawca: Sp. z o.o. «Diamond trading tour», 2017. – 40 str. – S. 8–10