УДК 004.056.055

А. В. Остапенко-Боженова

ПРОГРАМНИЙ МОДУЛЬ ДЛЯ РОЗГОРТАННЯ КЛЮЧА ПСЕВДОНЕДЕТЕРМІНОВАНИХ БЛОКОВИХ ШИФРІВ

Вінницький національний технічний університет

Анотація

Розроблено програмний модуль, що дозволяє розгортати секретний ключ для визначення набору базових ознак блокових шифрів з псевдонедетермінованою послідовністю криптопримітивів.

Ключові слова: шифрування, криптологія, блоковий шифр.

Abstract

A software module has been developed to allow the deployment of a secret key to determine a set of basic features of pseudo- undetermined block ciphers

Keywords: encryption, cryptology, block cipher.

Вступ

Змінити залежність криптографічної стійкості від складності обчислень або кількості ітерацій при конструюванні сучасних симетричних блокових шифрів (СБШ) можливо шляхом застосування недетермінованих структур [1]. У роботі [2] було запропонована модель блокових шифрів, що дозволить вносити ефект недетермінованості в складові криптографічного перетворення (ПНБШ). ПНБШ, за використання простих та швидких операцій перетворення, дозволяють будувати блокові шифри підвищеної швидкості, що підтримують заданий світовими стандартами рівень криптографічної стійкості.

Одним з головних етапів формування криптографічного перетворення для блокових шифрів з псевдонедетермінованою послідовністю крипто примітивів (ПНБШ) є формування набору ознак з ключової інформації [3].

Результати дослідження

Метою створення програмного модуля є практична реалізація одного з етапів криптографічного перетворення запропонованої моделі ПНБШ [2, 3], проведення тестування з формуванням ознак для ключової інформації різного розміру.

Таким чином проектований програмний засіб має розв’язувати такі задачі:

- генерування вхідних даних (секретний ключ різної довжини 64-1024 біт);
- виділення набору ознак для побудови перетворення раунду ПНБШ;
- тестування отриманих результатів.

Вихідними результатами роботи програми є:

- « k » – набір ключів;
- «Набір ознак Q_{pb}, Q_{rb}, Q_{vp}» – визначені ключові параметри для відповідного перетворення;

Програмна реалізація даного модуля здійснена мовою Java. Дана мова є об'єктно-орієнтованою мовою програмування, що надає можливості для реалізації великої кількості особливостей, серед яких робота з графічними примітивами [4].

Програмний модуль складається із одного файлу, після запуску якого користувач може обрати необхідний функціонал, який буде виконувати застосунок (рис.1).

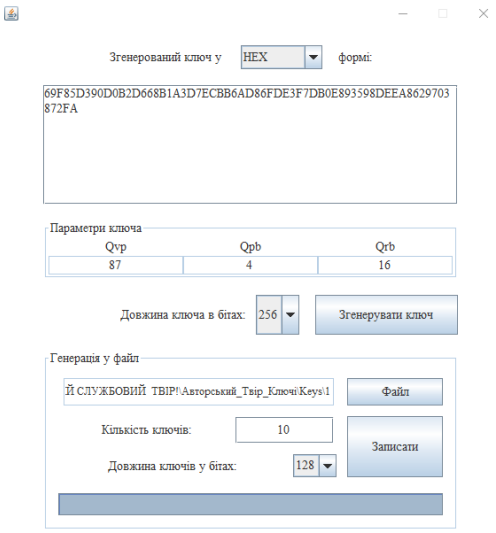

Рис. 1 – Вигляд основного вікна програмного модуля

Програмний засіб реалізує такі функцій:

– генерація ключа для демонстрації;
– генерація великої кількості ключів у обраний файл.

Функція генерації ключа для демонстрації реалізує процес відтворення ключа шифрування певної довжини та знаходження ключових ознак (параметрів).

Висновки

Було розглянуто формування ключових ознак раунду перетворення блокових шифрів для впровадження ефекту недетермінованості в процес конструювання нового виду СБШ, модель яких представлена у роботі [3].

На основі отриманих теоретичних результатів розроблено програмний модуль для генерування ключової формації, що може бути використано як базовий для програмної реалізації методів блокового шифрування з псевдонедетермінованою послідовністю криптопримітивів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Молдовян Н.А. Скоростные блочные шифры. — СПб, СПбГУ, 1998. – 212 с.
2. Лужецький В. А. Блочний шифр на основі псевдонедетермінованої послідовності криптопримітивів / Науковий вісник ВНТУ. – 2010. – №4.
   Режим доступу до ел. ресурсу: http://www.nbuv.gov.ua/e-journals/VNTU/2010_4/2010-4.htm
3. Остапенко А. В. Криптографічне перетворення ПНБШ / Тези доповідей П’ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп’ютерна інженерія» м. Івано-Франківськ, 27-29 травня 2015 року. – Івано-Франківськ: Супрун В.П., 2015. – С. 187-188.
4. Герберт Шилдт. Java. Полное руководство, 10-е издание = Java. The Complete Reference, 10th Edition. — М.: «Диалектика», 2018. — 1488 с.
5. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

Остапенко-Боженова Аліна Василівна — асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email : ostapenko-bozhenova_a_v@gmail.com

Alina Ostapenko-Bozhenova — Department of Chair Information Protection, Vinnytsia National Technical University, Vinnytsia, email : ostapenko-bozhenova_a_v@gmail.com