УДК 003.26.09:004.032.24-004.272.3
Крутих М.В. – ст. гр. СІ-41
Тернопільський національний технічний університет імені Івана Пулюя

КРИПТОАНАЛІЗ СПРОЩЕНОГО АЛГОРИТМУ AES

Науковий керівник: к.т.н, доцент Луцків А.М.

Одним з головних аспектів аудиту безпеки інформаційних систем є оцінка надійності використовуваних криптографічних алгоритмів. Криптоаналіз - наука про методи розшифрування зашифрованої інформації без призначеного для цього ключа. Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають криптографічного атакою на цей шифр. Криптографічну атаку, в ході якої вдалося розкрити шифр, називають зломом або розкриттям.

Основні методи криптоаналізу [1]:

- Атака на основі шифротексту.
- Атака на основі відкритих текстів і відповідних шифротекстів.
- Атака на основі підібраного відкритого тексту (можливість вибрати текст для шифрування).
- Атака на основі адаптивно підібраного відкритого тексту.

Advanced Encryption Standard (AES) [2], також відомий під назвою Rijndael — симетричний алгоритм блокового шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий в якості американського стандарту шифрування урядом США. AES було обрано на основі детального аналізу алгоритму вченими-криптологами, була показана його стійкість до цілої низки атак.

З точки зору криптоаналітичного дослідження доцільно розглядати спрощену версію даного алгоритму – mini-AES [3]. Цей алгоритм може бути використаний в навчальних цілях, щоб допомогти студентам, які вивчають криптографію та криптоаналіз [4], а також краще зрозуміти концепції, що лежать в звичайному алгоритмі AES.

Mini-AES - це 16-бітний блоковий шифр з 16-бітовим секретним ключем. Він складається з 2 раундів, де кожен раунд включає 4 основні операції, а саме NibbleSub, ShiftRow, iMixColumn і KeyAddition.

Для детального вивчення цього питання необхідні програмні реалізації алгоритму mini-AES і, можливо, програми для його криптоаналізу. У даний час здійснюються дослідженням цього алгоритму й ведеться розробка програмних засобів для його реалізації й криптоаналізу. Для цього використовується мова програмування Java.

Література:

1. Шнайер Б. Криптоанализ — М.: Триумф, 2002. — С. 19—22. — 816 с.

2. Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES)

3. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students - Cryptologia, XXVI (4), 2002.

4. Raphael Chung-Wei Phan, Impossible Differential Cryptanalysis of Mini-AES - Cryptologia, Vol. XXVII, No. 4, October 2003.