УДК 004.056.55:004.77:004.42
Б. Семеген, С. Лупенко, докт. техн. наук, проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АКТУАЛЬНІСТЬ РОЗРОБКИ МЕТОДІВ ПІДВИЩЕННЯ КРИПТОСТІЙКОСТІ СЛАБКИХ АЛГОРИТМІВ ШИФРУВАННЯ

UDC 004.056.55:004.77:004.42
B. Semehen, S. Lupenko, Dr.; Prof.

ACTUALITY OF DEVELOPMENT OF METHODS OF INCREASING CRYPTIC RESISTANCE OF WEAK ENCRYPTION ALGORITHMS

На даний час існує велика кількість методів криптоаналізу, які дозволяють зробити вразливими багато алгоритмів шифрування даних. Це становить загрозу конфіденційності інформації. Для збереження високого рівня захисту даних постійно розробляються все нові алгоритми шифрування із врахуванням і виправленням уразливостей, які були знайдені у попередніх алгоритмів. У сучасних комп'ютерних системах автоматизації будинків, пультів керуванням різними пристроями і інших засобах керування і передачі даних продовжують використовуватися слабкі алгоритми шифрування у зв'язку із їх простотою і оптимальністю алгоритму для забезпечення високої швидкодії у малопотужних пристроях для яких це критично важливо. Тому створення нових простих алгоритмів шифрування, або ж покращення стійкості попередніх простих алгоритмів є важливим у розвитку сучасних технологій із спрощеною архітектурою.

Для криптоаналізу поширеними є чотири типи атак на основі: тільки шифротексту, відкритого тексту, підібраного відкритого тексту, адаптивно підібраного відкритого тексту [1]. Три типи криптоаналізу із даних переліку основані на відкритому тексті кожен наступний із яких дає ширші можливості для криптоаналітика.

У зв'язку із тим, що багато шифрованих каналів передачі даних пропускають через себе дані із різних джерел, зокрема відкритих, тому виникає можливість зловмисникові виконувати передачу відомих для нього даних. Стає можливим виконувати криптоаналіз не тільки на основі відкритого тексту, а й на основі адаптивно підібраного відкритого тексту. Для каналу передачі даних який використовує слабкий алгоритм шифрування це становить особливу небезпеку.

В результаті важливою задачею для безпеки сучасних комп'ютерних систем є збільшення криптостійкості алгоритмів шифрування використовуючи методи які є ефективними по ресурсам і відповідно мають високу швидкодію. Для забезпечення підвищеної складності криптоаналізу на основі відкритого тексту важливим є добавлення певної невідомої складової до відкритого тексту, це добавляє невизначеності у шифрування і зникає відповідність між відкритим текстом та шифротекстом. Тому пропонується вводити додаткове визначене перемішування даних для кожного блоку, яке буде різним для кожного наступного блоку даних. Одним із таких є фрагментування даних на менші блоки і виконання над ними перестановки.

Література.

1. Шнайер Б. Прикладная криптография, 2-е издание: протоклы, алгоритмы и исходные тексты на языке С. – (перевод соригинла Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C (cloth) Publisher: John Wiley & Sons, Inc. Author(s): Bruce Schneier ISBN: 0471128457 Publication Date: 01/01/96).
2. Кнут, Дональд Эрвин. Искусство программирования, том 4, выпуск 2. Генерация всех кортежей и перестановок.: Пер. с английского - М.: ООО «И.Д. Вильямс», 2008. - 160 с.: ил. - Парал. тит. англ.