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

МЕТОД ПІДВИЩЕННЯ КРИПТОСТІЙКОСТІ СИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

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

METHODS OF INCREASING SYMMETRIC ENCRYPTION ALGORITHMS' CRYPTOSECURITY

Однією із найбільш поширених атак на алгоритми шифрування є атака відкритим текстом, за умови її здійсненності із подальшим криптоаналізом шифротексту для знаходження секретного ключа даного каналу передачі даних. Тому для забезпечення підвищеної криптостійкості до такого виду атак пропонується використовувати перемішування даних. У цьому разі, відкритий текст матиме подібні характеристики до невідомих даних із точки зору криптоаналізу.

У цьому методі виконується розбиття даних на підблоки і їх пересортування за спеціальним алгоритмом по наперед встановленій їх кількості, шляхом задання певного числа. Число, яке вказується для пересортування підблоків для першого блоку, генерується із гешу ключа, а для усіх наступних блоків це число генерується псевдовипадковим алгоритмом і розташовується вкінці даних попереднього блоку.

Запропонований алгоритм буде надлишковим, але підвищуватиме криптостійкість слабких алгоритмів шифрування при подачі даних опрацьованих вказаним чином.

Ускладнення атаки відкритим текстом відбувається через невизначеність позиції фрагментів відкритих даних, над якими була виконана перестановка і також, шляхом добавлення вкінці блоку певного випадкового числа, яке робить невизначеним шифротекст для одних і тих же відкритих даних блоку при їхній повторній передачі.

Зашифрований текст дешифрується у зворотному порядку, де кінцевим етапом є розстановка підблоків у правильному порядку за вказаним числом по даному алгоритму перестановки.

Описані перетворення над даними не спричинять високого навантаження на комп'ютерну систему і дозволять підвищити криптостійкість алгоритмів шифрування без втручання безпосередньо у самі алгоритми. Перетворення над даними виконується перед подачею даних у алгоритм шифрування.

Використаний метод є простим із точки зору логіки його роботи і, відповідно, програмної реалізації, тому може використовуватись як для більш потужних комп'ютерних систем, так і для малопотужних комп'ютерів у приладах низького енергоспоживання.

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.
3. R.J. Anderson, "Searching for the Optimum Correlation Attack, " K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995. to appear.