УДК 681.32

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ АЛГЕБРАЇЧНИХ ПОРІВНЯНЬ

А. В. Лужецький, д.т.н., професор
М. Л. Гаєвський, магістрант
Вінницький національний технічний університет
gaevskyy@ukr.net

Останнім часом багато вчених відходять від стандартних методів побудови блокових шифрів. Основою багатьох таких методів є використання різних теоретико числових перетворень. Основна ідея запропонованого способу шифрування полягає у виконанні обчислень з використанням матриці Уолша:

$$\mathbf{C} = (\mathbf{H} \times \mathbf{M}) \bmod m,$$
$$\mathbf{M} = (\mathbf{H} \times \mathbf{C}) \bmod m,$$

де **H** – матриця Уолша порядку N;

M – вектор відкритого повідомлення;

m – модуль;

C – вектор зашифрованого повідомлення.

Вектор відкритого повідомлення **M** складається з даних розрядністю n:

$$\mathbf{M} = \{m_1, m_2, ..., m_g\},$$

де m_i – дані розрядністю n.

У запропонованому способі існують два змінних параметри перетворення, які залежать від секретного ключа K: N – розмірність перетворень, який визначається функцією f_1(K), і n – розрядність даних, який визначається функцією f_2(K).

$$\mathrm{N} = f_1(\mathrm{K})$$
$$\mathrm{n} = f_2(\mathrm{K})$$

Розрядність блоку L дорівнює добутку розмірності перетворення та розрядності даних.

$$L = N \cdot n$$

Таким чином, розрядність блоку L також змінна величина.

Для забезпечення оптимального рівня крипостійкості та швидкості шифрування даних рекомендується виконувати 12 раундів перетворень. Розшифрування повідомлення виконується в зворотному до зашифрування порядку.

Для визначення змінних параметрів перетворення рекомендується використовувати лінійний регістр зсуву зі зворотнім зв'язком. Початковий стан регістра представляє собою секретний ключ. Оскільки стандартом AES рекомендується використовувати секретний ключ розміром не менше 128 розрядів, пропонується використовувати такий поліном для побудови лінійного регістра зсуву зі зворотнім зв'язком:

$$x^{128} + x^7 + x^2 + x + 1 = 0$$

Такий генератор випадкових чисел буде мати максимальний період:

$$T = 2^{128} - 1$$

Вихідна послідовність псевдовипадкових чисел ділиться на послідовності по 5 біт, 3 з яких визначають розмірність перетворень, а 2 – розрядність даних. Можливі варіанти розмірності перетворень такі:

2, 4, 8, 16, 32, 64, 128, 256.

Можливі варіанти розрядності даних:

8, 16, 32, 64

Перевагою швидкого перетворення Уолша є те, що його реалізація вимагає тільки операцій додавання і віднімання в кількості $N \cdot \log_2 N$, що забезпечує достатньо високу швидкість шифрування інформації.