УДК 681.32

В.А. Лужецький, А.В. Остапенко

Вінницький національний технічний університет, Вінниця

БЛОКОВИЙ ШИФР НА ОСНОВІ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ КРИПТОПРИМІТИВІВ

За підходами до реалізацій функцій шифрування виділяють блокові шифри побудовані на основі мереж Фейстеля, чергування процедур перестановок і підстановок (SP-мереж), структури «квадрат» (Square) та керованих операцій [1]. Постійно зростаючі вимоги до шифрів, врахування ними особливостей сучасної елементної бази обумовлює потребу у створенні нових підходів до реалізації блокових шифрів.

Пропонується будувати блоковий шифр використовуючи псевдовипадкову (з точки зору криптоаналітика) послідовність криптопримітивів. Ідея цього методу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень набір і послідовність виконання яких визначаються ознаками, що формуються з ключа.

З точки зору секретних систем за Шенноном [2] даний блоковий шифр можна представити як комбінацію «взваженої суми» та «добутку», тобто:

$$S=\prod_{i=1}^{n}\left(\sum_{j=1}^{m} p_{ij}\times T_{ij}\right); \quad \sum_{j=1}^{m} p_{ij}=1,$$

де T_{ij} – ij-а секретна система; p_{ij} – ймовірність вибору ij-ї секретної системи.

Основними аспектами розробки даного підходу є реалізація механізму формування ознак та створення множини базових мікроопераций. Тобто створення множини, що характеризує вигляд функції перетворення F() на певному етапі алгоритму. Тоді:

$$P_r=F_q\left(C_k,K_k\right);\ P=\{F_i,F_{i+1},\ldots,F_L\},$$

де P_r – раундові перетворення; r – кількість раундів; F_i – множина різних за виглядом функцій перетворення визначених ознакою q, (i = 1…L); C_k – зашифрований текст після r-го перетворення; K_k – раундовий ключ; r – кількість раундів.

Суть представленого методу полягає в шифруванні блоків даних змінної довжини шляхом формування ключа шифрування у вигляді множини раундових підключів, виділення з ключової інформації сукупності ознак, які визначають для поточного раунду кількість підблоків та їх розмірність, вид перетворення для їх почергового зашифрування, побудованого на основі набору базових операцій.

Загальний вигляд побудови перетворення запропонованого методу представлено на рис. 1, де K – секретний ключ; $k_1 \ldots k_R$ – раундові підключі; Q – ознаки (Q_{pb} кількість підблоків, Q_{rp} розрядність підблоку, Q_{vp} вид перетворення); **B** – множина базових операції; **M** – множина вхідних повідомлень; P_r – раундове перетворення.

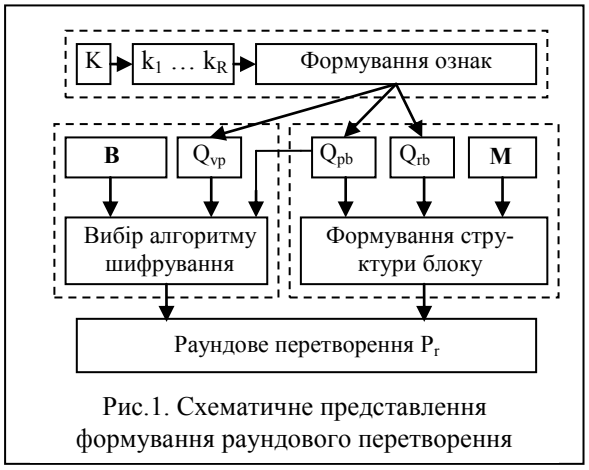

Рис.1. Схематичне представлення формування раундового перетворення

Визначений діапазон значень ознак дозволяє оперувати блоками змінної довжини розрядністю від 16 до 320 біт. Використовуючи вибрані ознаки, для одного раунду може бути побудовано 4096 різних модифікацій алгоритмів шифрування. Причому, алгоритм шифрування складається з відомих операцій, що дозволяє теоретично оцінити їх стійкість, але порядок їх застосування та структура оброблюваних ним блоків визначається секретним ключем.

Запропонована ідея використання псевдовипадкової (з точки зору криптоаналітика) послідовності криптопримітивів забезпечує додаткову стійкість блокового шифру, оскільки для його зламу необхідно аналізувати не один алгоритм, а певну їх множину.

Тому, при збереженні потрібного рівня криптостійкості можливо спростити кожен з алгоритмів, що забезпечить підвищення швидкості шифрування.

Список літератури

1. Баричев С.Г. Основы современной криптографии / С.Г. Баричев В.В. Гончаров, Р.Е Серов. – М.: Горячая линия — Телеком, 2002. — 175 с.

2. Шеннон К. Работы по теории информации и кибернетике: пер. с англ. – М.: Изд-во иностранной литературы, 1963. – 830 с.