УДК 681.3

В. Лужецький, І. Бугорська, С. Коломійчук (м. Вінниця)

ШИФРУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ

У концептуальній роботі К. Шенона, присвяченій організації секретного зв'язку, було показано, що будь-який блоковий шифр може бути побудований з використанням тільки процедур перестановок і підстановок (замін). Тривалий час у різних блокових шифрах ці процедури реалізовувалися за схемою, що називається мережею Фейстеля. Ця мережа достатньо ефективно реалізується у вигляді спеціалізованих пристроїв, але викликає певні труднощі при програмній реалізації на основі універсальних мікропроцесорів. Тому останнім часом спостерігається тенденція побудови блокових шифрів з використанням тільки арифметичних операцій, оскільки сучасні мікропроцесори найефективніше реалізують саме такі операції.

У доповіді розглядається побудова шифру на основі арифметичних операцій за модулем різних простих чисел, які є частиною секретного ключа.

Один раунд зашифрування відкритого тексту відбувається у два етапи.

Етап 1. Перестановка байтів відкритого тексту.

Відкритий текст довжиною L байтів розбивається на блоки довжиною N_0 байтів. У випадку, коли N_0 не ділить L, буде ще один блок довжиною N_1 байт, де N_1 - остача від ділення L на N_0.

Числа N_0 і N_1 представляються як сума трьох простих чисел:

$$N_0 = p_{01} + p_{02} + p_{03};$$
$$N_1 = p_{11} + p_{12} + p_{13}.$$

Далі блоки байтів розглядаються як сукупність трьох підблоків з довжинами p_{01}, p_{02}, p_{03} і p_{11}, p_{12}, p_{13}, відповідно. Якщо підблоки позначити a, b і c, то будемо мати такі варіанти розташування підблоків у межах блоку: $abc(N_S = 1)$; $acb(N_S = 2)$; $bac(N_S = 3)$; $bca(N_S = 4)$; $cab(N_S = 5)$; $cba(N_S = 6)$. Тут у дужках показано номер порядку підблоків у блоці.

Перестановки байтів у межах підблоків відбуваються за таким правилом. Якщо байт розташований на i-й позиції, то він пе-

реставляється на позицію з номером, що обчислюється за формулою:

$$j \equiv m_{ql} \cdot i \bmod p_{ql},$$

де $m_{ql} = 2 \div (p_{ql} - 1)$; $q = 0,1$ і $l = 1,2,3$.

Етап 2. Заміна кодових слів.

Текст, отриманий після перестановки байтів, розглядається як послідовність додатних 64-розрядних чисел $d_1 d_2 \ldots d_n$.

Число d_i замінюється числом Δ_i, яке обчислюється за формулою:

$$\Delta_i = d_i - d_{i-1},$$

де $i = 1 \div n$; $d_0 = k$ - частина секретного ключа.

Секретний ключ має такі складники:

$$Key = \{k, N_0, \delta, p_{01}, p_{02}, p_{03}, p_{11}, p_{12}, p_{13}, m_{01}, m_{02}, m_{03}, m_{11}, m_{12}, m_{13}, N_{S0}, N_{S1}\},$$

де N_{S0} і N_{S1} - номери порядку розташування підблоків у блоках довжини N_0 і N_1, відповідно;

δ - число, на яке збільшується N_0 для наступного раунду зашифрування.

Раунд розшифрування відбувається у такому порядку. Спочатку відновлюються кодові слова шляхом обчислення $d_i = \Delta_i + d_{i-1}$, а потім здійснюються перестановки байтів з використанням такого обчислення номера позиції:

$$j \equiv m_{ql}^{*} \cdot i \bmod p_{ql},$$

де $m_{ql}^{*} \equiv \dfrac{1}{m_{ql}} \bmod p_{ql}$.

Для забезпечення потрібної стійкості рекомендується виконувати від 1 до 5 раундів. Кожен наступний раунд починається з визначення довжини N_0 основного блоку: $N_0 := N_0 + \delta$. Потім здійснюється розкладання N_0 і N_1 на суму трьох простих чисел. Після цього визначаються m_{ql}. Якщо значення m_{ql}, що задані ключем Key, не перевищують $(p_{ql} - 1)$, то вони залишаються незмінними. Якщо деяке m_{qi} більше за $(p_{ql} - 1)$, то для нього вибирається значення, що дорівнює $(p_{ql} - 1)$.