УДК 004.056.5

МЕТОД ПОТОКОВОГО ШИФРУВАННЯ

В. А. Лужецький, д.т.н., професор,
А. В. Назимко, студент
Вінницький національний технічний університет

Потокові шифри класично використовують незалежний генератор псевдовипадкових чисел для формування гами. В результаті такого підходу злам шифру зводиться до зламу даного генератора. Генератори, що мають якісні характеристики рівномірного розподілу, зазвичай мають недостатні довжини інтервалів унікальності. Дані інтервали не дають можливості використовувати унікальні дані для гамування на всій інформації, що передається. В наслідок чого з'являється вразливість, яку використовують для зламу даного шифру

В пропонованому методі потокового шифрування відсутній незалежний генератор псевдовипадкових чисел. Формування гами відбувається на основі ключа для перших елементів даних та за визначеними правилами для наступних.

Дані, що підлягають зашифруванню, розбиваються на елементи:

$$M = m_1||m_2|| \dots ||m_l,$$

які не тільки безпосередньо зашифровуються, але й використовуються для генерування елементів гами

$$G = g_1||g_2|| \dots ||g_l.$$

Набір зашифрованих повідомлень:

$$C = c_1||c_2|| \dots ||c_l$$

одержується як результат реалізації функцій, аргументами яких є елемент повідомлення m_i та елемент гами g_i:

$$C_i = f_v(m_i, g_i)$$

Для генерування елемента гами використовуються певна кількість попередніх елементів відкритих повідомлень, яка визначається вектором *w*:

$$g_i = f_w(m_{i-1}, m_{i-2}, \dots, m_{i-h})$$

Вектор *w*, елементи $a_1, a_2 \dots a_k$ якого належать множині $\{0; 1\}$, вказує на ті елементи з множини $m_{i-1}, m_{i-2}, \dots, m_{i-k}$, що беруть участь в формування гами та відповідні операції між ними:

$$g_i = a_1 m_{i-1} * a_2 m_{i-2} * \dots * a_k m_{i-k}$$

Кожен відповідний показник a_1,a_2 … a_k вказують чи даний елемент братиме участь у відповідній операції з наступним елементом, чи, Якщо $a_j = 0$, то елемент m_{i-j} не використовується при формуванні *i*-го елемента гами.

Вектор *w* також вказує ту сукупність обернених операцій, що мають бути використані між кожною парою поряд розташованих елементів, тобто узагальнене позначення операції «*» буде обране з множини певних дозволених дій над даними.

Використання даного підходу щодо генерування та накладання гами дозволяє збільшити складність пошуку закономірностей та підвищує стійкість до злому по ключовим фразам та відомому відкритому повідомленні, оскільки такий підхід створює зав’язку даних зі способом генерування гами та їх накладанням.