УДК 681.32

БЛОКОВИЙ ШИФР НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ

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

Відомі блокові шифри реалізуються на основі сукупності арифметичних і логічних операцій та зсувів кодів. Однак найефективніше сучасні мікропроцесори реалізують арифметичні операції. Тому розробники перспективних блокових шифрів намагаються використовувати саме арифметичні операції за модулем 2^m для шифрування інформації. В доповіді розглядається побудова блокового шифру на основі арифметичних операцій за довільним модулем, який є секретним і є частиною ключів за шифрування і розшифрування.

Нехай X_0 – n-розрядний блок, тоді його зашифрування відбувається шляхом обчислень за формулою:

$$X = X_0 A \bmod m, \qquad НСД(A, m) = 1, \qquad (1)$$

а розшифрування блоку X за формулою:

$$X_0 = XA^{-1} \bmod m. \qquad (2)$$

При цьому ключ для зашифрування є конкатенацією $K=A||m$, а ключ розшифрування – $K=A^{-1}||m$.

Для забезпечення потрібної стійкості такого блокового шифру пропонується процедуру зашифрування (1) виконувати L разів ($L = \overline{2 \div (m-2)}$). Схематично процес зашифрування і розшифрування показано на рис. 1.

Якщо розрядність інформаційного блоку n_x, то розрядність коефіцієнта A доцільно обирати такою ж самою $n_x=n_A=n$, тоді розрядність модуля m має

дорівнювати $n_m=n+1$, тобто в деяких випадках зашифроване повідомлення може мати на один розряд більше порівняно з початковим блоком.

Інший підхід до побудови блокового шифру полягає в тому, що замість виконання L раундів обчислень з однаковими значеннями A і m пропонується здійснювати L раундів обчислень, в кожному з яких використовується інше значення m і A. При цьому має виконуватись умова $m_1<m_2<\ldots<m_L$. У даному випадку для кожного раунду використовується свій окремий секретний ключ $K_i = A_i||m_i$, $i = \overline{1 \div L}$. Схематично процес зашифрування і розшифрування показано на рис. 2.

Можливі варіанти формування K:

1. Якщо A_i =const, m_i = var, то $K=A||m_1||m_2||\ldots||m_L$.
2. Якщо A_i = var, m_i = const, то $K=A_1||A_2||\ldots||A_L||m$.
3. Якщо A_i = var, m_i = var, то $K=A_1||A_2||\ldots||A_L||$ $||m_1||m_2||\ldots||m_L$.

Зашифрування і розшифрування вимагає виконання L операцій множення за модулем, що значно менше порівняно з кількістю операцій, що потрібно для реалізації будь-якого відомого блокового шифру.

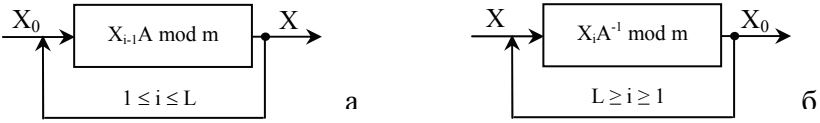

Рисунок 1 – Зашифрування A=const, m=const (а), розшифрування (б)

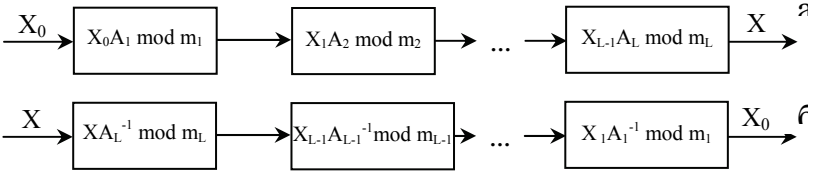

Рисунок 2 – Зашифрування A=var, m=var (а), розшифрування (б)