УДК 004.057.4

БЛОКОВИЙ ШИФР НА ОСНОВІ МЕРЕЖІ ФЕЙСТЕЛЯ

Буній Б.В.

Лагун А.Е., Львівський державний університет безпеки життєдіяльності, доцент кафедри управління інформаційною безпекою, к.т.н., доцент

У сучасному світі одним з найцінніших ресурсів є інформація, а з розвитком сучасних технологій, на забезпечення її конфіденційності потрібні затрати значних зусиль.

Одна з наук що займається забезпеченням інформації таких властивостей як конфіденційності, цілісності і автентичності є криптологія. Розвинулась вона через практичну потребу в передачі інформації в захищеному вигляді. Одним з її інструментів є шифрування. На цей час існує дуже велика кількість різновидів шифрів, проте в сучасній криптології найбільш розповсюдженими є блокові шифри, що пов'язано з особливістю обробки інформації невеликими блоками і високою швидкодією. Більшість сучасних шифрів, зокрема такі як: ГОСТ 28147-89, RC5, TEA чи CAST-256, створені на основі мережі Фейстеля та відрізняються тільки особливостями внутрішнього алгоритму [1, 2].

В процесі досліджень блокових шифрів було розроблено новий алгоритм шифрування який поєднав в собі деякі особливості інших шифрів і в той же час має перевагу в тому, що не потребує виконання операцій перестановок. Загальна схема алгоритму зображена на рис. 1.

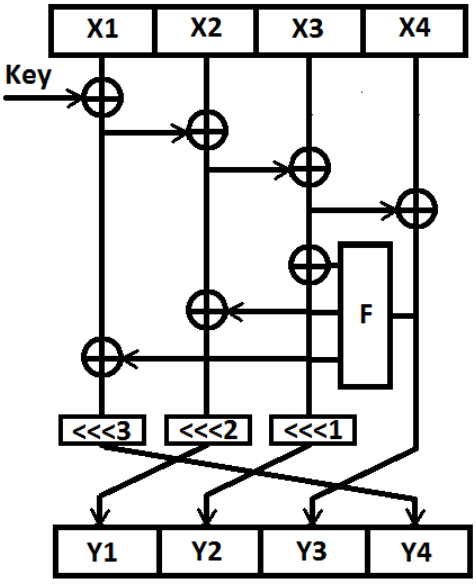

Рис. 1. Структура алгоритму розробленого шифру.

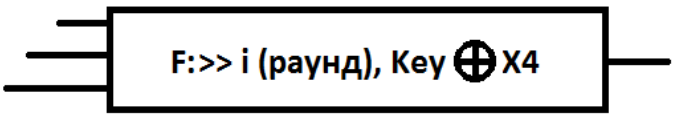

Рис. 2. Схема функції "F".

Дана операція в алгоритмі повторюється протягом 16 раундів, причому кожного разу додається раундовий ключ *Key*, що генерується автоматично для кожного раунду.

Попередньо повідомлення переводиться за ASCII таблицею в десяткові числа, які переводяться у двійкову систему числення. З отриманої послідовності бітів формуються блоки по 32 біти в кожному.

На першому етапі за лавиноподібною схемою ключ раунду додається за модулем два до першого блоку, результат в сою чергу додається до другого блоку і так аж до четвертого блоку (рис. 1). Четвертий блок разом із ключем раунду є вхідними даними для функції “F” (рис. 2), де вони додаються за модулем два, а отриманий результат зсувається на число *i* (номер раунду) вправо. Послідовність біт на виході з функції “F” додається за модулем два до решти блоків *X1, X2* та *X3*. Для цих же блоків відбувається операція зсуву бітів уліво, залежно від номеру блока: перший на три, другий на два, третій на один біт. По завершенні всіх операцій виконується кінцева перестановка блоків, результат якої подається на старт алгоритму. На останньому раунді кінцева перестановка не виконується, а зашифрований текст отримується з поточного порядку блоків.

Розроблений алгоритм було реалізовано мовою C++. Одержані результати показали ефективність процесу шифрування та розшифрування цього алгоритму. Метою подальших досліджень є визначення стійкості розробленого шифру за допомогою критеріїв, визначених в методиці NIST.

ЛІТЕРАТУРА

1. Яковлев А.В. Криптографічний захист інформації / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.М. Шанкин. – ТГТУ, 2006. – 140 с.

2. Михайленко М.С. Методи та засоби блокового симетричного шифрування з підвищеною стійкістю / М.С. Михайленко // автореферат дисертації (ДСК). – Харків. – 2008.