УДК 004.056.5

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ АЛГОРИТМУ TWOFISH

Тимошенко Л.М.[1)], Фаренюк В.О.[2)]
Одеський національний політехнічний університет
[1)] к.е.н., доцент; [2)] студент

Під час проектування систем безпеки зазвичай використовують шаблонні рішення, але вони не завжди враховують особливості кожного об'єкта, тому актуальна розробка системи, яка дозволить забезпечити надійність конфіденційної інформації для конкретної приватної структури.

В результаті виконаного в [1] аналізу зроблено висновок про те, що криптоалгоритм Twofish використовує новий підхід, при якому половина ключа використовується для зміни роботи самого алгоритму шифрування, і в цьому підалгоритмі в якості власного ключа шифрування застосовується інша половина ключа, що приводить до поділу ключа і, на думку аналітиків, підвищує стійкість алгоритму до атак [2].

Метою даної роботи є дослідження симетричного криптоалгоритму шифрування Twofish. Основними його характеристиками є довжина блоку шифрування 128 біт; допустимі довжини ключів шифрування 128, 192 і 256 біт; відсутність «слабких» ключів.

На рисунку 1 показано структурну схему роботи алгоритму Twofish, який використовує 16-раундову архітектуру Файстеля з бієктивною функцією *F* і додатковими «відбілюваннями» на вході і виході. Відмінність від «чистої» файстелевої структури в наявності функціональних блоків, що виконують циклічні однобітові зсуви вправо і вліво.

128-бітовий блок *P* відкритого тексту (16 байт $p_0,\ldots,p_{15}$) розбивається на чотири 32-бітових слова P_0, P_1, P_2 і P_3 зі збереженням прямого порядку байтів:

$$P_i = \sum_{j=0}^{3} p_{(4i+j)} \cdot 2^{8j}, \quad i = 0,\ldots,3$$

На етапі вхідного «відбілювання» виконується операція XOR між цими словами і чотирма ключами K_0, K_1, K_2, K_3:

$$R_{0,i} = P_i \oplus K_i \quad i = 0,\ldots,3$$

Після цього відбувається 16 раундів шифрування. У кожному раунді два «лівих» слова є вхідними для функцій g (біти одного з вхідних слів спочатку циклічно зсуваються на 8 позицій вліво). Для отриманих вихідних слів функції g застосовується псевдоперетворення Адамара і додаються два раундових ключі K_{2r+8} і K_{2r+9}, де *r* – номер раунду шифрування.

Далі між модифікованими в такий спосіб «лівими» словами і двома «правими» словами (біти одного з яких циклічно зсуваються на одну позицію вліво) виконується операція XOR, після чого циклічному зсуву на 1 біт вправо піддається інше з тепер вже видозмінених «правих» слів. «Ліва» і «права» пари слів потім міняються місцями для наступного раунду шифрування. Таким чином:

$$(F_{r,0}, F_{r,1}) = F(R_{r,0}, R_{r,1}, r),$$
$$R_{r+1,0} = ROR(R_{r,2} \oplus F_{r,0}, 1),$$
$$R_{r+1,1} = ROL(R_{r,3}, 1) \oplus F_{r,1},$$
$$R_{r+1,2} = R_{r,0} \ldots . R_{r+1,3} = R_{r,1}$$

де *r* = 0,…,15, а *ROR* і *ROL* - функції двох аргументів, що виконують побітовий циклічний зсув першого аргументу вправо і вліво відповідно на кількість позицій, рівну другому аргументові. Після реалізації всіх 16-ти раундів шифрування останній обмін місцями «лівої» і «правої» пар слів скасовується, і між отриманими 32-бітовими словами і ключами K_4, K_5, K_6, K_7 виконується операція XOR (етап вихідного «відбілювання»):

$$C_i = R_{16,(i+2) \bmod 4} \oplus K_{i+4}, \quad i = 0,\ldots,3$$

Отримані слова C_0, C_1, C_2, C_3 потім об'єднуються в 128-бітовий блок C шифрованого тексту:

$$c_i = \left[\frac{C_{[i/4]}}{2^{8(i \bmod 4)}} \right] \bmod 2^8, \quad i = 0,\ldots,15$$

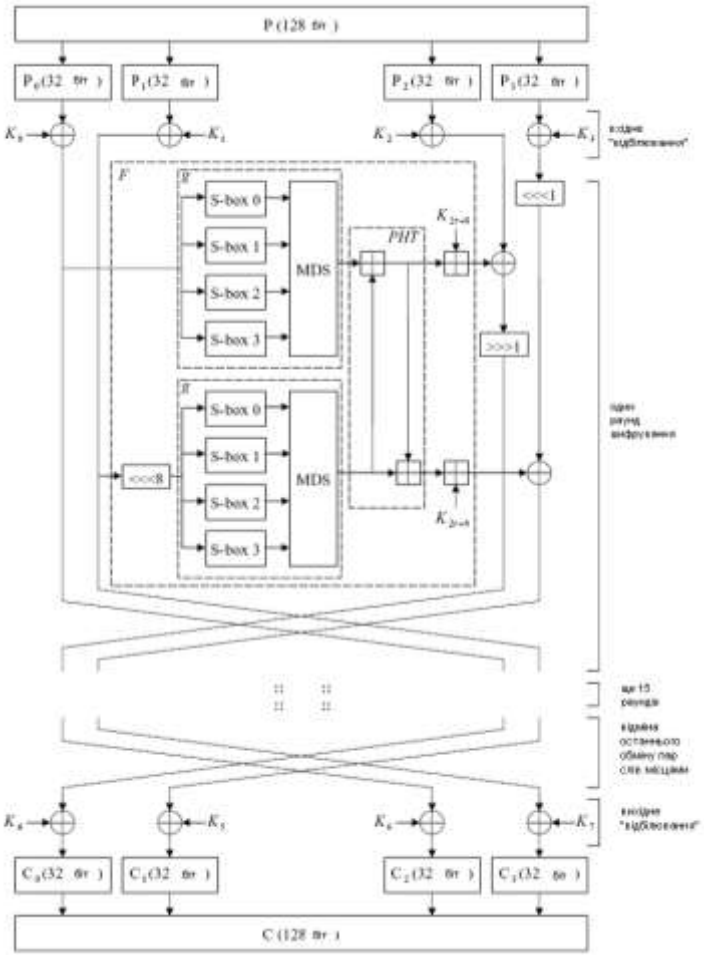

Рисунок 1 - Структура роботи алгоритму шифрування Twofish

де $[x]$ — ціла частина x. Функція F є функцією трьох аргументів: двох вхідних слів R_0, R_1 і номера раунду шифрування r, необхідного для вибору належних раундових ключів. Перетворення R_0 функцією g дає T_0. Біти R_1 спочатку циклічно зсуваються вліво на 8 позицій, далі результат перетворюється за допомогою функції g в T_1 і до T_0 і T_1 додаються два раундових ключі:

$$T_0 = g(R_0)$$
$$T_1 = g(ROL(R_1, 8))$$
$$F_0 = (T_0 + T_1 + K_{2r+8}) \bmod 2^{32}$$
$$F_1 = (T_0 + 2T_1 + K_{2r+9}) \bmod 2^{32}$$

де F_0 і F_1 - виходи функції F. Функція g є основа алгоритму шифрування. Вхідне 32-бітове слово X розбивається на 4 байти. Кожен байт проходить через відповідний S-box, що залежить від раундового ключа і описується бієктивною функцією, що перетворить «вхідний» байт у «вихідний».

В результаті для шифрування конфіденційної та приватної інформації за допомогою алгоритму Twofish був розроблений програмний комплекс, що включає засоби реалізації алгоритмів шифрування та дешифрування з використанням основних блочних режимів.

Список використаних джерел

1. E. Biham and L.R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. In K. Nyberg, editor, Advances in Cryptology — EuroCrypt'98. Springer Verlag, 1998.
2. Stinson D.R. Cryptography: Theory and Practice. – N.Y.: CRC Press Inc., 2005. – 434 p.