

СЕКЦІЯ «ЗАХИСТ ІНФОРМАЦІЇ»

УДК 004.75:339.722

Бондаренко О.О.¹, Філобок Є.В.¹, Козіна Г.Л.²

¹ студ. гр. РТ-716 НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ КИТАЙСЬКОГО СТАНДАРТУ ШИФРУВАННЯ SM4 ДЛЯ ЗАХИСТУ БЕЗДРОВОХИХ МЕРЕЖ

В даній роботі досліджено китайський стандарт шифрування для захисту бездротових мереж – алгоритм SM4 [1,2] в режимі шифрування CBC (Cipher Block Chaining). Цей режим підпорядковує розбиття відкритого тексту на блоки однакової довжини – 128 біт (рис.1). Для здійснення шифрування потрібні 128 – бітні синхропосилка та ключ відповідно.

Стандарт SM4 використовує 32 раунди для обробки одного блоку.

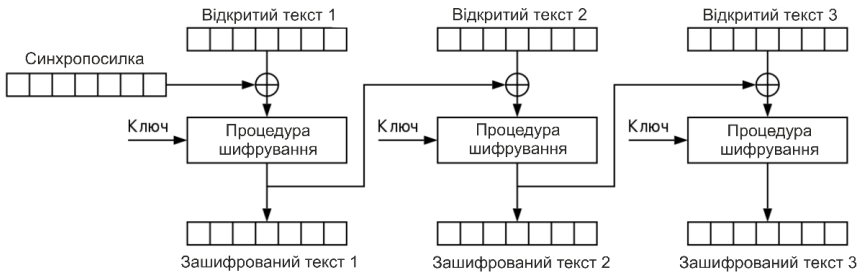


Рисунок 1 – Схема шифрування стандарту SM4 у режимі CBC

Для початку перша частина відкритого тексту складається за модулем 2 з синхропосилкою. Після цього починається процедура шифрування.

На рис. 2 зображено повний алгоритм для зашифровування одного блоку.

Вихідний блок та ключ діляться, кожен, на чотири 32 - бітних частини – «слова». Наступним етапом йде генерація раундових ключів, яка підпорядковує використання змішаної підстановки T'.

Після цього раундові ключі використовуються у процедурі шифрування. Також використовується змішана підстановка T, але з деякими відмінностями.

Алгоритм шифрування складається з 32 раундів. Відкритий 128-бітний блок даних розбивається на 4 блоки по 32 біта: (X_0, X_1, X_2, X_3) .

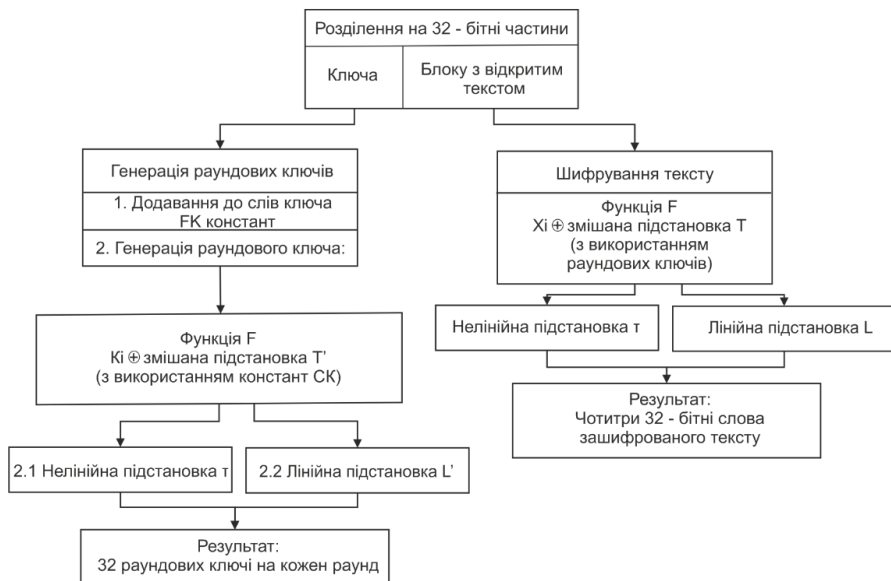


Рисунок 2 – Алгоритм шифрування стандарту SM4

Процес шифрування виконується таким чином:

$$X_{i+4} = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0, 1, \dots, 31.$$

Результатом шифрування є блок

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}).$$

Перетворення $T(\cdot)$ є суперпозицією нелінійної і лінійної заміни.

В результаті отримуємо новий зашифрований 128 - бітний блок, який надалі слугує у якості синхропосилки для другої частини відкритого тексту. Таким чином шифрується весь відкритий текст.

Для розшифрування шифртексту використовуються такі кроки.

Спочатку розшифровується перший шифрблок. Для розшифрування зашифрованого блоку відбувається той ж самий алгоритм, який відображено на рисунку 2 та в наданих формулах, але раундові ключі використовуються у зворотному напрямі. Потім для отримання першого блоку відкритого тексту результат розшифрування додається до синхропосилки.

Останні блоки розшифровуються аналогічно, тільки результат розшифрування шифрблок додається до попереднього шифрблоку.

Приклад шифрування:

Відкритий текст представлений у 16-ричній системі: 50 75 6E 69 73 68 6D 65 6E 74 20 67 69 76 65 73 .

Синхропосилка: 49 66 20 6F 6E 65 20 64 6F 65 73 20 6E 6F 74 20 .

Крок I – Складання відкритого тексту з синхропосилкою.

Результат: 19 13 4E 06 1D 0D 4D 01 01 11 53 47 07 19 11 53

Крок II – Ділення отриманого результату на чотири 32-бітні слова та генерація 32 раундових ключів.

Крок III – Проведення нелінійної підстановки T та лінійної підстановки L.

Як результат отримується 128-бітний блок зашифрованого тексту:

B2 FE 1D DA 6C D3 A3 BE CA D0 85 37 60 56 80 A4.

Слід зазначити, що оскільки в китайському стандарті використовуються тільки операції заміни, зсуву і складання по модулю 2, шифрування виконується дуже швидко.

Цей стандарт, який був відкритий в 2006 році, являє собою блискуче з'єднання переваг класичної мережі Фейстеля, яка робить однаковими алгоритми шифрування і розшифрування, і сучасних підходів, відображених в стандартах США (FIPS 197, тобто RIJNDAEL), України (ДСТУ 7624:2014) та інших.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The SM4 Block Cipher Algorithm And Its Modes Of Operations [Електронний ресурс]. – Режим доступу: <https://tools.ietf.org/id/draft-crypto-sm4-00.html#rfc.section.12>
2. SMS4 Encryption Algorithm for Wireless Networks [Електронний ресурс]. – Режим доступу: <https://eprint.iacr.org/2008/329.pdf>