УДК 004.056.055

В. А. Лужецький, д. т. н., проф.; А. В. Остапенко

БЛОЧНИЙ ШИФР НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНОЇ ПОСЛІДОВНОСТІ КРИПТОПРИМІТИВІВ

Запропоновано новий підхід до реалізації блочного шифру, який базується на використанні псевдонедетермінованих послідовностей криптопримітивів та розбитті повідомлення на блоки різної довжини на кожному з раундів перетворення.

***Ключові слова**: симетричні блочні шифри, криптографія, псевдонедетерміновані послідовності.*

Вступ

Постійно зростаючі вимоги до шифрів, врахування ними особливостей сучасної елементної бази, створення нових видів атак обумовлює потребу в розробці та дослідженні нових підходів до побудови блочних шифрів.

Відповідно до реалізацій функцій шифрування виділяють блочні шифри, побудовані на основі мереж Фейстеля (Feistel network) [1, 2, 3], чергування процедур перестановок і підстановок (SP-мереж) [1, 4, 5], структури «квадрат» (Square) [1, 6] та керованих операцій [7].

Блочні шифри на основі мережі Фейстеля мають недоліки з точки зору швидкості та простоти виконання операцій, оскільки за один раунд шифрується лише половина блоку вхідного повідомлення [8]. Використання табличних замін якісно впливає на швидкість шифрування, яке базується на SP-мережах та структурі «квадрат» (Square).

Мета роботи

Метою роботи є підвищення швидкості блочного шифрування даних при забезпеченні заданого рівня криптографічної стійкості шляхом розробки блочного шифру на основі псевдонедетермінованої послідовності криптопримітивів.

Постановка задач

Будь-який блочний шифр може бути описаний такою алгебраїчною моделлю:

$$\sum = \{\mathbf{M}, \mathbf{K}, \mathbf{C}, \mathbf{E}, \mathbf{D}\},$$

де $\mathbf{M} = \{m_j\}$ – множина відкритих повідомлень $(j = j \ldots J)$; $\mathbf{K} = \{k_i\}$ – множина ключів $(i = i \ldots I)$; $\mathbf{C} = \{c_j\}$ – множина криптограм; $\mathbf{E} = \{E_{ki}\}$ – множина алгоритмів зашифрування; $\mathbf{D} = \{D_{ki}\}$ – множина алгоритмів розшифрування.

Множина **E** утворюється відображенням **M**×**K**→**C**, при цьому E_{ki} описується функцією $F(k_i, m_j)$. Відображення **C**×**K**→**M** утворює множину **D** алгоритмів розшифрування. Окремі алгоритми розшифрування D_{ki} описуються функцією $F^{-1}(k_i, m_j)$.

Як правило, алгоритми зашифрування та розшифрування є ітераційними і складаються з послідовності R перетворень (раундів) [9]. Причому в кожному раунді перетворення використовується окремий раундовий ключ k_r, який отримується із загального секретного ключа $k \in \mathbf{K}$. Виходячи з цього, криптограма $c \in \mathbf{C}$ для відкритого повідомлення $m \in \mathbf{M}$ і ключа k одержується як результат виконання послідовності раундових перетворень:

$$c_r = F(k_r, c_{r-1}), \quad (1)$$

де c_r – зашифровані дані після r-го перетворення $\left(c_1 = m, c = c_R, r = \overline{1 \ldots R}\right)$; $F\left(k_r, c_{r-1}\right)$ – функція раундового перетворення.

Відповідно відкритий текст m для криптограми c і ключа k одержується як результат перетворення:

$$m_r = F^{-1}\left(k_r, m_{r-1}\right), \tag{2}$$

де m_r – розшифровані дані після r-го перетворення $\left(m_1 = c, m = m_R\right)$.

Алгебра секретних систем, описана в роботі К. Шеннона [9, 10], розкриває два способи комбінування секретних систем з метою отримання нової секретної системи.

Спосіб, що називається «взважена сума» складається із попереднього вибору системи T_i з деякою ймовірністю p_i. Після того як вибір зроблено, система T_i використовується відповідно до її визначення. При цьому нова система має множину відображень, вона складається із сукупності всіх множин відображення, використаних секретних систем з імовірностями їх використання, що дорівнюють добутку ймовірності вибору цих відображень та ймовірності вибору секретної системи. Тобто:

$$S = \sum_{i=1}^{n} p_i \cdot T_i, \ \sum_{i=1}^{n} p_1 = 1, \tag{3}$$

де S – комбінована секретна система; T_i – i-та секретна система з n набору секретних систем; p_i – імовірність вибору i-ої секретної системи.

Повний ключ системи S вказує на те, яка з систем використовується і з яким ключем.

Спосіб «добуток» складається з послідовного застосування секретних систем, за умови, що система T_{i+1} має область визначення (простір мови) таку, що її можна прирівняти з областю визначення (простором криптограм) системи T_i, тобто:

$$S = \prod_{i=1}^{n} T_i. \tag{4}$$

При цьому повний ключ системи S складається із ключів всіх систем, які використовуються.

Аналіз розглянутих підходів щодо побудови блочних шифрів показує, що шифри на основі мережі Фейстеля, SP-мережі, структури «квадрат» можуть бути описані як добуток секретних систем (3), при цьому T_i можна розглядати як раундові перетворення.

Блочні шифри на основі керованих операцій також можна описати добутком систем (3). У цьому випадку на кожному раунді виконуються різні перетворення з фіксованою послідовністю операцій, але із змінними параметрами операцій. Наприклад, виконання операції циклічного зсуву вправо на 3 розряди в першому раунді і на 7 розрядів у другому.

Ці перетворення описуються однією і тією ж функцією, але в якості аргументів використовуються результати попереднього перетворення і раундовий ключ. Тобто алгоритм блочного шифру є детермінованим.

Оскільки набір і послідовність виконання операцій є детермінованими, криптографічна стійкість розглянутих блочних шифрів визначається розміром ключа, складністю виконуваних операцій або кількістю раундів у разі використання простих операцій.

Для зменшення кількості раундів, а отже підвищення швидкості шифрування, у разі використання набору простих операцій, пропонується застосовувати недетерміновану послідовність операцій (з точки зору зловмисника), яка визначається секретним ключем.

Оскільки при шифруванні буде використовуватись визначений набір алгоритмів, в яких послідовність виконуваних операцій визначається ключем, тому в подальшому ці алгоритми будемо називати псевдонедетермінованими. Такий підхід до шифрування призводить до

того, що зловмиснику буде необхідно перебрати усі можливі алгоритми шифрування.

Ідея побудови блочного шифру

Пропонується будувати блочний шифр на основі використання псевдонедетермінованих алгоритмів. У загальному випадку вони складаються з набору функцій перетворень $F_1, F_2, \ldots F_L$ і операцій, які з використанням секретного ключа k формують послідовність $a(1), a(2), \ldots, a(i)$ [10].

Процедура зашифрування відкритого повідомлення m з використанням k полягає в застосуванні функцій F у порядку, що визначається послідовністю $a(i)$:

$$c = F_k(m) = F_{a(i)}(\ldots(Fa(2)(Fa(1)(m)))\ldots) \quad (5)$$

Таким чином, алгоритм шифрування на основі псевдонедетермінованих послідовностей криптопримітивів складається з відомих перетворень, що дозволяє теоретично оцінити стійкість шифру, відповідно до правила Керкоффа, але порядок їх застосування визначається секретним ключем k і тому є недетермінованим процесом з точки зору криптоаналітика.

Ідея запропонованого підходу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень (криптопримітивів), набір і послідовність виконання яких визначаються певною множиною ознак, що формуються з ключової інформації.

З точки зору секретних систем за Шенноном цей блочний шифр можна представити як комбінацію «взваженої суми» (3) та «добутку» (4), тобто:

$$S = \prod_{i=1}^{n} \left(\sum_{j=1}^{m} p_{ij} \cdot T_{ij} \right), \sum_{j=1}^{m} p_{ij} = 1.$$

Виходячи з вищевикладеного, пропонується така модель блочного шифру:

$$\sum = \{\mathbf{M}, \mathbf{K}, \mathbf{F_E}, \mathbf{F_D}, \mathbf{Q}, \mathbf{P}, \mathbf{C}\}, \quad (6)$$

де $\mathbf{M} = \{m_j\}$ – множина відкритих повідомлень; $\mathbf{K} = \{k_i\}$ – множина ключів; $\mathbf{F_E} = \{F_{Eki}\}$ – множина функцій перетворення для зашифрування; $\mathbf{F_D} = \{F_{Dki}\}$ – множина функцій перетворення для розшифрування; $\mathbf{Q} = \{q_p\}$ – множина ознак $(p = 1 \ldots P)$; $\mathbf{B} = \{b_h\}$ – множина базових операцій $(h = 1 \ldots H)$; $\mathbf{C} = \{c_j\}$ – множина криптограм.

Основними аспектами розробки запропонованого підходу є реалізація функції формування ознак **Q** та реалізація вибору базових операцій **B**.

Ознака $q \in \mathbf{Q}$ визначає певний набір операцій **B**, які складають раундову функцію F, тому перетворення на певному етапі алгоритму матиме вигляд:

$$P_r = F_q(c_q, k_r),$$

де P_r – раундове перетворення; F_q – функція раундового перетворення визначена ознакою q; c_q – інформація, що обробляється у поточному раунді.

Таким чином, алгоритм блочного шифрування **A** може бути представлений сукупністю раундових перетворень P_r, функції перетворення яких та структура оброблюваних ними даних залежать від ознак q:

$$\mathbf{A} = \{P_1, P_2, \ldots, P_R\}.$$

Процес формування ознаки перетворення передбачає виділення на кожному етапі зашифрування із ключової інформації (поточного раундового підключа k_r) таких ознак:

– кількість підблоків Q_{pb};

– розрядність підблоку Q_{rb} (біт);
– вид функції раундового перетворення Q_{vp}.

Кожна з цих ознак є якимось цілим числом у заданих межах.

Структура оброблюваного блоку для цього шифру складається з певної кількості підблоків змінної довжини. При цьому кількість блоків та їх довжина визначаються ознаками Q_{pb} та Q_{rb}. З урахуванням цього довжина блоку N_b:

$$N_b = Q_{pb} \cdot Q_{rb}.$$

На рис. 1 зображений приклад розбиття оброблюваної інформації на блоки змінної довжини.

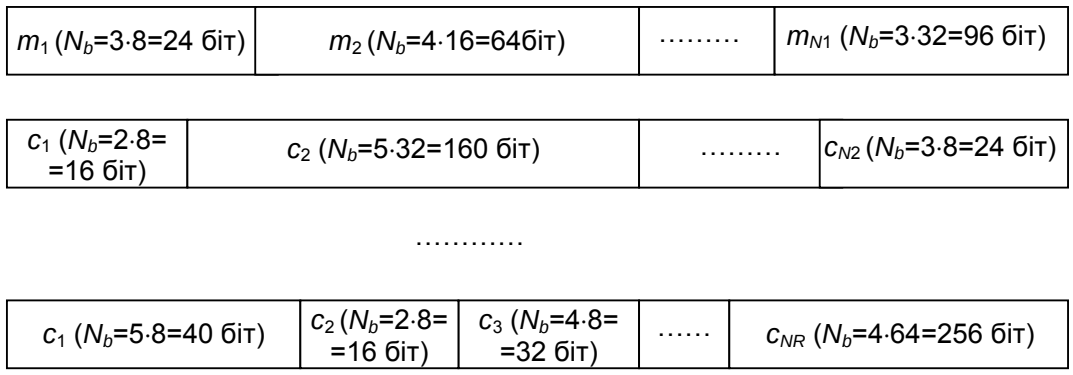


Рис. 1. Схема розбиття на блоки змінної довжини

Особливості запропонованого підходу обумовлюють велику кількість можливих модифікацій алгоритмів блочного шифрування. За допомогою обраного діапазону значень ознак може бути побудовано N_m різних алгоритмів для одного раунду перетворення:

$$N_m = Q_{pb} \cdot Q_{rb} \cdot Q_{vp}.$$

Невизначеність для зловмисника конкретної послідовності криптопримітивів у конкретному алгоритмі шифрування та велика кількість можливих модифікацій послідовностей роблять практично неможливим попереднє дослідження статистичних властивостей кожної з них, що значно ускладнює задачу криптоаналізу.

Базові операції для псевдонедетермінованого блочного шифру

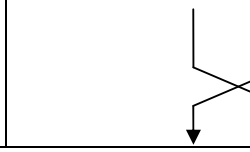
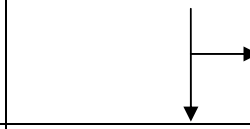
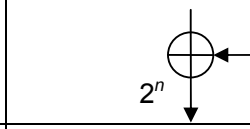
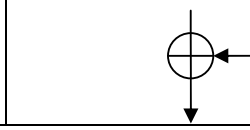
Для побудови псевдонедетермінованого алгоритму авторами пропонується множина базових операцій B, яка складається з двох видів операцій: одноопераднді та двоопераднді.

Одноопераднді операції виконуються над одним підблоком даних (циклічний зсув на k біт, інвертування, відсутність перетворення). Двоопераднді виконуються над двома підблоками даних (додавання за модулем 2, додавання за модулем 2^n, перестановка підблоків).

Схематичне позначення запропонованого набору базових операцій та їх мнемонічний опис наведено в табл. 1.

Таблиця 1

Базові операції

Назва операції	Схематичне позначення	Мнемонічне позначення
Одноопернадні операції		
Відсутність перетворення		NOP
Інвертування даних		NOT
Циклічний зсув вправо на k біт		LLC
Циклічний зсув вліво на k біт		RLC
Двоопернадні операції		
Перестановка блоків		PR
Двоопернадні лівосторонні операції		
Додавання за модулем 2^n		L^n
Додавання за модулем 2		L^2
Двоопернадні правосторонні операції		
Додавання за модулем 2^n		R^n
Додавання за модулем 2		R^2

Вищеописані операції дозволяють побудувати велику кількість криптопримітивів та їх модифікацій для оперування у блочному шифрі.

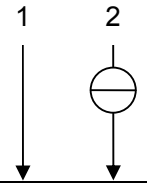
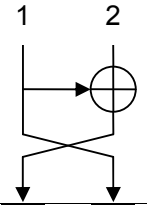
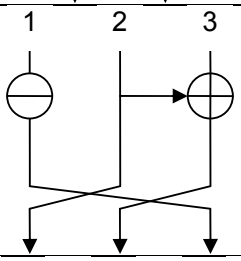
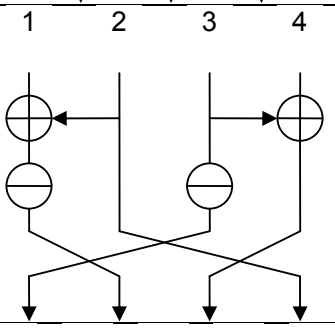
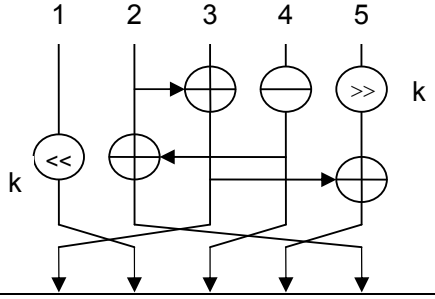
Розглянемо варіанти можливих перетворень блочного шифру з використанням представленого набору базових операцій. Для цього введемо деякі позначення:

P – перетворення; O_a – виконання одноопернандної операції над підблоком a $\left(a = 1 \ldots Q_{pb}\right)$; D_{ab} – виконання двоопернандної операції над підблоками a та b $\left(b = 1 \ldots Q_{pb}, b \rangle a\right)$; PR_{ab} – перестановка підблоків a та b; $||$ – паралельне виконання дій; $\rightarrow$ – послідовне виконання дій.

Приклади можливих перетворень для різної кількості підблоків та їх схематичний і мнемонічний опис наведені в табл. 2.

Таблиця 2

Позначення перетворень

Схематичне позначення	Мнемонічне позначення
	$P=NOP_1 \| \| NOT_2$
	$P=L^2_{12} \rightarrow PR_{12}$
	$P=(NOT_1 \| \| L^2_{23}) \rightarrow PR\ (PR_{12} \rightarrow PR_{23})$
	$P=(R^2_{12} \| \| L^2_{34}) \rightarrow$ $\rightarrow (NOT_1 \| \| NOP_2 \| \| NOT_3 \| \| NOP_4) \rightarrow$ $\rightarrow PR(PR_{23} \rightarrow PR_{12} \rightarrow PR_{32})$
	$P=(NOP_1 \| \| R^2_{23} \| \| NOT_4 \| \| RLC_5) \rightarrow$ $\rightarrow (LLC_1 \| \| L^2_{24} \| \| R^2_{35}) \rightarrow$ $\rightarrow PR\ (PR_{23} \rightarrow PR_{12} \rightarrow PR_{34} \rightarrow PR_{45})$

Отже, сформована множина базових операцій В є основою для різноманітних за структурою раундових перетворень, а запропонований мнемонічний опис операцій однозначно визначає їх будову.

Застосування вищевикладеної ідеї блочного шифру дозволяє досягти відповідного рівня криптографічної стійкості блочних шифрів з детермінованою структурою, завдяки використанню псевдонедетермінованих послідовностей криптопримітивів. Це дає можливість зменшити кількість раундів шифру R та спростити функцію раундового перетворення F, використовуючи операції, які швидко виконуються на сучасних процесорах, без втрати криптостійкості. Таким чином, досягається збільшення швидкості блочного

шифрування.

Висновки

Запропоновано новий підхід до реалізації блочного шифру, який базується на використанні псевдонедетермінованих послідовностей криптопримітивів та розбитті повідомлення на блоки різної довжини на кожному з раундів перетворення. Саме це дозволяє ускладнити процес зламу, оскільки необхідно здійснювати перебір усіх можливих комбінацій базових операцій на кожному з раундів та усіх можливих варіантів розбиття повідомлення на блоки та блоків на підблоки.

СПИСОК ЛІТЕРАТУРИ

1. Аграновский А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2002. – 256 с.

2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 346 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.: ил.

4. Kam J. Structured design of substitution-permutation encryption networks / J. Kam, G. Davida // IEEE Transactions on Computers. – 1979. – Vol. 28, №10. – P. 747.

5. Heys H. Substitution-permutation networks resistant to deferential and linear cryptanalysis / H. Heys, S. Tavares // Journal of Cryptology. – 1996. – Vol. 9, №1. – P.1 – 19.

6. Daemen J. The block cipher SQUARE / J. Daemen, V. Rijmen, L. Knudsen // Fast Software Encryption: FSE'97, Israel, January 1997 / Computer Science. Springer – Verlag. – 1997. – Vol. 1267. – P. 149 – 165.

7. Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов. / Н. А. Молдовян, А. А. Молдовян, М. А. Ефремов. – СПб.: БХВ-Петербург, 2004. – 448 с.

8. Алферов А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузмин. – М.: Гелиос АРВ, 2001. – 479 с.

9. Шеннон К. Работы по теории информации и кібернетики / К. Шеннон – М., 1963. – 829 с.

10. Адигеев М. Г. Введение в криптографію. Ч.1. Основные понятия, задачи и методы криптографии / М. Г. Адигеев. – Ростов-на-Дону: Ростовский гос. ун-т, 2002. – 35 с.

Лужецький Володимир Андрійович – д. т. н., професор, завідувач кафедри захисту інформації.

Остапенко Аліна Василівна – аспірант кафедри захисту інформації.
Вінницький національний технічний університет.