

УДК 003.26:004.056.55

А.В. Марченко, Н.В. Лукашевич, В.М. Кінзерявий
С.О. Гнатюк, к.т.н., О.В. Шевченко, к.т.н.

БЛОКОВИЙ СИМЕТРИЧНИЙ АЛГОРИТМ ШИФРУВАННЯ

Національний авіаційний університет, e-mail: icaocentre@nau.edu.ua

У даній роботі представлено блоковий симетричний алгоритм шифрування на основі мережі Файстеля. Запропонований алгоритм відноситься до галузі криптографічного захисту інформації і може бути використаний для підвищення рівня конфіденційності електронних інформаційних ресурсів.

Ключові слова: криптографія, алгоритм шифрування, криптостійкість, мережа Файстеля.

Вступ

Сучасний світ характеризується тенденцією постійного підвищення ролі інформації. З підвищенням значущості і цінності інформації, відповідно зростає і важливість її захисту. Одним із можливих способів захисту інформації при її передачі та зберіганні є криптографічний захист. На сьогодні для шифрування даних використовуються симетричні криптографічні алгоритми, розподіл секретних ключів яких виконується за допомогою асиметричної криптографії. Відомо більше десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Не дивлячись на різноманіття існуючих криптографічних алгоритмів, дослідження спрямовані розробку нових та підвищення стійкості і швидкості відомих алгоритмів, ніколи не втрачуть своєї актуальності.

Аналіз досліджень та постановка задачі

Переважна більшість сучасних алгоритмів шифрування [1-6] працюють таким чином: над даними виконується деяке перетворення за участю секретного ключа шифрування, яке повторюється певну кількість разів (раундів). При цьому, за структурою їх прийнято ділити на такі, що були побудовані на основі: мережі Файстеля, SP-мереж та структури "квадрат". В алгоритмах побудованих на мережах Файстеля, розбивається оброблюваний блок даних на кілька підблоків (найчастіше – на два), один з яких обробляється якоюсь функцією і накладається на один або кілька інших підблоків. На відміну від мережі Файстеля, SP-мережі обробляють за один раунд цілий блок даних. Для структури "квадрат" характерно представлення блоку даних у вигляді двовимірного байтового масиву. Криптографічні перетворення можуть виконуватися над окремими байтами масиву, а також над його рядками або стовпцями. На даних структурах побудовані практично всі блокові симетричні алгоритми. Використання кожної структури дає свої переваги так і недоліки. На даний момент існує велика кількість таких алгоритмів, проте практично усі вони не досконалі – або повільні або не забезпечують належної стійкості. Тому, є потреба у розробці нових більш ефективних алгоритмів шифрування.

Метою роботи є підвищення рівня конфіденційності електронних інформаційних ресурсів шляхом розробки нового перспективного блокового симетричного алгоритму шифрування. Поставлена задача вирішуються за рахунок синтезу фрагментів обчислювальних структур відомих алгоритмів шифрування RC6 та AES.

Виклад основного матеріалу дослідження

1. Термінологія та позначення. *Біт* – мінімальна одиниця кількості інформації, яка дорівнює одному двійковому розряду, який може бути рівним одному з двох значень/станів (0 або 1). *Байт* – одиниця кількості інформації (частина машинного слова), яка складається із восьми бітів, кожний з яких має свій ваговий коефіцієнт (від найбільш значущого, з коефіцієнтом 2^7 (старший біт) до найменш значущого, з коефіцієнтом 2^0 (молодший біт)). *Відкритий текст* – блок даних розміром 128 бітів (16 байтів), що підлягає зашифровуванню, а також блок даних того ж розміру після розшифровування (розміри відкритого тексту й шифротексту збігаються). *Шифротекст* – блок даних розміром 128 бітів (16 байтів) після зашифровування, або цей же блок даних, що підлягає розшифровуванню (розміри відкритого

тексту й шифротексту збігаються). *Ключ шифрування (секретний ключ, K)* – блок даних розміром 128 бітів (16 байтів), 256 бітів (32 байтів), 512 бітів (64 байтів), що використовується в якості встановлюваного секретного параметра в процедурі зашифрування або розшифрування. *Алгоритм шифрування (шифр)* – опис послідовності операцій перетворення відкритого тексту в шифротекст із застосуванням ключа шифрування, або опис відповідного зворотного перетворення. *Зашифровування* – застосування алгоритму шифрування для одержання шифротексту з відкритого тексту з використанням ключа шифрування. *Розшифрування* – застосування алгоритму шифрування для одержання відкритого тексту із шифротексту з використанням ключа шифрування. *Шифрування* – зашифровування або розшифрування. *Процедура розширення підключів* – алгоритм формування із ключа шифрування – підключів, для виконання раундових перетворень. *Підключ (K_i)* – блок даних розміром 32 біти (4 байта), що отриманий із ключа шифрування в результаті виконання процедури розширення підключів. *Раунд* – інтерактивна процедура, що здійснює перетворення робочого стану на вході процедури в поточний стан на її виході із застосуванням відповідних підключів. *Кількість раундів (r)* – кількість цифрових перетворень при шифруванні. *Таблиця підстановки* – таблиця заміни (підстановки) байтових значень, що реалізує нелінійне перетворення. \lll – циклічний по бітний зсув вліво. \ggg – циклічний по бітний зсув вправо. \ll – по бітний зсув вліво. \gg – побітний зсув вправо. $[+]$ – додавання за модулем 2^8 кожного елемента однієї матриці з кожним елементом іншої. $[\times]$ – множення двох матриць за модулем 2^8 . $[*]$ – множення кожного байту матриці на константу за модулем 2^8 .

2. Опис алгоритму. В основу запропонованого шифру був покладений алгоритм шифрування RC6, який побудований на основі мережі Файстеля. У RC6 відкритий текст розбивається на чотири 32-бітні підблоки A, B, C, D над якими виконуються наступні перетворення [2]: 1) Часткове вхідне відбілювання. Відбілюються підблоки B і D за допомогою підключів: $B = B + K_0 \bmod 2^{32}$, $D = D + K_1 \bmod 2^{32}$; 2) 20 раундових перетворень. Для кожного раунду i ($i = \overline{1, \dots, 20}$) спочатку з підблоків B і D обраховуються допоміжні 32-бітні підблоки U, T . За допомогою яких змінюють підблоки A і C , після чого до A і C додається за модулем 2^{32} значення відповідних підключів: $A = ((A \oplus T) \lll U) + K_{2i} \bmod 2^{32}$, $C = ((C \oplus U) \lll T) + K_{2i+1} \bmod 2^{32}$. У кінці раунду підблоки зсуваються: $(A, B, C, D) = (B, C, D, A)$; 3) Часткове вихідне відбілювання. Відбілюються підблоки A і C за допомогою підключів: $A = A + K_{42} \bmod 2^{32}$, $C = C + K_{43} \bmod 2^{32}$.

У запропонованому алгоритмі шифрування пропонується представляти усі підблоки A, B, C, D , допоміжні підблоки U, T та усі підключі у вигляді матриць 2×2 , після чого усі операції вже проводяться над матрицями, що певним чином нагадує AES. Змінюються процедура обчислення U, T : вводиться блок підстановок та операція множення матриці на матрицю. Також, збільшується кількість підключів раундів, тепер в кожному раунді використовується по 4 підключі. Крім того, замінені процедура розширення ключів – використовується процедура розширення ключів AES.

Представлення вхідних та вихідних даних алгоритму шифрування. До вхідних даних алгоритму належать: відкритий текст і ключ шифрування. На виході отримуємо шифротекст. Вхідні, вихідні блоки даних алгоритму представляються у вигляді чотирьох 32-бітних підблоків A, B, C, D представлених у вигляді матриць розміром 2×2 :

$$A = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \quad B = \begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} \quad C = \begin{pmatrix} C_{00} & C_{01} \\ C_{10} & C_{11} \end{pmatrix} \quad D = \begin{pmatrix} D_{00} & D_{01} \\ D_{10} & D_{11} \end{pmatrix},$$

Допоміжні підблоки U, T та усі підключі після завершення процедури розширення ключів також представляються у вигляді матриць:

$$U = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \quad T = \begin{pmatrix} T_{00} & T_{01} \\ T_{10} & T_{11} \end{pmatrix} \quad K_i = \begin{pmatrix} K_{i00} & K_{i01} \\ K_{i10} & K_{i11} \end{pmatrix}$$

Параметри алгоритму

Розмір блоку та довжина ключа шифрування. Запропонований алгоритм шифрування підтримує довжину блоку даних у 128 бітів з підтримкою ключа шифрування довжиною 128, 256, 512 бітів.

Кількість раундів шифрування. Мінімальне допустиме число раундів шифрування (r) залежить від довжини ключа шифрування. При довжині ключа 128 бітів $r = 18$, при довжині 256 бітів $r = 20$, а при довжині 512 бітів $r = 22$.

Процедура зашифрування. На вхід процедури подається підключі K_i і відкритий текст, який розбивається на підблоки (матриці) A , B , C , D . Спочатку виконується початкове відбілювання підблоків B і D . Потім виконуються r раундових перетворень. Далі виконується кінцеве відбілювання підблоків A і C . Отримані у результаті зашифрування підблоки об'єднують у шифротекст. Загальна схема алгоритму зашифрування зображена на рис. 1.

Початкове та кінцеве відбілювання. Перед початком шифрування даних підблоки B і D відбілюють за допомогою відповідних підключів: $B = (B + K_0)$, $D = (D + K_1)$. Така ж операція виконується наприкінці шифрування тільки з блоками A і C : $A = (A + K_{4r+2})$, $C = (C + K_{4r+3})$. Під даною операцією мається на увазі додавання за модулем 2^8 кожного байту вказаного підблоку з кожним байтом вказаного підключа.

У виразі (1) показано приклад додавання двох матриць:

$$(X + Y) = \begin{pmatrix} X_{00} & X_{01} \\ X_{10} & X_{11} \end{pmatrix} + \begin{pmatrix} Y_{00} & Y_{01} \\ Y_{10} & Y_{11} \end{pmatrix} = \begin{pmatrix} (X_{00} + Y_{00}) \bmod 2^8 & (X_{01} + Y_{01}) \bmod 2^8 \\ (X_{10} + Y_{10}) \bmod 2^8 & (X_{11} + Y_{11}) \bmod 2^8 \end{pmatrix} \quad (1)$$

Раундові перетворення. Для кожного раунду i ($i = \overline{1, \dots, r}$) виконується наступне:

1) Матриці B і D подаються на вхід функцій $Ft()$ і $Fu()$ відповідно. В результаті отримують матриці T і U .

2) За (1) додають за модулем 2^8 кожний байт блоків A і C з кожними байтом T і U відповідно: $A = (A + T)$, $C = (C + U)$.

3) Виконують циклічний по бітний зсув елементів матриць A і C в залежності від елементів матриць U і T : $A = (A \lll U)$, $C = (C \lll T)$.

Приклад зсуву елементів однієї матриці в залежності від елементів іншої:

$$(X \lll Y) = \begin{pmatrix} X_{00} \lll ((Y_{00} \gg 0) \bmod 2^3) & X_{01} \lll ((Y_{01} \gg 1) \bmod 2^3) \\ X_{10} \lll ((Y_{10} \gg 2) \bmod 2^3) & X_{11} \lll ((Y_{11} \gg 3) \bmod 2^3) \end{pmatrix}.$$

4) За (1) додають за модулем 2^8 кожний байт блоків A і C з кожними байтом підключів K_{4i-2} і K_{4i-1} відповідно: $A = (A + K_{4i-2})$, $C = (C + K_{4i-1})$.

5) У кінці раунду підблоки зсуваються вліво: $(A, B, C, D) = (B, C, D, A)$.

Функції $Ft()$ і $Fu()$ На рис 2. зображена схема роботи функцій $Ft()$ і $Fu()$ для i -го раунду ($i = \overline{1, \dots, r}$). Як видно вони практично однакові, за винятком підключів, які в них використовуються, та констант l , m .

Опишемо послідовність виконання функцій:

1) Кожний байт початкового значення підблоків U і T заміняють використовуючи таблицю підстановок (S -блок) (див. табл.1): $U = S(U)$, $T = S(T)$. Дана таблиця підстановок взята з алгоритму AES. Для заміни кожний байт U і T розбивають на дві частини: молодші 4 біти будуть означати необхідний стовпець, старші – необхідний рядок, їх перетин у таблиці і буде результатом. Наприклад, якщо байт який потрібно замінити $= \{53\}$, то результат заміни необхідно шукати на перетині рядка з індексом “5” та стовпця з індексом “3”, в результаті отримаємо $\{ed\}$.

2) Кожен байт U і T перемножують на розраховані для кожного раунду константи l і m за модулем 2^8 : $U = (U * m)$ і $T = (T * l)$. 3) За (1) обраховують допоміжні матриці UU і TT : $UU = (U + K_{4i+1})$, $TT = (T + K_{4i})$. 4) Перемножують матриці U і UU , T і TT : $U = (U \times UU)$, $T = (T \times TT)$ за модулем 2^8 . 5) Кожен байт U і T циклічно зсувають вліво на розраховані для кожного раунду константи l і m відповідно: $U = (U \lll l)$, $T = (T \lll m)$.

Процедура розширення підключів. Процедура розширення ключів взята з алгоритму шифрування AES [2]. Тільки з одним доповненням – кожен 32-бітне слово (підключ), після завершення процедури, представляють у вигляді матриці: $K_i = \begin{pmatrix} K_{i00} & K_{i01} \\ K_{i10} & K_{i11} \end{pmatrix}$.

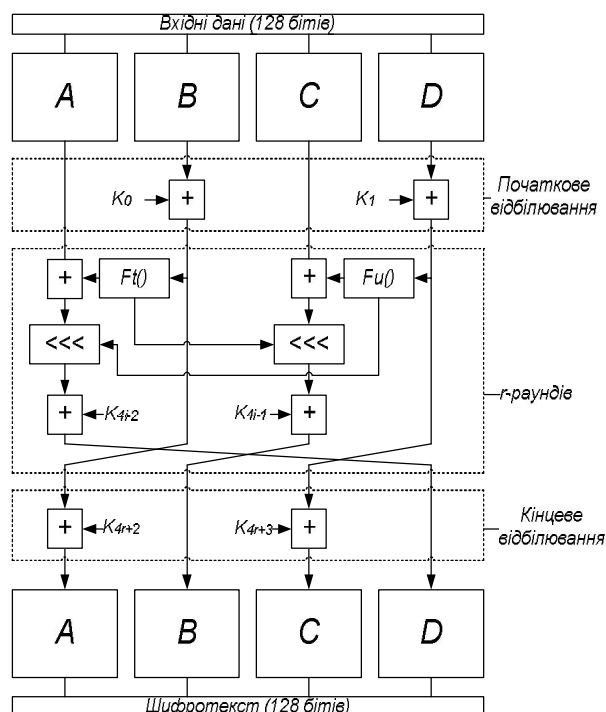


Рис. 1 Загальна схема роботи процедури зашифрування

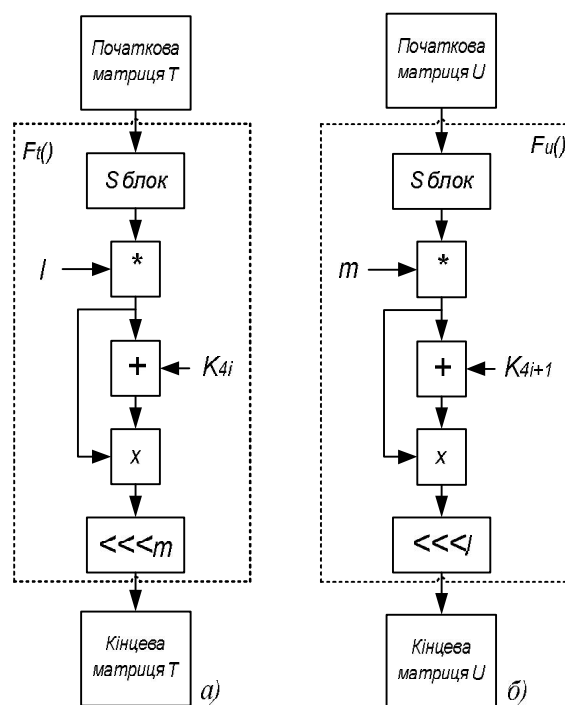


Рис.2 Для i -ого раунду функції:
а) $F_t()$; б) $F_u()$

Розрахунок констант l і m для кожного раунду. Для i -ого раунду l і m розраховуються так:

$$l = (((K_{(4*i-2)00} * K_{(4*i-1)11}) \bmod 2^8) >> 1) \bmod 2^4 + 2,$$

$$m = (((K_{(4*i-2)01} * K_{(4*i-1)10}) \bmod 2^8) >> 4) \bmod 2^4 + 2.$$

Процедура розшифрування

Розшифрування відбувається за оберненою схемою алгоритму зашифрування, тільки підключі подаються у зворотному порядку.

Висновки. У роботі наведено опис перспективного блокового симетричного алгоритму шифрування, що побудований на основі синтезу фрагментів обчислювальних структур відомих і надійних алгоритмів шифрування RC6 та AES. Даний алгоритм може бути застосований для підвищення рівня захищеності (конфіденційності) електронних інформаційних ресурсів при їх передачі інформаційно-комунікаційними системами та мережами.

Список літературних джерел

1. Мао В. Современная криптография: Теория и практика / Венбо Мао. — М.: Издательский дом «Вильямс», 2005. — 768 с.
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. — СПб.: БХВ-Петербург, 2009 — 576 с.
3. Шнайер Б. Практическая криптография / Н. Фергюсон, Б. Шнайер. - М.: Вильямс, 2005. - 425 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М.: Триумф, 2002. — 816 с.
5. Сушко С.О. Математичні основи криптоаналізу: навч. посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Кораблев. —Д.: Національний гірничий університет, 2010. — 465 с.
6. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — М.: Горячая линия – Телеком, 2002. — 175 с.

Таблиця 1															
Таблиця підстановок															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b
a	0e	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b
d	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb