УДК 004.056.55; 004.051

В. Яковина, О. Одуха, М. Сенів, О. Білас
Національний університет “Львівська політехніка”,
кафедра програмного забезпечення

ДОСЛІДЖЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК АЛГОРИТМУ СИМЕТРИЧНОГО ШИФРУВАННЯ RC5 ДЛЯ ПОБУДОВИ МОДУЛЯ ЗАХИСТУ РОЗПОДІЛЕНОЇ СИСТЕМИ ТЕПЛОВОГО ПРОЕКТУВАННЯ

Досліджено швидкість програмної реалізації та характеристик дифузії та конфузії алгоритму RC5. Показано, що дифузійні характеристики алгоритму RC5-32/12/16 практично відповідають сильному лавинному критерію і мають статистично однорідний розподіл. Швидкість шифрування на процесорі AMD Athlon X2 5000+ становить 212,77±0,01 Мбайт/с. Подано рекомендації щодо ефективності застосування цього алгоритму для побудови підсистеми захисту інформації у розподіленому комплексі теплового проектування.

The studies of software performance as well as diffusion and confusion characteristics RC5 algorithm have been performed. It is shown that the diffusion characteristics of RC5-32/12/16 algorithm almost satisfy the strict avalanche criterion and are uniformly distributed. The encryption velocity at AMD Athlon X2 5000+ processor is 212.77±0.01 Mbytes/s. The recommendations concerning effective usage of this algorithm for creating information security module of distributed thermal design system are given.

Вступ

Засоби захисту інформації часто використовують фізичні або криптографічні механізми. За криптографічним підходом можна лінійно упорядкувати способи захисту за складністю найкращих відомих алгоритмів злому у межах заданої моделі порушника. Таке впорядкування дає змогу порівнювати варіанти захисту і вибирати якнайкращий. Фізичні підходи зазвичай цього не допускають. Отже, безпеку інформаційної системи (у межах нетривіальної моделі порушника) можна гарантувати, якщо завдання порушення безпеки розв'язується алгоритмом, складність якого настільки велика, що реалізувати його практично неможливо [1, 2]. Вивченням таких засобів захисту і займається криптографія. Перевагами криптографічних засобів захисту інформації порівняно з іншими є:

- еквівалентність або зведеність загрози до математичної задачі, що дає змогу довести безпеку інформаційної системи за умови, що вказана задача є складною;
- можливість прогнозування безпеки інформаційної системи;
- можливість порівняння однотипних засобів захисту інформації, що забезпечують захист від одних і тих самих загроз, і вибору найкращого варіанта.

Криптографія пов'язана з різними галузями математики (алгебра, теорія чисел, теорія імовірності, теорія складності, обчислювальна математика та ін.), з теорією зв'язку, а також з численними технічними дисциплінами, що створюють фундамент для побудови апаратури та програмного забезпечення захисту даних і злому шифрів.

При побудові будь-якої розподіленої інформаційної системи і системи теплового проектування електронних пристроїв зокрема необхідно забезпечити такі сервіси безпеки, як конфіденційність, цілісність, аутентифікація, неповторюваність і коректність даних, ідентифікація суб'єкта інформаційної системи тощо. Усі ці сервіси безпеки забезпечує криптографічний захист інформації за допомогою таких механізмів, як алгоритми симетричного шифрування, алгоритми шифрування з

відкритим ключем, алгоритми хешування та алгоритми генерування псевдовипадкових чисел. У попередніх роботах [3, 4] було проаналізовано і досліджено алгоритми для створення послідовностей псевдовипадкових чисел для успішного функціонування криптографічних протоколів модуля захисту інформації системи розподілення обчислень для задач теплового проектування електронних пристроїв нового покоління. У цій статті розглядаються питання забезпечення конфіденційності даних за допомогою алгоритмів симетричного блокового шифрування. Сьогодні існує багато ряд алгоритмів симетричного блокового шифрування, які широко використовуються при побудові програмних комплексів захисту інформації, зокрема стандарт шифрування РФ ГОСТ 28147–89, стандарт шифрування США AES (Rijndael), алгоритми Blowfish, RC5 та ін. Однак основні характеристики цих алгоритмів, такі як дифузія, конфузія та швидкість програмної реалізації на сучасних платформах, що впливають на ступінь їхньої захищеності та реальні експлуатаційні властивості програмних продуктів на їх основі, залишаються недостатньо дослідженими.

Отже, метою цієї роботи було експериментальне дослідження характеристик дифузії та конфузії, а також швидкодії програмної реалізації алгоритму RC5-32/12/16 з метою дослідження його криптостійкості та придатності для забезпечення конфіденційності інформації в системі розподілення обчислень для задач теплового проектування.

Опис алгоритму та методики дослідження

Криптографічний захист даних забезпечується їх перетворенням, яке може бути представлене функцією з множини входів в множину виходів. Ця функція може бути як оборотною, так і необоротною. Крім того, вона може залежати від змінного параметра – ключа, який зазвичай буває секретним. Така функція називається криптографічним примітивом.

Здатність криптографічного примітиву протистояти атакам називається стійкістю. Порушення інформаційної безпеки, забезпечуваної криптографічним примітивом, називається його розкриттям, або зломом. Криптографічний алгоритм (криптоалгоритм) – це алгоритм, що реалізовує криптографічний примітив. Під стійкістю криптоалгоритму розуміють стійкість відповідного криптографічного примітива [1].

Симетричним шифром називають сукупність взаємно однозначних перетворень множини відкритих даних в множину зашифрованих даних, здійснюваних за певними правилами за допомогою секретного змінного параметра – ключа, причому знання ключа на передавальному боці дає змогу обчислити ключ на приймальному, і навпаки [1]. Якщо шифр здійснює оборотне відображення слів фіксованої довжини n біт в слова фіксованої довжини m біт, то цей шифр називають блоковим, а число n – довжиною блоку. Щоб можна було оборотним чином зашифрувати будь-яке слово довжини n біт, необхідно виконати нерівність $m>n$. До блокових належать шифри RC5, ГОСТ 28147-89, Rijndael та ін. Часто блоковий шифр реалізується послідовним виконанням нескладних процедур, що передбачають додавання блоку тексту з блоком ключа, підстановку (заміну) слів тексту, перестановку або зсув і т.п. Послідовність цих процедур зазвичай чергується. Одиничне повторення процедур, що чергуються, називається ітерацією, або циклом *шифрування*. *Ітерованим* називають симетричний блоковий шифр, одержаний шляхом виконання декількох ітерацій (циклів шифрування), як правило, однакових або дещо відмінних. Кожна ітерація містить набір нескладних оборотних операцій перетворення шифрованого тексту.

Вважають, що наукова криптографія починається з доповіді К. Шеннона "Математична теорія криптографії", представленої в 1945 р., яка пізніше була викладена у його статті [5]. Секретною системою (або просто системою) Шеннон називає скінченну множину взаємно однозначних відображень множини відкритих текстів (повідомлень) в множину шифрограм. Вид відображення повністю визначається способом шифрування і ключем.

Шифр T, що визначається ключем i, позначається T_i. Чистим називається шифр, у якого для будь-яких трьох ключів i, j, k існує такий ключ l, що $T_i T_j^{-1} T_k = T_l$ і всі ключі рівноімовірні, інакше шифр називається змішаним [5]. У чистому шифрі множини відкритих текстів, як і множина зашифрованих текстів, розпадаються на такі непересічні підмножини (області транзитивності), що

цей відкритий текст може бути перетворений на будь-який з текстів, що знаходяться в області транзитивності, вибором відповідного ключа. При повному переборі ключів кожен елемент даної підмножини відкритих текстів може бути переведений в будь-який елемент відповідної підмножини зашифрованих текстів такої ж потужності. При цьому кількість ключів, що переводять будь-який відкритий текст з цієї підмножини у кожний з елементів підмножини зашифрованих текстів, є однаковою для всіх відкритих текстів і є дільником потужності множини ключів.

Секретна система називається досконалою, якщо зашифрований текст не надає жодної інформації про відкритий текст [5]. Якщо *P(X)* – апріорна імовірність відкритого тексту *X* і *P(X|Y)* – умовна імовірність того, що шифрограмі *Y* відповідає відкритий текст *X*, то досконала система задається рівністю $P(X) = P(X \mid Y)$. Ця рівність еквівалентна рівності $P(Y) = P(Y \mid X)$ для шифрограм, де *P(Y)* – апріорна імовірність шифрограми *Y* і *P(Y|X)* – умовна імовірність того, що шифрограма *Y* відповідає відкритому тексту *X*. У досконалій системі кількість ключів повинна бути кратною кількості відкритих текстів, а кожен відкритий текст повинен переводитись у кожен зашифрований текст однією і тією самою кількістю ключів. Наприклад, якщо чистий шифр містить єдину область транзитивності, то він є досконалим.

Природні мови володіють надлишковістю, в них не всі відкриті тексти є рівноймовірними, що дає змогу ввести до розгляду умовну ентропію. Ненадійністю ключа називається умовна ентропія H(K|Y) ключа K при відомій шифрограмі Y, ненадійністю повідомлення – умовна ентропія H(X|Y) відкритого тексту X при відомій шифрограмі Y. Ці ентропії визначаються так [5]:

$$H(K \mid Y) = \sum_{Y,K} P(Y,K) \log P(K \mid Y),$$

$$H(X \mid Y) = \sum_{Y,X} P(Y,X) \log P(X \mid Y),$$

де *P(Y,K)* – імовірність появи ключа *K* і шифрограми *Y* при заданому розподілі ймовірності відкритих текстів, *P(K|Y)* – імовірність того, що для ключа *K* з'явилася шифрограма *Y* при заданому розподілі ймовірності відкритих текстів.

Якщо мова володіє нульовою надлишковістю (всі символи рівноімовірні, всі слова заданої довжини рівноімовірні і т. п.), то ненадійність ключа і повідомлення не залежить від довжини шифрограми, відомої порушнику. Такі секретні системи називаються ідеальними. Якщо порушник знає тільки шифрограми, то розкрити ключ ідеальної системи він не може. Для того, щоб система наблизилася до ідеальної, треба максимально зменшити надлишковість мови.

Деякі методи криптоаналізу, наприклад, частотний метод аналізу моноалфавітної підстановки, засновані на використанні надлишковості відкритих текстів, яка визначається статистичними властивостями шифрограм. Розглядаючи статистичні методи криптоаналізу, Шеннон приписує кожній статистиці S (набору шифрограм) деяку "роздільну потужність". Нехай H(K|S) – ненадійність ключа при статистиці S. Зважене середнє $\sum P(S) H(K \mid S)$ (сума береться за всіма шифрограмами) дає середню ненадійність ключа при відомому S. "Роздільною потужністю" статистики S називається різниця $H(K) - \sum P(S) H(K \mid S)$. Для протистояння статистичному криптоаналізу Шеннон пропонує в шифрі забезпечити розсіювання (дифузію, diffusion) і перемішування (конфузію, confusion). При розсіюванні статистична структура відкритих текстів, що приводить до надмірності шифрограм, "розпилюється" по шифрограмам великої довжини, в результаті статистика стає важкообчислюваною. При перемішуванні співвідношення між простими статистиками в множині шифрограм і простими підмножинами в множині ключів стають складними і безладними.

Отже, бажаною властивістю будь-якого алгоритму шифрування повинна бути висока чутливість результату до зміни початкових даних [6, 7] – будь-які малі зміни відкритого тексту чи ключа повинні приводити до значних змін у шифрованому тексті (лавинний ефект). Зокрема, зміна значення одного біта відкритого тексту чи ключа має спричиняти зміну значень багатьох бітів шифрованого тексту. Аналогічний сильніший критерій [8], що називається строгим критерієм

лавинного ефекту (SAC – strict avalanche criterion), вимагає, щоб для будь-яких *i* та *j* при інвертуванні вхідного біта *i* будь-який вихідний біт *j* змінювався з імовірністю ½.

RC5 – це алгоритм симетричного шифрування, розроблений Роном Райвестом у середині 90-х років [9]. Перевагами алгоритму RC5 порівняно з іншими сучасними алгоритмами симетричного блокового шифрування є:

- Придатність для апаратної та програмної реалізації. У RC5 використовуються тільки елементарні обчислювальні операції, які зазвичай застосовуються в мікропроцесорах.
- Швидкість виконання. RC5 є простим алгоритмом, що працює з даними розміром в машинне слово. Усі основні операції передбачають також роботу з даними довжиною в слово.
- Адаптованість до процесорів з різною довжиною слова. Довжина слова в бітах є параметром RC5 – із зміною довжини слова змінюється сам алгоритм.
- Змінна кількість раундів. Кількість раундів є другим параметром RC5. Цей параметр дає змогу вибрати оптимальне співвідношення необхідної швидкості роботи і вимог до ступеня захисту.
- Змінна довжина ключа. Довжина ключа є третім параметром RC5. Як і в попередньому випадку, цей параметр дає змогу знайти прийнятний компроміс між швидкістю роботи та необхідним рівнем безпеки.
- Простота. Структура RC5 дуже проста не тільки для реалізації, але й для оцінки її криптоаналітичної стійкості.
- Низькі вимоги до пам'яті. Низькі вимоги до пам'яті роблять RC5 придатним для використання в смарт-картах та інших подібних пристроях з обмеженим об'ємом пам'яті.
- Високий ступінь захисту. RC5 покликаний забезпечити високий ступінь захисту за умови вибору відповідних значень параметрів.
- Залежність циклічних зсувів від даних. В RC5 використовуються циклічні зсуви, величина яких залежить від даних, що повинно підвищувати криптоаналітичну стійкість алгоритму.

Алгоритм RC5 вбудований в багатьох основних продуктах компанії RSA Data Security Inc., зокрема BSAFE, JSAFE та S/MAIL. RC5 фактично являє собою родину алгоритмів шифрування, що визначається трьома такими параметрами (табл. 1).

Тобто, RC5 шифрує блоки відкритого тексту довжиною 32, 64 чи 128 бітів в блоки шифрованого тексту тієї самої довжини. Довжина ключа може змінюватись від 0 до 2040 бітів. Конкретна версія RC5 позначається RC5-*w*/*r*/*b*. Наприклад, RC5-32/12/16 використовує 32-бітові слова (64-бітові блоки відкритого і шифрованого тексту), 12 раундів шифрування і ключ довжиною 16 байтів (128 бітів). Райвест пропонує використовувати RC5-32/12/16 як "стандартну" версію RC5.

Таблиця 1

Параметри алгоритму RC5

Параметр	Визначення	Допустимі значення
w	Розмір слова в бітах. Довжина блока становить 2 слова	16, 32, 64
r	Кількість раундів	0, 1 … 255
b	Кількість 8-бітових байтів (октетів) в таємному ключі *K*	0, 1 … 255

В алгоритмі RC5 виконуються три елементарні операції (а також обернені до них):

- Додавання. Додавання слів виконується за модулем 2^w. Оберненою операцією є віднімання за модулем 2^w.
- Побітове виключне АБО.
- Циклічний зсув ліворуч. В алгоритмі використовується циклічний зсув слова *x* ліворуч на *y* бітів, оберненою операцією є циклічний зсув слова *x* праворуч на *y* бітів.

Двома найбважливішими особливостями RC5 є простота алгоритму та використання керованих даними циклічних зсувів. Циклічні зсуви – єдина нелінійна складова цього алгоритму. Райвест стверджує [9], що у зв'язку з тим, що величина зсуву визначається даними, що обробляються алгоритмом, лінійний та диференційний криптоаналіз алгоритму буде серйозно утруднений.

Для ефективного використання RC5 у неоднорідному середовищі специфікація RFC 2040 [10] визначає чотири різні режими роботи цього алгоритму.

- Блоковий шифр RC5. Алгоритм прямого шифрування, при якому береться блок даних заданого розміру (2^w бітів) і з нього за допомогою залежного від ключа перетворення генерується блок шифрованого тексту такого самого розміру. Цей режим часто називають режимом ECB (режим електронної шифрувальної книги).
- RC5-CBC. Режим зв'язаних шифрованих блоків для RC5. У режимі CBC обробляються повідомлення, довжина яких кратна розміру блока RC5 (тобто кратна 2*w* бітам). Режим CBC забезпечує вищий ступінь захисту, ніж ECB, оскільки генерує різні блоки шифрованого тексту для однакових повторних блоків відкритого тексту.
- RC5-CBC-Pad. Модифікація режиму CBC, призначена для роботи з відкритим текстом будь-якої довжини. Довжина шифрованого тексту в цьому режимі перевищує довжину відкритого тексту не більш ніж на довжину одного блоку RC5.
- RC5-CTS. Режим запозичення шифрованого тексту (ciphertext stealing) теж є модифікацією CBC. У цьому режимі допускається обробка відкритого тексту будь-якої довжини і генерується шифрований текст тієї самої довжини.

Тобто алгоритм шифрування RC5 має значні переваги, які дають змогу використовувати його на процесорах з різною архітектурою та різною довжиною машинного слова, ефективно використовувати апаратні та програмні реалізації алгоритму, роблять його програмну реалізацію ефективною з погляду використання обчислювальних потужностей процесора і пам'яті. На відміну від аналогічних алгоритмів (російського стандарту ГОСТ 28147-89 чи стандарту США Rijndael) низькі вимоги до апаратних ресурсів та змінні параметри алгоритму дають змогу легко адаптувати алгоритм RC5 до змін у вимогах безпеки програмного комплексу, що робить цей алгоритм (у версії RC5-32/12/16, яка забезпечує розумний компроміс між швидкодією і ступенем захисту) оптимальним для використання як засобу забезпечення конфіденційності розроблюваної системи розподілення обчислень для задач теплового проектування електронних пристроїв нового покоління.

Для визначення основних параметрів, що впливають на криптостійкість та ефективність програмної реалізації обраного алгоритму шифрування, було проведено такі експерименти:

- Для випадкового блоку відкритого тексту створювався парний, в якому *i*-й біт був інвертований; пара блоків шифрувалась з однаковим випадковим ключем; дифузія визначалась як кількість (у %) різних бітів для отриманої пари блоків шифрованого тексту. Експеримент проводився 10 разів для кожного *i* (*i*=0…63), а результати усереднювались.
- Для випадкового ключа шифрування створювався парний, в якому *i*-й біт був інвертований; однаковий випадковий блок відкритого тексту шифрувався з використанням створеної пари ключів; конфузія визначалась як кількість (у %) різних бітів для отриманої пари блоків шифрованого тексту. Експеримент проводився 10 разів для кожного *i* (*i*=0…127), а результати усереднювались.
- Було створено множину тестових файлів випадкового вмісту розміром від 10 МБ до 1 ГБ, які шифрувались з використанням однакового ключа шифрування, при цьому програмно вимірювався час шифрування кожного файла. Експерименти проводились 10 разів для кожного розміру файла, а результати усереднювались. Швидкодія програмної реалізації алгоритму визначалась як коефіцієнт нахилу прямої, що описує залежність розміру відкритого тексту від часу шифрування. Експерименти проводились на комп'ютері з процесором AMD Athlon X2 5000+ (2,7 ГГц) та обсягом оперативної пам'яті 2048 МБ.

Результати тестування

Усереднене для 10 експериментів для кожного біта блоку значення дифузії алгоритму RC5-32/12/16 наведено на рис. 1. Максимальне значення дифузії становить 55,31 %, мінімальне – 43,91 % зі середнім значенням 49,88 %. Отже, можна зробити висновок, що алгоритм RC5-32/12/16 задовольняє сильний лавинний критерій і має добрі характеристики надійності. Крім того, були

розраховані основні статистичні характеристики розподілу значення дифузії та конфузії за номером біта блоку, які наведено в табл. 2. Основними характеристиками в нашому випадку є структурні характеристики вибірки: мода і медіана. Вони практично визначають структуру вибіркових даних і визначаються через ці дані. Ці показники мають статус основних або головних при асиметричному розподілі даних, причому, у випадку асиметрії розподілу мода або медіана беруть на себе роль середнього значення, відстань між ними може характеризувати ступінь асиметрії, крім того, медіана вважається найстійкішою характеристикою вибірки, а тому може бути основою для критерію оптимального розподілу даних в інтервалах. Як бачимо, в нашому випадку значення медіани і моди практично збігається з середнім значенням показника дифузії, що підтверджує добру статистичну однорідність даних. Дещо гірші характеристики, особливо значно більше значення дисперсії (4,02 порівняно з 2,3), ніж для алгоритму DES [4], найімовірніше пояснюється тим, що в алгоритмі RC5 як нелійний елемент використовуються залежні від даних циклічні зсуви, а не фіксовані S-матриці, як в алгоритмі DES, тому залежно від даних можливий більший розкид параметрів дифузії. Однак мінімальне значення дифузії 43,91 % є незначно гіршим ніж для алгоритму DES (45 %), що виправдовує такий підхід і не знижує криптостійкість алгоритму з погляду дифузійних характеристик разом з підвищенням криптостійкості стосовно інших методів криптоаналізу [9, 11].

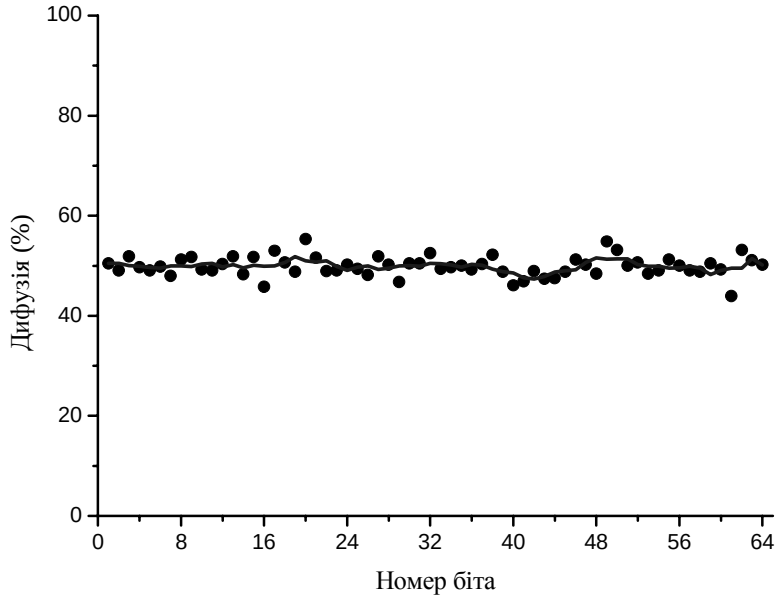

Рис. 1. Усереднене значення дифузії для алгоритму RC5-32/12/16 (точки – експериментальні значення, лінія – згладжування за 5-ма точками).

Таблиця 2

Статистичні характеристики розподілу значень дифузії та конфузії

Параметр	Дифузія	Конфузія
Найбільше значення	55,31	55,47
Найменше значення	43,91	45,94
Розмах	11,40	9,53
Медіана	49,92	49,84
Середнє арифметичне значення	49,88	50,34
Значення моди	49,06	47,97
Дисперсія*	4,02	4,92
Стандартне відхилення*	2,00	2,22

* Дисперсія D і стандартне відхилення σ^2 визначались як $D = \overline{x^2} - \overline{x}^2$, $\sigma^2 = \sqrt{D}$.

На рис. 2 наведено усереднене по 10 експериментам для кожного біта ключа шифрування значення конфузії алгоритму RC5-32/12/16. Максимальне значення конфузії становить 55,47 %, мінімальне – 45,94 %. Основні статистичні показники залежності конфузії він номера біта ключа наведено в табл. 2. Як видно з цієї таблиці, статистичні характеристики розподілу значень конфузії залежно від номера біта ключа є дещо нижчими ніж характеристики розподілу дифузії, однак однорідність розподілу значень конфузії залишається доволі високою з дисперсією 4,92, що підтверджується також значеннями моди та медіани, які становлять 47,97 і 49,84 відповідно при середньому значенні показника конфузії 50,34 %. Порівняно з алгоритмом DES [4] максимальне і середнє значення конфузії є дещо вищими (54,0 % і 49,8 % для алгоритму DES відповідно) при майже однаковому мінімальному значенні (46,0 % для DES), однак розподіл значень дифузії алгоритму DES від номеру біта ключа є однорідніщим з дисперсією 3,5 проти 4,92 для досліджуваного алгоритму RC5.

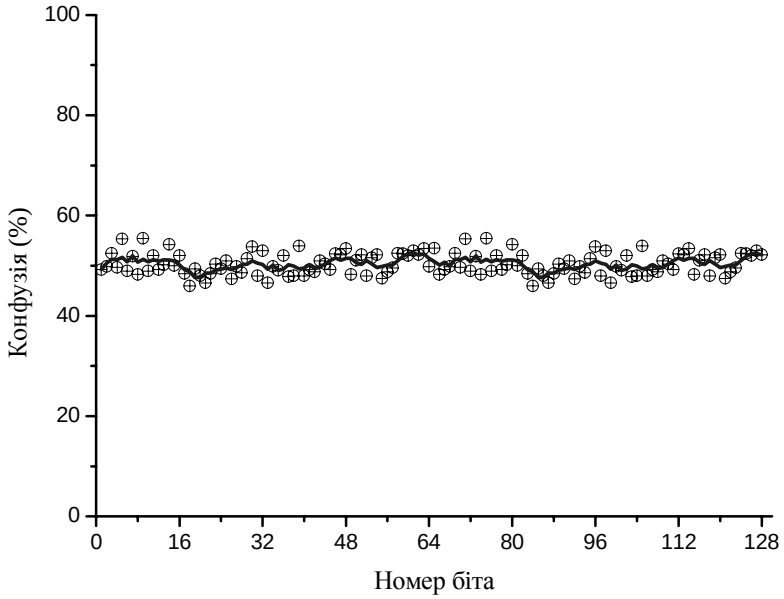

Рис. 2. Усереднене значення конфузії для алгоритму RC5-32/12/16 (точки – експериментальні значення, лінія – згладжування за 5-ма точками)

Для визначення швидкодії програмної реалізації у вихідному коді тестової програми використовувались функції, що на основі довжини такту процесора (кванта часу на такт) вираховували кількість тактів між двома точками програми. Так було визначено швидкодію програмної реалізації алгоритму шифрування без урахування зчитування даних в оперативну пам'ять і запис на диск. Методом найменших квадратів було апроксимовано залежність часу шифрування від розміру файла лінійною функцією і показано, що експериментальні дані з високою точністю апроксимуються лінійною залежністю (коефіцієнт кореляції не менший ніж 0,99903).

Швидкодія програмної реалізації алгоритму визначалась як коефіцієнт нахилу прямої, що описує залежність розміру відкритого тексту від часу шифрування. Розрахована так швидкість шифрування цієї реалізації алгоритму RC5-32/12/16 становить 212,77±0,01 Мбайт/с, що майже на порядок перевищує отриману нами швидкість програмної реалізації алгоритму DES (11,08 Мбайт/с на процесорі Intel Celeron D 351) [12] і підтверджує високу швидкість роботи алгоритму, описану в літературі [9].

Отже, незважаючи на дещо нижчі характеристики дифузії і конфузії алгоритму RC5-32/12/16 порівняно з DES, він залишається достатньо стійким за цими параметрами і значно переважає алгоритм DES за низкою інших параметрів і властивостей, зокрема швидкість його програмної реалізації є майже на порядок більшою і менш вимогливою до ресурсів центрального процесора і пам'яті, що відіграє особливу роль в системах, основним навантаженням яких є розв’язання

ресурсомістких задач теплового проектування. Тобто алгоритм RC5-32/12/16 залишається оптимальним вибором для реалізації модуля забезпечення конфіденційності інформації системи розподілення обчислень для задач теплового проектування.

Висновки

У роботі експериментально досліджено швидкість програмної реалізації та характеристики дифузії та конфузії алгоритму RC5-32/12/16 для усіх бітів блоку відкритого тексту і ключа відповідно.

Встановлено, що середнє значення дифузії і конфузії алгоритму RC5-32/12/16 становить 49,88 % та 50,34 % відповідно, а дисперсія значень залежно від номера біта блоку (чи ключа) становить 4,02 % і 4,92 %. Однорідність розподілу значень цих характеристик підтверджується також значеннями моди та медіани, які майже не відрізняються від середнього арифметичного значення. Дифузійні характеристики алгоритму RC5-32/12/16 практично відповідають сильному лавинному критерію і мають достатній статистично однорідний розподіл.

Швидкість шифрування алгоритму RC5-32/12/16 на процесорі AMD Athlon X2 5000+ становить 212,77±0,01 Мбайт/с, що майже на порядок перевищує швидкість програмної реалізації алгоритму DES і підтверджує високу швидкість роботи алгоритму, описану в літературі. Показано, що швидкодія програмної реалізації алгоритму є лінійною в усьому дослідженому діапазоні розмірів вхідних файлів. Показано доцільність використання алгоритму RC5-32/12/16 для задач шифрування даних за умов обмежених ресурсів центрального процесора і оперативної пам'яті.

Отже, завдяки високій швидкості програмної реалізації, низьким вимогам до апаратних ресурсів та високим характеристикам криптостійкості алгоритм RC5-32/12/16 є оптимальним вибором для реалізації модуля забезпечення конфіденційності інформації системи розподілення обчислень для ресурсомістких задач теплового проектування.

1. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – СПб.: НПО "Профессионал", 2004. – 478 с. 2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – 816 с. 3. V. Yakovyna, A. Odukha, V. Smirnov Testing random number generators // Proceedings of the 2nd International Conference of Young Scientists Computer Science and Engineering CSE-2007, Lviv, Ukraine, 2007. – P. 25–28. 4. Яковина В.С., Федасюк Д.В., Салій С.І., Сенів М.М. Дослідження характеристик криптостійкості алгоритму симетричного шифрування DES // Вісник Нац. ун-ту "Львівська політехніка" Комп'ютерні системи проектування. Теорія і практика. – в друці. 5. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Иностр. Лит-ра, 1963. – С. 333–402. 6. M. Robsaw Block Ciphers // RSA Laboratories Technical Report TR-601, August 1995. 7. Столлингс В. Криптография и защита сетей: принципы и практика. – М.: Вильямс, 2001. – 672 с. 8. A.F. Webster and S.E. Tavares On the Design of S-Boxes // Advances in Cryptology CRYPTO'85 Proceedings, Springer-Verlag, 1986, pp. 523-534. 9. R.L. Rivest The RC5 Encryption Algorithm // Proceedings of the Second International Workshop on Fast Software Encryption, Leuven Belgium, 1994, pp. 86-96. 10. R. Baldwin, R. Rivest The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms // RFC 2040, October 1996. 11. B.S. Kaliski, Yinqun Lisa Yin On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm //Advances in Cryptology Crypto'95 Proceedings, Springer-Verlag, 1995, pp. 171–184. 12. Яковина В., Федасюк Д., Сенів М., Білас О. Порівняння швидкодії програмної реалізації алгоритмів симетричного (DES) та асиметричного (RSA) шифрування // Вісник Нац. ун-ту "Львівська політехніка" Комп'ютерні науки та інформаційні технології. – 2007. – № 598. – С. 181–185.