УДК 004.056.55

Віталій Гаража, Олександр Доренський
Кіровоградський національний технічний університет, Україна

ОСОБЛИВОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ AES

Vitaliy Garazha, Olexandr Dorensky

FEATURES OF THE SOFTWARE IMPLEMENTATION OF THE AES ALGORITHM

Одним із найнадійніших методів захисту інформаційних ресурсів інформаційно-комунікаційних систем є використання криптографічних засобів [1]. Для забезпечення конфіденційного передавання інформації сучасна криптографія передбачає можливість використання значного розмаїття симетричних алгоритмів шифрування. До типових симетричних алгоритмів, призначених для шифрування даних, можна віднести алгоритми DES, 3DES, IDEA, AES, Twofish, Blowfish, CAST-5 (CAST-128) та інші, які можуть бути використані як самостійно, так і у режимах типу ECB, CBC, OFB та CFB [2]. Типовою областю їх застосування є передавання даних. Проблемою, яка виникає під час передавання інформації, є надійність алгоритму, яка визначається рядом критеріїв: довжиною ключа, кількістю раундів шифрування, довжиною блока даних відкритого тексту та математичною складністю реалізації раунду шифрування тощо.

Метою роботи є дослідження особливостей програмної реалізації алгоритму шифрування AES для розробки системи шифрування даних (файлів).

Аналіз [2-5] показав, що серед найпоширеніших алгоритмів шифрування оптимальними з погляду специфіки їх роботи, рівня захисту та простоти імплементації є алгоритми AES та RSA. Водночас, симетричний алгоритм AES, наприклад, відповідно до дослідження [4], має значно кращу часову характеристику: якщо 1 Мб даних асиметричний RSA шифрує за 7,5 сек., то AES – за 0,51 сек. Тобто програмна реалізація криптографічних перетворень над даними на основі алгоритму AES є більш ніж в 10 разів швидша ніж при використанні RSA. Таким чином, алгоритм AES можна вважати доцільним для програмної реалізації з метою подальшого впровадження і використання, що є актуальною задачею. Також слід відзначити, що Rijndael стандарту AES – це швидкий і компактний алгоритм з простою математичною структурою, завдяки чому він є простим для аналізу під час оцінювання рівня захисту.

Беззаперечним доказом ефективності і досконалості AES (від англ. Advanced Encryption Standard), який відомий також під назвою Rijndael, є шлях його розробки і ухвалення як стандарту США, що детально викладено у літературі [6].

AES є нетрадиційним блоковим шифром, оскільки не використовує мережу Фейштеля для криптоперетворень [6]. Він оперує 128-бітними блоками даних і довжиною ключа розрядністю 128, 192 або 256. Вхідні, проміжні і вихідні результати перетворень, що виконуються в рамках алгоритму, називають станами (state) [7], які можна представити матрицею 4x*Nb* (*Nb* – кількість 32-бітних слів вхідного блоку), елементами якої є чотири рядки по *Nb* байт в порядку S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, S_{11}, S_{21}, S_{31} і т.д. Ключ шифрування, як і масив State [7], представляється прямокутним масивом (матрицею) з чотирма рядками.

Загальна ідея алгоритму, що досліджується, – перетворення вхідного повідомлення у шифротекст за допомогою послідовного застосування до масиву State ряду трансформацій: побайтова нелінійна підстановка в state-блоках з використанням фіксованої таблиці замін розмірністю 8x256; циклічний зсув рядків масиву State ліворуч на різну кількість байт; множення стовпців стану, що розглядаються як многочлени над $GF(2^8)$; побітове XOR вмісту state з поточним [6].

До основних особливостей AES, який специфікує алгоритм Rijndael [5, 6], та його програмної реалізації можна віднести те, що він є симетричним блоковим шифром, який працює з блоковими даними довжиною 128 біт та використовує ключі 128, 192 і 256 біт (версії AES-128, AES-192, AES-256) [6]. Дослідження [5] показали, що однією з особливостей програмної реалізації і важливою перевагою з погляду криптостійкості, впровадженні й

практичного застосування зазначеного алгоритму є також те, що він може працювати і з іншими довжинами блоків даних та ключів. Хоча така можливість не входить до стандарту [7], проте вона може бути ефективно застосована на практиці.

Як і DES [6] (а також більшість симетричних блочних шифрів), алгоритм, що досліджується, складається з великої кількості перетворень – раундів. За найменшого варіанта, коли розміри блока й ключа є 128-бітними, кількість раундів складає 10. Для більш великих масивів даних і ключів кількість раундів може зростати [5].

Особливості програмної реалізації AES також випливають з особливостей самого алгоритма. Серед них, зокрема, слід відзначити нову архітектуру "Квадрат", що забезпечує надшвидке "розсіювання" та "перемішування" інформації, при чому за один раунд перетворенню підлягає весь вхідний блок [5]. Крім того в алгоритмі застосовується байт-орієнтована структура, що під час програмної реалізації процесу шифрування забезпечує розробку на 8-розрядних мікроконтролерах. Варто відзначити одну з найважливіших особливостей AES: ефективна апаратна та програмна реалізація на різноманітних платформах. Зокрема важливим для програмної реалізації AES є те, що у структурі алгоритму закладена можливість паралельного виконання операцій, що на багатопроцесорних ЕОМ дозволить збільшити швидкість шифрування у кілька разів.

У роботі досліджено й обґрунтовано особливості програмної реалізації алгоритму блочного кодування Rijndael, який ухвалений як американський стандарт шифрування AES. За результатами досліджень запропоновано оптимальну модель даних, структуру програми AES-модуля, інтерфейсу користувача для розробки системи шифрування даних дослідженим шифрометодом. Крім того у доповіді наведено результати проведеного аналізу основних переваг і недоліків застосування алгоритму AES для розробки ПЗ шифрування та його впровадження, визначено практичну цінність роботи, перспективи й напрямки подальших досліджень.

Література

1. Квасніков В.П. Блоковий симетричний криптоалгоритм "Luna" / Квасніков В.П., Кінзерявий В.М., Гнатюк С.О. // Захист інформації. – 2011. – №3. – С. 78-88.

2. Бурачок Р.А. Використання симетричних алгоритмів шифрування при передаванні мультимедійних даних / Р.А. Бурачок, П.О. Гуськов, Р.І. Бак // Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 156-160.

3. Баричев С.Г. Стандарт AES. Алгоритм Rijdael / Баричев С.Г., Гончаров В.В., Серов Р.Е. // Основы современной криптографии. – М.: "ГЛ-Телеком", 2002. – 247 с.

4. Дудикевич В. Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв'язку / В.Б. Дудикевич, Ю.Л. Пархуць // Інформаційна безпека. 2011. – №1 (5). – С. 83-87.

5. Фисун С.Н. Методика шифрования данных с использованием программно-методического комплекса VisualAES / С.Н. Фисун, А.И. Копылов // Радіоелектронні і комп'ютерні системи. – 2012. – № 5 (57). – С. 83-85.

6. Основи захисту інформації: Навч. посібник. / [Смірнов О.А., Віхрова Л.Г., Осадчий С.І. та ін.]. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.

7. Панасенко С.П. Алгоритмы шифрования. Спец. справочник / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.