УДК 004.056.55

І. М. Журавська, М. П. Мусієнко, Д. І. Румянков

БЛОКОВИЙ МЕТОД ШИФРУВАННЯ ДЛЯ РУХОМИХ ОБ'ЄКТІВ З ОБМЕЖЕНИМИ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ

Чорноморський національний університет імені Петра Могили, Миколаїв

Анотація. Проаналізовані особливості створення блокових методів шифрування, які працюють за рахунок комбінування простих операцій (логічних побітових операцій та бітових зсувів) під час обчислювального процесу, що виконується на мікроконтролерах малогабаритних рухомих об'єктів. В результаті роботи було створено новий блоковий метод шифрування, який надає захист інформації не тільки при використанні на великих ЕОМ та ПК, а й при шифруванні у пристроях на мікроконтролерах. Запропонований метод дозволяє підвищити ефективність шифрування інформації при застосуванні обмежених обчислювальних ресурсів та може використовуватися для захисту трафіка безпілотних літальних апаратів (БПЛА).

Ключові слова: симетричні блокові методи шифрування, захист трафіку БПЛА.

Аннотация. Проанализированы особенности создания блочных методов шифрования, работающих за счет комбинирования простых операций (логических побитовых операций и битовых сдвигов) при вычислительном процессе, выполняемом на микроконтроллерах малогабаритных подвижных объектов. В результате работы был создан новый блочный метод шифрования, который предоставляет защиту информации не только при использовании на больших ЭВМ и ПК, но и при шифровании в устройствах на микроконтроллерах. Предложенный метод позволяет повысить эффективность шифрования информации при применении ограниченных вычислительных ресурсов и может использоваться для защиты трафика беспилотных летательных аппаратов (БПЛА).

Ключевые слова: симметричные блочные методы шифрования, защита трафика БПЛА.

Abstract. The article provides the features of the block encryption methods' creation based on combining simple operations (bitwise logical operations and bit shifts) when computing process runs on microcontrollers of small moving objects. As a result, the new block encryption method was created that provides protection of information not only for use on mainframe computers and PCs, but also for encryption in devices based on microcontrollers. The proposed method can improve the efficiency of data encryption when using the limited computing resources. This method can be used to protect the traffic of unmanned aerial vehicles (UAVs).

Key words: symmetric block encryption methods, UAV traffic protection.

Вступ

Всі сучасні криптосистеми спираються на принцип Керкгоффса, відповідно якому секретність закодованих даних визначаються секретністю лише ключа кодування інформації користувача [1]. Тобто, усі алгоритми шифрування даних загальновідомі.

Найвідомішими блоковими методами шифрування є запроваджені у США стандарти шифрування DES та AES [2]. Але кожний з них має свої переваги та недоліки. Загальними недоліками для будь-якого методу є його зависока вибагливість до кількості та ємності обчислювальних ресурсів чи слабка криптостійкість до зламу.

Останнім часом стало популярним використання блокових методів шифрування для захисту трафіка рухомих об'єктів – безпілотних літальних апаратів (БПЛА) [3].

В такому разі використання методів шифрування не обмежується тільки їх застосуванням на комп'ютерах чи супер-комп'ютерах, але й потребує модифікації для роботи на мікроконтролерах. Але застосування методів шифрування в комп'ютерних системах на мікроконтролерах створює обмеження в використаних обчислювальних ресурсах, що змушує робити метод «легшим», – тобто таким, котрий буде використовувати якомога менше обчислювальних ресурсів.

Таким чином, постає проблемне питання щодо використання методу шифрування в сучасних об'єктах на мікроконтролерах, що мають ресурси оперативної пам'яті до 1 Мбайт [4].

Метою роботи є розробка блокового методу шифрування зі зниженими вимогами до обчислювальних ресурсів за рахунок використанням простих логічних операцій.

Результати дослідження

Хід Розглядаючи всі сучасні системи та програмне забезпечення (ПЗ), які використовують схожі методи шифрування даних, прототипом дослідження стала загальновідома програма Skype, яка використовує метод AES з довжиною ключа всередині метода 256 біт. Так як всі методи генерації ключів та реалізація раундів є неопублікованою інформацією, можна припустити, що для забезпечення захисту інформації користувачів виконана модифікація блокового методу, яка знаходиться на віддаленому сервері.

Розглядаючи усі доступні дані, за основу необхідно взяти простий алгоритм, який задовільнить вимогам стійкості криптосистеми та швидкого виконання кодування та декодування даних.

Під час дослідження роботи кожного з блокових методів шифрування DES та AES було виділено основні операції, які застосовуються: додавання, перемішування, здвиг бітів та бінарна операція XOR [5].

Справді, одним з легких та найпростіших відносно обчислювальних ресурсів є алгоритм з використанням операції XOR. Виходячи з цього, була прийнята спроба розробити блоковий метод, в основу якого буде покладена дана операція, але перед цим необхідно оцінити його криптостійкість щодо спроби злому та отримання інформації.

Розглядаючи концепцію використання операції XOR в існуючих методах потокового шифрування, наприклад, в комплексі ВРС-алгоритма для шифрування відеосигналів, які передаються поточно з літального пристрою, можна зауважити, що така задача є не цілком пріоритетною [6]. Таке суперечення обумовлено тим, що головною метою шифрування даних є підвищити прихованість наступних дій БПЛА в умовах зорового контакту з противником.

Так як кодування передаваної відеоінформації з рухомого пристрою вимагає немалих ресурсів, то, відповідно, вбудовувати в керуючий модуль алгоритм шифрування відеоданих не є цілком позитивним напрямом. Це обумовлене тим, що така складна архітектура модуля потребує великих обчислювальних ресурсів, й одна система повинна виконувати багато задач в одиницю часу – й саме шифрування даних, й передачу даних, й геопозиціонування рухомого об’єкту, й аналіз перешкод руху або відпрацювання команд кібер-оператора тощо. Описане рішення за сумою факторів обумовлює критичне застосування такої кіберфізичної системи, та може привести до втрати самого літального апарату [7].

Для забезпечення більш стабільної роботи комплексу системи керування необхідно розробляти окремо модуль кодування даних й налаштовувати з’єднання з керуючим модулем, що відповідно збільшує вагу БПЛА й вимагає конструктивних вдосконалень та в результаті веде до збільшення розміру апарату й підвищує вірогідність його виявлення тактичним противником [3].

Взагалі ідея шифрування відеопотоку не є гарною, так як командний пункт повинен якомога швидше отримати розвідувальні дані й надалі скерувати літальний апарат в потрібний квадрат ландшафту й гарантувати його бойову здатність до розвідувальних цілей.

Підвищити час виявлення маршруту БПЛА можливо за рахунок кодування його наступних координат геопозиціонування, які вказують наступну точку положення в просторі [3]. Тому дана мета є першопочатковою для забезпечення успіху в моніторингових операціях.

Навіть якщо прийняте рішення щодо кодування відеопотоку, наприклад, за допомогою ВРС-алгоритма, то для кодування геопозиційних координат такий або подібний метод не є доцільним за його “прожерливість” до обчислювальних ресурсів та архітектурну складність. А саме конкатенація даних з номером сеансу для розпізнавання «Свій-Чужий» є небезпечною, й таким чином, умовний противник, підібравши номер сеансу зв’язку, може заволодіти конфіденційними даними користувачів чи організації.

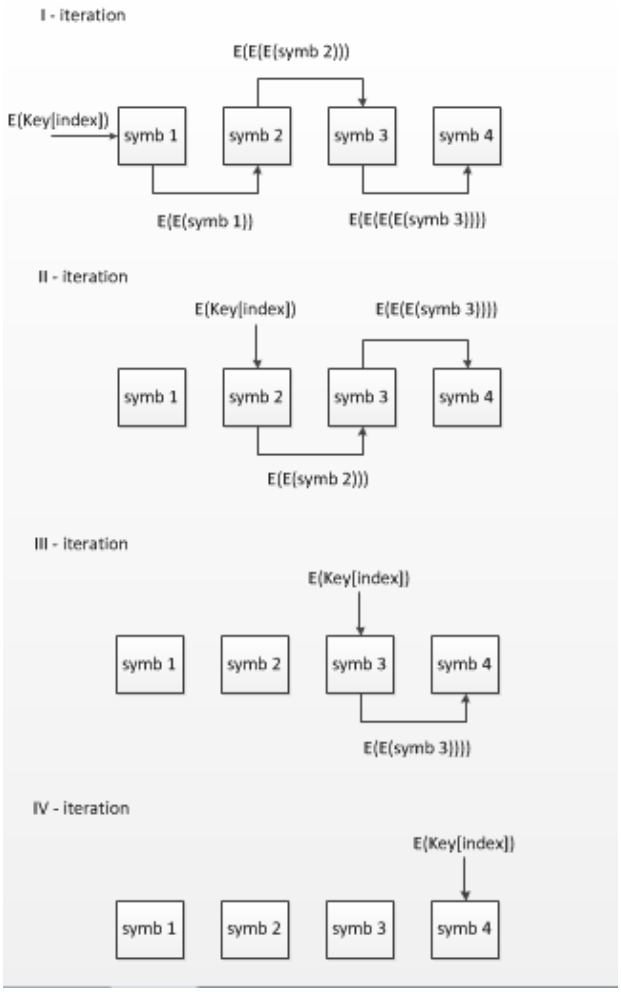

Рисунок 1 – Раунди блокового шифрування інформації

Маючи необхідний інструмент для виконання шифрування даних, доцільно розпочати роботу та дослідження кодування інформації простою операцією XOR [5]. Таким чином, маючи одну бінарну операцію в алгоритмі, можна сказати, що вже є реалізація симетричного алгоритму кодування, який кодує інформацію за принципом використання операції XOR між значенням ключа й відповідним бітом; натомість отримуємо нове значення в поточній позиції множини даних (послідовність бітів).

Але, виконуючи таку схему шифрування, бажаної безпеки не отримаємо. Такий алгоритм шифрування легко зламується навіть без комп’ютера.

Тому, окрім бінарної операції, необхідно використовувати комбінацію інших можливих операцій. Необхідно створити схему послідовності етапу шифрування (так званий «раунд» в криптографії), за якої б можна отримати унікальне значення кожного біту задля того, щоб вирішити проблему зламу XOR-шифрування, тобто визначити індекс збігу.

Але зробити в початковому наборі кожний біт унікальним неможливо, так як їх значення знаходиться у виборці, яка обмежена значенням 255. Тому для вирішення питання унікальності необхідно скористатися розбиттям інформації на блоки по 32/64/128/256 бітів. Таким чином можна досягнути унікальності набору в блоці.

Але цього недостатньо, так як сама інформація хоч й кодується, але можливість дістати її першопочатковий образ залишається можливим. Для забезпечення криптостійкості необхідно застосувати перемішування цих блоків між собою у певному порядку [8]. Причому, порядок перемішування генерується ґеш-функцією, яка може розбити блоки на 10/12/14 в залежності від довжини ключа [9]. Таким чином досягається унікальність набору, чим й підвищується криптостійкість системи.

Після етапу перемішування блоків необхідно використати повторне розбиття блоку на більш малі частини, які б займали по 32 біти, але перед цим необхідно виконати перевірку на умову повноти. Сутність повноти блоку полягає в тому, що вхідна інформація повинна ділитися націло на 32 біти; якщо ж цього не виконується, то вона доповнюється дописуванням спеціального символу.

Таким чином, розбивши вже закодовану інформацію на менші блоки, можна перейти до основного кодування інформації – це кодування наступного блоку попереднім блоком, щоб зав'язати відповідну послідовність розташування малих блоків (рис. 1).

Дослідження створеного методу показало, що його застосування не потребує великих ресурсних витрат на генерацію раундових ключів. Це надає змогу виконувати операції кодування та декодування інформації в короткі проміжки часу, що й забезпечує високу криптостійкість даної системи. Так, наприклад, використання такого «легкого» методу шифрування в мікроконтролерах малих БПЛА надає змогу розробити рухомий об'єкт невеликого розміру, що, в свою чергу. суттєво збільшує час виявлення БПЛА в умовах розвідувальних дій. Крім того, що малі розміри такого об'єкту роблять можливим здешевити виготовлення, вони ще й збільшують шанс, що літальний апарат вийде неушкодженим з території протипротивника [3].

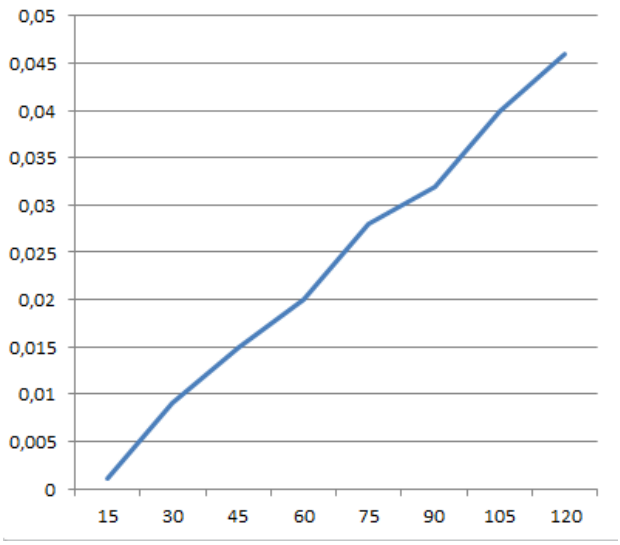

Рисунок 2 – Залежність часу шифрування (*c*) від обсягу інформації (байт)

Головна ідея методу полягає в тому, що інформація кодує сама себе, але за участю ключа користувача, який корегує схему кодування. Даний метод шифрування відповідає вимогам сучасності й надає повну свободу вибору ключа користувачем. Такий ключ може складатися з будь-яких символів з таблиці ASCII (окрім NULL).

На графіку рис. 2 зображено залежність кодування та декодування даних, що визначається за величинами часу та ємністю інформації (у байтах). Як видно з рис. 2, застосування даного методу кодування даних в літальних пристроях забезпечить швидку детермінацію напряму, який надсилає командний пункт (сервер).

Так як в запропонованому методі використовуються прості логічні операції, то кожна операція виконується в середньому 5 мкс. Тому нескладно обчислити теоретичний час P кодування даних:

$$P = P_{сер} \cdot m \cdot (k1 + k2 + k3), \qquad (1.1)$$

де P – загальний теоретичний час; $P_{сер}$ – опосередкований час виконання кожної операції; m – вага (обсяг) вхідної інформації; $k1$ – кількість операцій зсуву; $k2$ – кількість операцій логічного виключення; $k3$ – кількість пов'язаних блоків.

Треба зауважити, що в (1.1) величини k1, k2, k3 динамічно змінюються в залежності від довжини ключа та інформації, що шифрується.

З аналізу рис. 2 можна дійти висновку, що достатній обсяг поодиноких даних для передачі з БПЛА (показання датчиків окремих величин, координати знайдених об'єктів тощо) може бути зашифрованим

за дуже невеликий час, який не перевищує значення, співвідносні з часом в 1 с, необхідним сучасному обладнанню для зламу систем БПЛА з відомими характеристиками [10]. Це дозволить комп'ютерній системі рухомого об'єкта встигнути до зламу не тільки зашифрувати, а й передати та потім знищити з власних носіїв дані, отримані з датчиків та/або відеокамер.

Висновки

1. Під час виконання дослідження було проаналізовано блокові алгоритми кодування інформації й віднайдені основні риси, які характерні для кожного з них. Було сформовано фундаментальні правила для методу, який би забезпечив належний рівень захисту конфіденційної інформації, що передається в умовах неможливості забезпечення охорони периметру рухомої мережі (кібер-фізичної системи).

2. Були проаналізовані методи, які створюються шляхом комбінування операцій, простих для обчислювального процесу як ЕОМ, так і мікроконтролерних пристроїв. До таких операцій можна віднести операції зсуву, додавання, перемішування, логічного виключення.

Встановлено, що запропонований підхід дозволяє підвищити криптостійкість шифрованої інформації при зменшеному часі шифрування, у т. ч. на процесорах з низькою обчислювальною потужністю, які використовуються в БПЛА.

3. В результаті роботи було створено метод, який надає захист інформації шляхом шифрування не тільки на великих ЕОМ та ПК, а й може бути ефективно використаний в комп'ютерних системах на мікроконтролерах. Застосування методу шифрування в сфері використання БПЛА, які базуються на побудові архітектури керуючого пристрою на мікроконтролерах, надає відповідних результатів, головний з яких, – це перевага над тактичним ворогом у «неочікуваному маневруванні». Крім того, вірогідність, що БПЛА уціліє, збільшується на 30% за рахунок кодування команд щодо наступного місця знаходження літального пристрою.

4. Отримане співвідношення часу шифрування розробленим методом блоку даних для передачі іншому об'єкту мережі з часом, необхідним для зламу бортової системи БПЛА сучасним обладнанням, свідчить про достатньо високу криптостійкість та доцільність використання запропонованого методу, використання якого сприятиме подовженню життєвого циклу БПЛА.

Список літератури

1. Альбов, А. Квантовая криптография. – СПб. : ООО «Страта», 2015. – 248 с.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4, 0-471-11709-9.

3. Малые беспилотные летательные аппараты: теория и практика / МакЛэйн Т. У., Биард Р. У. – М. Техносфера: Мир электроники, 2015. – 312 с. – ISBN 978-5-94836-393-6.

4. Сидоренко, Б. Микроконтроллеры Atmel SAM D – Cortex-M0+: оптимальное соотношение производительности и энергоэффективности // Электроника: наука | технология | бизнес. – 2014. – № 3 (00134). – С. 78–85.

5. Rosen, Kenneth. (2006). *Discrete Mathematics and Its Applications* (6th Ed.). McGraw-Hill Education. 1006 p. ISBN 978-0073229720.

6. Белецкий, А. Я. Программно-моделирующий комплекс ВРС алгоритма поточного шифрования и помехоустойчивого кодирования видеосигналов, передаваемых с борта БПЛА / А. Я. Белецкий, А. В. Максименко, Д. А. Навроцкий, А. Д. Свердлова, А. И. Семенюк // Захист інформації. – 2014. – Т. 16, № 3. – С. 184–191.

7. Musiyenko, M.P., Zhuravska, I.M., Burlachenko, I.S. and Denysov, O.O. (2016), "The Principles of the Cyber-Physical Components' Organization Based on the Methods of the Multi-Agent Interaction of the Moving Objects", Advances in Cyber-Physical Systems, Vol. 1 No. 1, pp. 48-57. Available from http://vlp.com.ua/files/special/10_289.pdf [Accessed 18 Sep. 2016].

8. Журавська, І. М. Підвищення ефективності шифрування керуючого трафіку БПЛА засобами модифікованого блокового методу [Текст] / І. М. Журавська, М. П. Мусієнко, Д. І. Румянков // Методи та засоби кодування, захисту й ущільнення інформації : тези доп. V-ї Міжнар. наук.-практ. конф., 19-21 квітня 2016 р., Вінниця. – Вінниця : Вид-во Вінниц. нац. техн. ун-ту», 2016. – С. 75–77.

9. Лужецький, В. А. Криптографічні примітиви для реалізації керованого хешування / В. А. Лужецький, Ю. В. Баришев // Вісник Вінницького політехнічного інституту : наук. журнал / ВНТУ. – 2011. – № 1. – С. 108–111.

10. Взлом беспилотника займет у комплекса РЭБ "Шиповник-АЭРО" секунду // Интерфакс. Новости ВПК. – 2016. – 14 сентября. – Режим доступа : URL : http://vpk.name/news/163641_vzlom_bespilotnika_zaimet_u_kompleksa_reb_shipovnikaero_sekundu.html (дата обращения 18.09.2016).

Стаття надійшла: 20.09.2016.

Відомості про авторів

Журавська Ірина Миколаївна – к. т. н., доцент кафедри комп'ютерної інженерії Чорноморського національного університету імені Петра Могили Миколаїв, 54003, Україна.

Мусієнко Максим Павлович – д-р техн. наук, професор, декан факультету комп'ютерних наук Чорноморського національного університету імені Петра Могили, Миколаїв, 54003, Україна.

Румянков Дмитро Ігорович – бакалаврант кафедри інтелектуальних інформаційних систем Чорноморського національного університету імені Петра Могили, Миколаїв, 54003, Україна.