DOI 10.15276/imms.v10.no1-2.100
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 100-108

ИССЛЕДОВАНИЕ РЕЖИМОВ ШИФРОВАНИЯ С ПРОПУСКОМ БЛОКОВ

А.В. Соколов, А.О. Корж

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Блочные симметричные шифры являются неотъемлемой частью любой современной комплексной системы защиты информации. Сегодня внимание исследователей сосредоточено на повышении эффективности и быстродействия блочных симметричных шифров, тем не менее, как показывает практический опыт реализации реальных систем шифрования данных, большое значение для обеспечения высокой криптографической стойкости и быстродействия современных систем шифрования имеет также режим шифрования, с помощью которого применяется тот или иной криптографический алгоритм. В настоящей статье предлагаются новые режимы шифрования: с пропуском блоков, а также с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Предложенные режимы шифрования позволяют обеспечить экономию примененных в программе операций шифрования данных с помощью блочного симметричного шифра. Для разработанных режимов шифрования вычислены параметры, позволяющие обеспечить высокий уровень стохастического качества, полученного на выходе шифротекста, что подтверждается проведенными испытаниями в соответствии с набором стохастических тестов NIST. При этом установлено, что режим шифрования с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей обеспечивает значительное повышения числа уровней защиты применяемого криптопреобразования, а также показывает наилучшие результаты при прохождении набора стохастических тестов NIST. Разработанные режимы шифрования являются обоснованным решением для использования в приложениях, работающих на платформах с ограниченными вычислительными и энергетическими ресурсами, в первую очередь, на мобильных устройствах. При этом предпочтительным является выбор режима с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Отметим также, что представленные режимы шифрования позволяют объединить воедино преимущества блочных симметричных шифров и генераторов псевдослучайных ключевых последовательностей.

Ключевые слова*:* криптография, режим шифрования, блочный симметричный шифр.

Введение

Построение современных систем передачи, обработки и хранения информации сегодня во многом сопряжено с задачами обеспечения её защиты. Одним из важнейших компонентов практически любой системы защиты информации являются блочные симметричные шифры (БСШ) [1].

Стремительное развитие методов криптоанализа, а также наращивание вычислительных мощностей современных компьютеров диктует необходимость совершенствования современных БСШ для повышения их криптографической стойкости, что является основной задачей большинства современных криптографических исследований.

С другой стороны, многие используемые современные вычислительные системы, например, распространенные сегодня мобильные устройства, обладают очень ограниченным уровнем вычислительных и энергетических ресурсов, что накладывает значительные ограничения на разрабатываемые приложения. В частности, желание

разработчиков увеличить быстродействие своих приложений, а также повысить общее время автономности вычислительного устройства зачастую приводит к необходимости отказаться от применения БСШ, например, для передачи файловых вложений большого размера в ущерб кибербезопасности.

Данный аспект практического использования методов криптографии органично ставит перед исследователями не только задачу повышения криптографической стойкости шифров, но и задачу повышения их быстродействия.

В работе [2] была предложена концепция шифрования с переменной фрагментацией блоков, позволяющая значительно снизить количество необходимых итераций основного шага криптопреобразования, таким образом снижая вычислительные затраты на шифрование одного блока входной информации. Данная концепция стала основой для разработки криптографического алгоритма, адаптированного для работы на мобильных устройствах [3]. Тем не менее, практический опыт использования данного БСШ показывает, что даже он достаточно сильно снижает быстродействие приложений при передаче больших файлов. Данный момент приводит к необходимости исследования не только вопросов повышения быстродействия самих БСШ, но и методов их применения к шифруемым данным – режимов шифрования. В частности, актуальным является построение режимов шифрования, в которых небольшие объемы чувствительной информации шифруются с применением режимов шифрования, обеспечивающих высокий уровень криптостойкости, в то время как более значительные объемы менее критичной информации шифруются с применением режимов шифрования, обладающих большим быстродействием.

Цель и задачи

Целью настоящей статьи является разработка режимов шифрования с пропуском блоков.

Для достижения цели статьи необходимо решить следующие задачи:

- разработать новые режимы шифрования с пропуском блоков, которые бы обеспечивали экономию операций применения БСШ при приемлемом уровне качестве шифрования;
- исследовать параметры режимов шифрования с пропусками блоков, обеспечивающие на практике высокий уровень криптографического качества операции шифрования.

Основная часть

Помимо криптографической стойкости самого используемого БСШ, в контексте безопасности и быстродействия применяемого криптографического алгоритма имеет огромное значение также и режим, с помощью которого он применяется к шифруемым данным.

Определение 1 [4]. Режим шифрования – это метод применения блочного шифра (алгоритма), позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных.

Простейшим из существующих режимов шифрования является режим Electronic Codebook (ECB), который предусматривает разбиение открытого текста на N блоков, размер каждого из которых определяется параметрами используемого шифра. Далее происходит их последовательное шифрование без установления какой-либо взаимосвязи между ними (рис. 1).

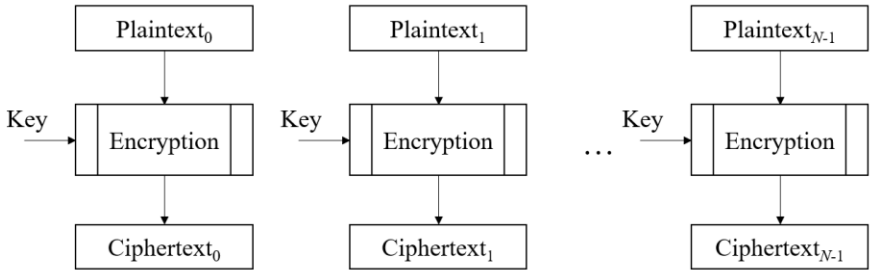
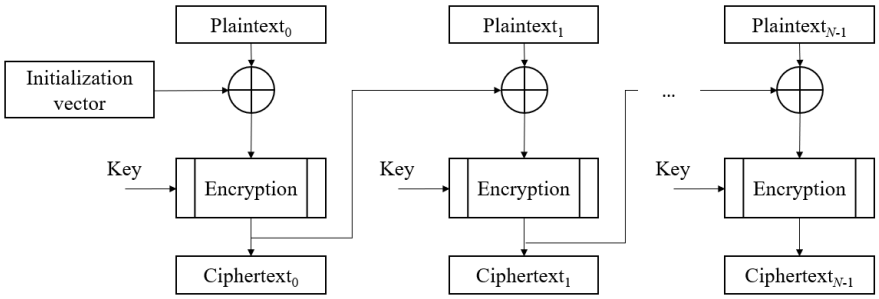


Рис. 1. Схема шифрования в режиме ECB

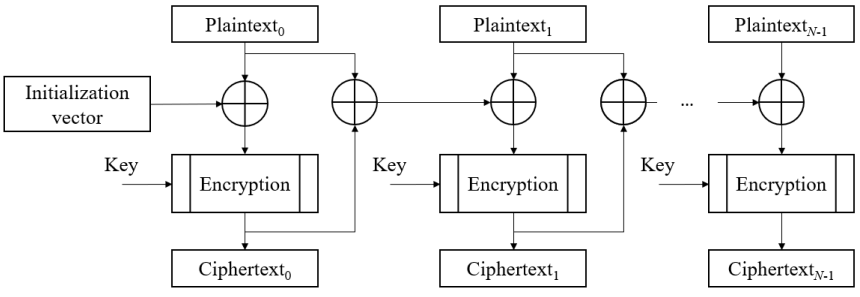
Данный режим шифрования характеризуется крайне низким уровнем криптографического качества при использовании любого, даже самого качественного БСШ, в виду сохранения статистических особенностей блоков открытого текста. Данный режим строго не рекомендуется применять на практике [4].

Отметим также, что классическим подходом к оценке качества криптограмм является использование в отношении них пакета стохастических тестов NIST [5]. Эксперименты показывают, что применение данного пакета тестов к последовательностям, полученным с помощью применения криптоалгоритма AES [6] в режиме ECB приводит к провалу в прохождении указанного пакета стохастических тестов. В частности, рассмотренный пример шифрования файлов показал, что криптограммы не проходят тесты Binary matrix rank test (показатель $P-value=0.00019$) и Linear complexity test (показатель $P-value=6.85\cdot10^{-6}$).

Следующими, более совершенными режимами шифрования являются режимы сцепления блоков (CBC) и распространяющегося сцепления блоков (PCBC), схемы которых представлены на рисунке 2.



а



б

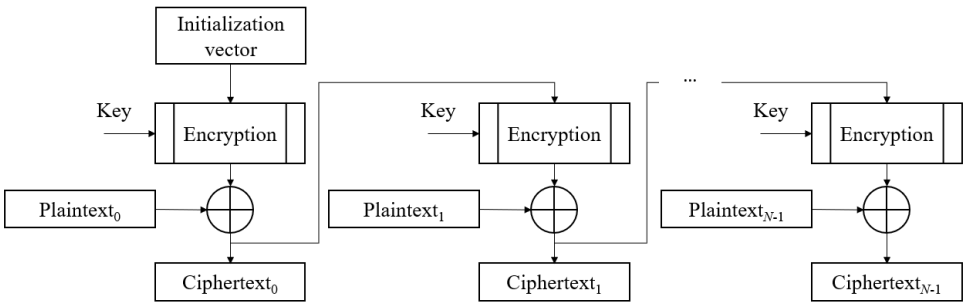
Рис. 2. Режимы шифрования CBC и PCBC: а – режим шифрование CBC; б – режим шифрование PCBC

В данных режимах предусмотрено использование вектора инициализации, который складывается с первым блоком отрытого текста, после чего происходит

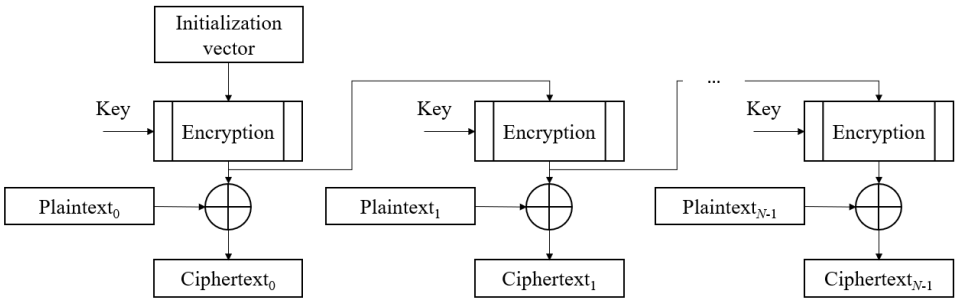
шифрование полученной суммы. Для последующих блоков данный вектор инициализации представляет собой либо предыдущий блок зашифрованного текста (CBC), либо сумму предыдущих блоков зашифрованного и открытого текста (PCBC).

Шифрование данных в представленных режимах обеспечивает высокий уровень криптографического и стохастического качества зашифрованных последовательностей, что экспериментально подтверждается прохождением пакета стохастических тестов NIST.

Еще двумя часто используемыми на практике режимами шифрования являются режим обратной связи по шифротексту (CFB) и режим обратной связи по выходу (OFB), схемы которых представлены на рисунке 3.



а



б

Рис. 3. Режимы шифрования CFB и OFB: а – режим шифрование CFB; б – режим шифрование OFB

Данные режимы предусматривают маскировку входного текста путем сложения его по модулю 2 с результатом шифрования векторов инициализации, в качестве которых используется шифротекст предыдущего блока (CFB) или гамма из предыдущего блока до сложения с вектором открытого текста (OFB). Указанные режимы шифрования также обеспечивают высокий уровень криптографического и стохастического качества получаемых криптограмм, достаточный для прохождения набора стохастических тестов NIST.

Помимо перечисленных основных режимов шифрования существуют и некоторые другие, например, с аутентификацией данных [4].

Отметим, что шифрование во всех перечисленных режимах предполагает применение процедуры шифрования выбранным криптоалгоритмом ко всем без исключения блокам входных данных. Тем не менее, как показывают исследования, данное действие не является обязательным для достижения достаточного уровня криптографического и стохастического качества.

В настоящей работе предлагается модификация перечисленных основных режимов шифрования, позволяющая сократить количество необходимых операций «шифрование блока», необходимых для зашифрования файла. Так, на этапе подготовки

к процедуре шифрования выбираются константы M и C. В начале процедуры шифрования значением 0 инициализируется переменная i. Перед применением блока шифрования выполняется проверка условия $i \bmod M \in \{0,1,...,C\}$ и, если условие ложно – шифрование данного блока не выполняется. По завершении обработки блока значение переменной i увеличивается на 1.

В зависимости от конкретных значений M и C происходит пропуск операции шифрования для того или иного блока открытого текста. Так, например, если $M = 2$ и $C = 0$ происходит пропуск операции шифрования для каждого второго блока открытого текста.

При этом указанная модификация может быть применена к любому из рассмотренных нами режимов шифрования (рис. 1–3). Для краткости изложения материала, в качестве примера мы приводим на рис. 4 схему режима шифрования с пропуском блоков на примере модификации режима CBC.

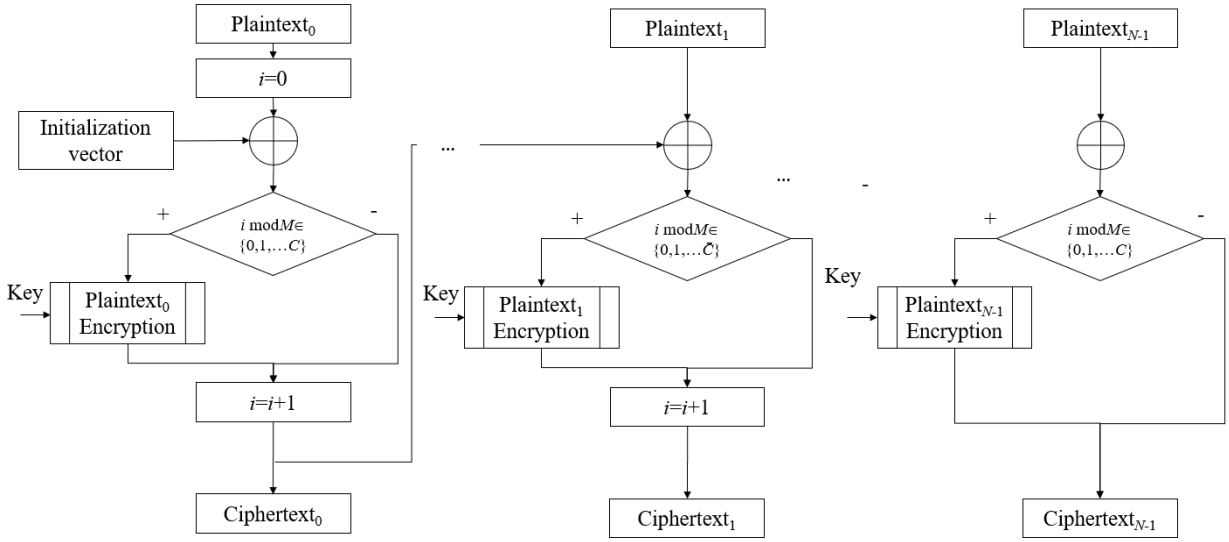


Рис. 4. Модификация режима шифрования CBC с пропуском блоков

При этом схема расшифрования строится аналогично схеме шифрования (рисунке 4).

В настоящей работе были проведены вычислительные эксперименты, в рамках которых шифровались файлы различного размера и содержания с помощью криптоалгоритма AES в различных режимах шифрования с пропуском блоков при различных значениях M и C. После выполнения шифрования к полученным криптограммам применялся набор стохастических тестов NIST.

Полученные в данных вычислительных экспериментах результаты свидетельствуют, что при шифровании информации при значениях $M = 25$ и $C = M - 2$ (данные значения обеспечивают пропуск шифрования каждого 25-го блока отрытого текста) для полученных криптограмм выполняются все стохастические тесты из набора NIST. Таким образом, для реализации операции шифрования файла требуется на $(1/25) \cdot 100\% \simeq 4\%$ меньшее количество блоков шифрования.

Тем не менее, полученного выигрыша в количестве необходимых операций шифрования с помощью БСШ, например, AES может оказаться недостаточно для шифрования крупных файлов.

Далее мы предлагаем еще один режим шифрования (рис. 5), позволяющий значительно сократить необходимое количество блоков шифрования БСШ. Для реализации этой схемы используется такой криптографический примитив как генератор псевдослучайных ключевых последовательностей (ГПКП), который может

быть построен, например, в соответствии со схемами [7] или [8]. При этом быстродействие данных криптографических примитивов значительно превышает быстродействие блочных симметричных криптоалгоритмов [8].

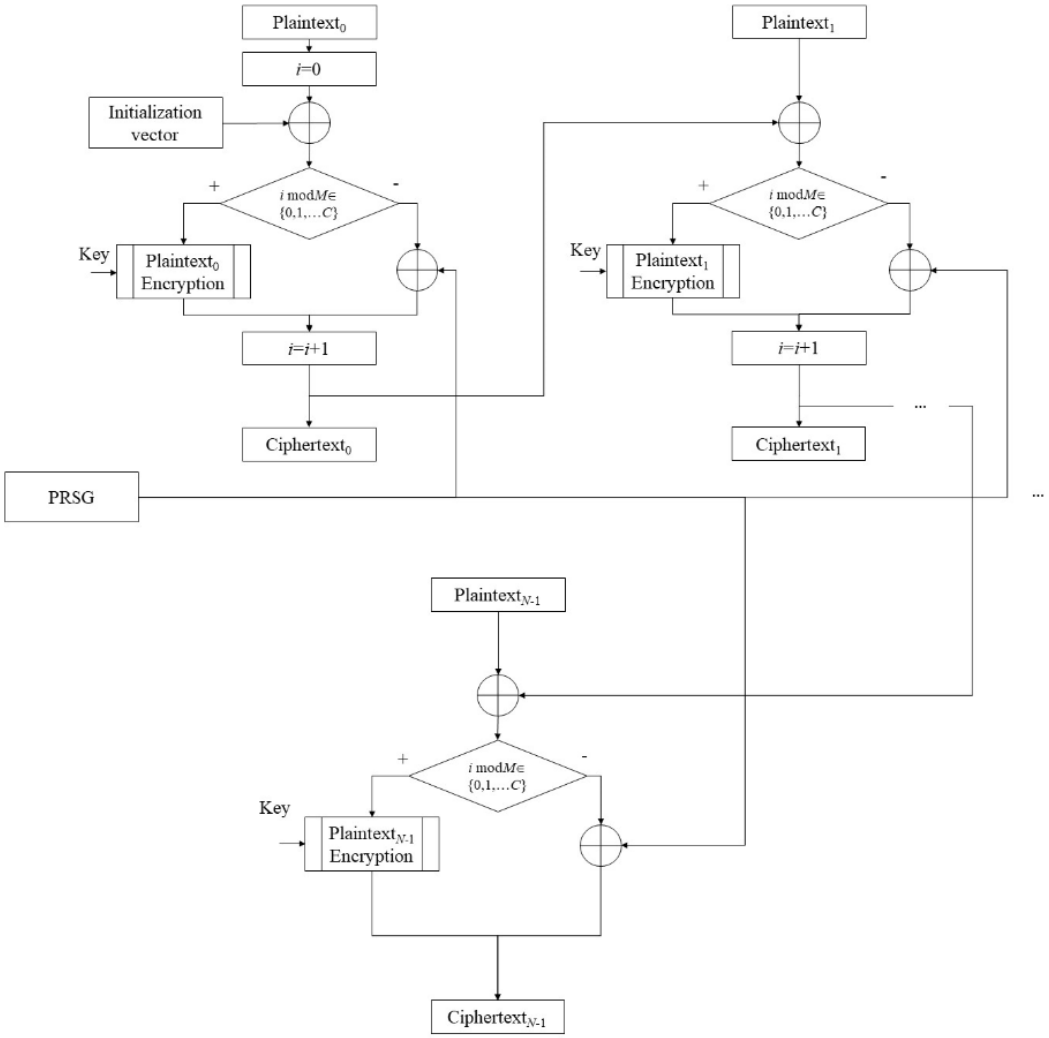


Рис. 5. Режим шифрования CBC с пропуском блоков и применшеним ГПКП

Перед началом операции шифрования выбранная схема ГПКП инициализируется с помощью дополнительного фрагмента ключа. Аналогично модифицированному режиму шифрования с пропуском блоков (рис. 4), в данном режиме шифрования вводятся параметры M и C. В начале процедуры шифрования значением 0 инициализируется переменная i. Перед применением блока шифрования выполняется проверка условия $i \bmod M \in \{0,1,...,C\}$ и, если условие ложно – вместо шифрования данного блока выполняется его гаммирование с помощью очередного сегмента гаммы, полученного с помощью ГПКП. По завершении обработки блока значение переменной i увеличивается на 1.

Отметим, что схема расшифрования строится аналогично схеме шифрования (рис. 5).

Эмпирические исследования показали, что наилучшим образом себя показывает применение данного режима шифрования с режимом CFB, в то время как оптимальными являются значения параметров $M = 2$ и $C = 0$, т.е. сложение с гаммой ГПКП происходит для каждого второго шифруемого блока открытого текста.

Отметим также, что число уровней защиты получившейся схемы определяется произведением числа уровней защиты выбранного БСШ и ГПКП. Например, при

использовании БСШ AES-256 и ГПКП на основе дуальных пар бент-последовательностей [7] общее число уровней защиты получившейся криптографической системы достигает значения $\Psi \simeq 2^{256} \cdot 2^{165} = 2^{421}$, что является очень значительной величиной. Перспективным является также применение генераторов псевдослучайных ключевых последовательностей на основе совершенных алгебраических конструкций многозначной логики [9].

В таблице 1 приведены результаты выполнения стохастических тестов для шифрования исходных данных до шифрования, после шифрования в режимах CFB, CFB с пропуском блоков, CFB с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей.

Таблица 1.

Результаты стохастических тестов NIST

№	Тест	Открытый текст		CFB		CFB с пропуском блоков		CFB с пропуском блоков и ГПКП	
		P-value	Pass rate	P-value	Pass rate	P-value	Pass rate	P-value	Pass rate
1	Monobit test	0	✗	0.71	✔	0.49	✔	0.8	✔
2	Frequency within block test	0	✗	0.4	✔	0.18	✔	0.99	✔
3	Runs test	0	✗	0.7	✔	0.32	✔	0.84	✔
4	Longest run ones in a block test	10^{-191}	✗	0.64	✔	0.31	✔	0.54	✔
5	Binary matrix rank test	0	✗	0.68	✔	0.18	✔	0.7	✔
6	DFT test	0	✗	0.9	✔	0.09	✔	0.96	✔
7	Non overlapping template matching test	0.125	✔	1	✔	0.99	✔	1	✔
8	Overlapping template matching test	0	✗	0.91	✔	0.85	✔	0.84	✔
9	Maurers universal test	0	✗	0.73	✔	0.16	✔	0.38	✔
10	Linear complexity test	10^{-11}	✗	0.22	✔	0.11	✔	0.03	✔
11	Serial test	0	✗	0.25	✔	0.12	✔	0.68	✔
12	Approximate entropy test	0	✗	0.34	✔	0.19	✔	0.9	✔
13	Cumulative sums test	0	✗	0.81	✔	0.34	✔	0.55	✔
14	Random excursion test	0.22	✔	0.2	✔	0.04	✔	0.31	✔
15	Random excursion variant test	0.11	✔	0.1	✔	0.02	✔	0.02	✔

Анализ данных, показанных в таблице 1 позволяет установить высокий уровень стохастического качества криптограммы, полученной в режиме CFB с пропуском блоков и использованием ГПКП.

Выводы

Отметим основные результаты проведенных исследований. В статье предложены новые режимы шифрования: с пропуском блоков, а также с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Применение данных режимов шифрования позволяет уменьшить количество применяемых в программе операций шифрования данных с помощью блочного симметричного шифра, что является особенно актуальным для использования в приложениях, работающих на требовательных к вычислительным и энергетическим ресурсам платформах. При этом предпочтительным является выбор режима с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей.

Для предложенных режимов шифрования вычислены параметры, обеспечивающие высокий уровень стохастического качества криптограмм при оптимальном уровне экономии применяемых в программе операций шифрования данных с помощью блочного симметричного шифра. Так, для режима шифрования с пропуском блоков количество сэкономленных операций шифрования данных с помощью блочного симметричного шифра составляет $\sim 4\%$ и 50% для режима с пропуском блоков и использованием ГПКП.

Число уровней защиты информации в случае применения режима с пропуском блоков и использованием ГПКП составляет $\Psi \simeq 2^{256} \cdot 2^{165} = 2^{421}$, что значительно превосходит число уровней защиты, обеспечиваемых другими режимами шифрования.

Проведенные в статье исследования органично ставят задачу дальнейшего повышения криптографической стойкости и быстродействия генераторов псевдослучайных ключевых последовательностей, в частности, на основе совершенных алгебраических конструкций.

Список литературы

1. Knudsen L.R., Robshaw M. The Block Cipher Companion. Springer, 2011. 284 p.
2. Жданов О.Н., Соколов А.В. Алгоритм шифрования с переменной фрагментацией блока. *Проблемы и достижения в науке и технике: сб. материалов науч.-практ. конф., 1 июня 2015 г.* Омск. 2015. № 2. С. 153-159.
3. Соколов А.В., Корж А.О., Лопуленко О.В. Модифікований алгоритм шифрування зі змінною фрагментацією блоків. *WayScience: матеріали VII міжнародної наук.-практ. конф., 6-7 червня 2019*, Дніпро. 2019. С. 1592-1596.
4. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley. 2015. 784 p.
5. Rukhin A., Soto J., Nechvatal J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology Special Publication. 2010. 131 p.
6. FIPS 197. Advanced encryption standard. 2001. URL: http://csrc.nist.gov/publications/.
7. Мазурков М.И., Соколов А.В., Барабанов Н.А. Генератор ключевых последовательностей на основе дуальных пар бент-функций. *Праці Одеського політехнічного університету*. 2013. №3. С. 150-156.
8. Соколов А.В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов. *Праці Одеського політехнічного університету,* 2014.43(1). С. 180-186.
9. Соколов А.В., Жданов О.Н., Барабанов Н.А. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций. *Проблемы физики, математики и техники*. 2016. V.26(1). С. 85-91.

ДОСЛІДЖЕННЯ РЕЖИМІВ ШИФРУВАННЯ З ПРОПУСКОМ БЛОКІВ

А.В. Соколов, А.О. Корж

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Блокові симетричні шифри є невід'ємною частиною будь-якої сучасної комплексної системи захисту інформації. Сьогодні увага дослідників зосереджена на підвищенні ефективності і швидкодії блокових симетричних шифрів, проте, як показує практичний досвід реалізації реальних систем шифрування даних, велике значення для забезпечення високої криптографічної стійкості і швидкодії сучасних систем шифрування має також режим шифрування, за допомогою якого застосовується той або інший криптографічний алгоритм. У цій статті пропонуються нові режими шифрування: з пропуском блоків, а також з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей. Запропоновані режими шифрування дозволяють забезпечити економію застосованих в програмі операцій шифрування даних за допомогою блокового симетричного шифру. Для розроблених режимів шифрування обчислені параметри, що дозволяють забезпечити високий рівень стохастичної якості, отриманого на виході шифротекста, що підтверджується проведеними тестами відповідно до набору стохастичних тестів NIST. При цьому встановлено, що режим шифрування з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей забезпечує значне підвищення числа рівнів захисту застосовуваного криптоперетворення, а також показує найкращі результати при проходженні набору стохастичних тестів NIST. Розроблені режими шифрування є обґрунтованим рішенням для використання в додатках, що працюють на платформах з обмеженими обчислювальними і енергетичними ресурсами, в першу чергу, на мобільних пристроях. При цьому переважним є вибір режиму з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей. Відзначимо також, що представлені режими шифрування дозволяють об'єднати воєдино переваги блокових симетричних шифрів і генераторів псевдовипадкових ключових послідовностей.

Ключові слова: криптографія, режим шифрування, блоковий симетричний шифр.

STUDY OF BLOCK SKIP ENCRYPTION MODES

A.V. Sokolov, A.O. Korzh

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: radiosquid@gmail.com

Block symmetric ciphers are an integral part of modern complex information security systems. Today, the attention of researchers is focused on increasing the efficiency and performance of block symmetric ciphers. However, it is shown by the practical experience of implementation of data encryption systems, that block cipher modes of operation are also of great importance for the efficiency and performance of encryption systems. In this paper we propose new block cipher modes of operation: with block skipping, as well as with block skipping and the use of pseudo-random key sequence generator. The proposed block cipher modes of operation make it possible to reduce the amount of used in the program data encryption operations (i.e. the amount of the block symmetric cipher runs). For the developed block cipher modes of operation, the parameters are calculated to ensure a high level of stochastic quality of the obtained ciphertext, which is confirmed by the tests carried out in accordance with the NIST stochastic test suite. At the same time, it was found that the block cipher mode of operation with skipping of blocks and the use of a pseudo-random key sequence generator, provides a significant increase in the number of information protection levels of the applied cryptographic transformation, and also shows the best results when passing the NIST stochastic tests suite. The developed block cipher modes of operation are a reasonable solution for use in applications running on platforms with limited computing and power resources, primarily on mobile platforms. In this case, it is preferable to select a block cipher mode of operation with skipping of blocks and use of pseudo-random key sequence generator. Note also that the presented block cipher modes of operation allow to combine the advantages of block ciphers and generators of pseudo-random key sequences.

Keywords: cryptography, encryption mode, block symmetric cipher.