Бобрышева Г.В., Звозникова А.О. Анализ алгоритмов блочного симметричного шифрования Mars и TwoFish. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVI Междунар. научно-техн. конф. – Пенза: ПДЗ, 2016. – С. 139-144.

УДК 004.056.55

# АНАЛИЗ АЛГОРИТМОВ БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ MARS И TWOFISH

Г.В. Бобрышева, А.О. Звозникова

# ANALYSIS ALGORITHMS MARS AND TWOFISH BLOCK SYMMETRIC ENCRYPTION

G.V. Bobrysheva, A.O. Zvoznikova

**Аннотация.** Рассматриваются особенности построения систем блочного симметричного шифрования и приводятся результаты анализа алгоритмов блочного симметричного шифрования Mars и TwoFish.

**Ключевые слова:** шифрование, дешифрование, блочный симметричный шифр, ключ, алгоритм, операция, криптографическая стойкость, подстановка, перемешивание

**Abstract.** The paper discusses the features of the construction of block symmetric encryption systems, and presents the results of analysis of Mars and TwoFish block symmetric encryption algorithms.

**Keywords:** encryption, decryption, the block cipher is a symmetric key algorithm, operation, cryptographic resistance, substitution, stirring

Для обеспечения криптографического закрытия данных, передаваемых по компьютерным сетям, широко применяются на практике блочные симметричные системы шифрования.

Блочный симметричный шифр состоит из двух взаимосвязанных алгоритмов: алгоритм шифрования E и алгоритм дешифрования E-1. Входными данными служат блок исходных данных размером n бит и k-битный ключ. На выходе получается n-битный зашифрованный блок данных. Для любого фиксированного ключа функция дешифрования является обратной к функции шифрования $E_к^{-1}(E_к(M))=M$ для любого блока M и ключа K. При этом исходный и зашифрованный блоки данных имеют фиксированную разрядность, равную между собой, но необязательно равную длине ключа.

Ключ Key является параметром блочного криптоалгоритма и представляет собой некоторый секретный блок двоичной информации фиксированного размера, используемый как для шифрования, так и дешифрования сообщений. Ключ выбирается из $2^n!$ возможных перестановок, где $n$ – это фиксированный параметр блочного шифра, равный размеру блока.

До середины 90-х годов была приемлема длина блока данных 64 бита. В настоящее время схемы блочного симметричного шифрования позволяют зашифровывать открытый текст произвольной длины и используют блоки данных размером 128 и более бит с использованием ключа размером 128, 192 и 256 бит [1].

Особенностью блочных симметричных шифров является использование сложной комбинации большого количества операций подстановок и перестановок. Многие такие шифры исполняются в несколько (иногда до 80) проходов, используя на каждом проходе «ключ прохода». Множество «ключей прохода» для всех проходов называется «расписанием ключей» (key schedule).

Типичным способом построения алгоритмов блочного симметричного шифрования является сеть Фейстеля, позволяющая строить схему шифрования на основе функции F(D, K), где D – порция данных, размером вдвое меньше блока шифрования, а K – «ключ прохода» для данного прохода. От функции не требуется обратимость – обратная ей функция может быть неизвестна. Достоинство сети Фейстеля заключается в почти полном совпадении процессов шифрования и дешифрования, что существенно облегчает аппаратную реализацию алгоритмов и, в частности, упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и дешифрования. Единственное отличие процесса дешифрования от шифрования в данном случаи состоит в использовании «ключей прохода» в расписании в обратном порядке.

Операции перестановки, применяемые в блочных симметричных криптосистемах, позволяют перемешивать биты данных по некоему закону и дают возможность достижения «эффекта лавины». Операция перестановки линейна: f(a) xor f(b) == f(a xor b). В аппаратных реализациях тривиально реализуется как перепутывание проводников.

Операции подстановки выполняются как замена значения некоей части сообщения (часто в 4, 6 или 8 бит) на стандартное, жестко встроенное в алгоритм иное число путем обращения к константному массиву. Операция подстановки обеспечивает в алгоритмах блочного симметричного шифрования нелинейность.

Характерной особенностью блочных криптоалгоритмов является тот факт, что в ходе своей работы они производят преобразование блока входной информации фиксированной длины и получают результирующий блок того же объема, но недоступный для прочтения сторонним лицам, не владеющим ключом. Таким образом, схему работы блочного шифра можно описать функциями Z = EnCrypt(X, Key) и X = DeCrypt(Z, Key).

Преобразование исходного текста (открытого текста) в шифротекст на основе блочных симметричных алгоритмов осуществляется с использованием следующих принципов:

- рассеивание (diffusion): изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;
- перемешивание (confusion): использование преобразований, затрудняющих получение статистических зависимостей между шифротекстом и открытым текстом.

Реализация данных принципов позволяет использовать блочный шифр для вычисления контрольных сумм пакетов данных и в хешировании паролей.

Среди систем симметричного шифрования известны алгоритмы блочного шифрования Mars и TwoFish, которые в 2000 г. вошли в число 5 финалистов конкурса выбора преемника для шифра DES, являвшегося американским стандартом шифрования AES (Advanced Encryption Standard) с 1977 года. Однако победителем конкурса стал алгоритм Rijndael, который и был принят в качестве стандарта [2].

Алгоритм шифрования Mars разработан и опубликован корпорацией IBM в 1998 г. Данный алгоритм позволяет обрабатывать исходный текст произвольной длины блоками данных размером 128 бит. Обработка блоков данных осуществляется в течение 32 раундов с использованием ключей длиной 128, 192, 256 и 1248 бит.

Особенностью алгоритма Mars является высокая криптографическая стойкость шифра, допускающая его эффективную реализацию как на 32-разрядных платформах, так и в ограниченных рамках, например, для организации защиты данных на смарт-картах.

Высокая криптографическая стойкость данного алгоритма достигается за счет применения:

- простейших операций: сложение, вычитание, исключающее или;
- подстановок с использованием таблиц замены;
- фиксированного циклического сдвига;
- зависимости операции циклического сдвига от обрабатываемых данных;
- умножения по модулю 232, основным достоинством которого является то, что старшие биты зависят от почти всех битов в операндах нелинейным способом;
- ключевого забеливания;
- двойного перемешивания, что обеспечивает сложность для криптоанализа.

К недостаткам алгоритма Mars исследователи относят достаточно большой размер табличных подстановок (512x4 = 2048 байт), что может сказаться на реализации в системах с ограниченными ресурсами ПЗУ [3]. Процедура расширения ключа и 32-разрядное умножение также достаточно сложны для слабых микрочипов, подобных смарт-картам и контроллерам. Из-за применения умножения и сдвигов на переменное число бит шифр потенциально нестоек к атакам по потребляемой мощности и времени исполнения. Алгоритм слабо поддается распараллеливанию.

Скорость декодирования при 128-битном ключе составляет 66 Мбит/с, при ключе, равном 256 бит, скорость равна 69 Мбит/с.

Алгоритм блочного симметричного шифрования Twofish является одной из наиболее удачных разработок компании Counterpane Internet Security, основанной и возглавляемой Брюсом Шнайером. Данный алгоритм позволяет обрабатывать исходный текст произвольной длины блоками данных размером 128 бит с использованием ключей длиной 128, 192 и 256 бит.

Достоинством алгоритма Twofish является возможность использования ключей шифрования с длинами, отличными от допустимых и не превосходящими 256 бит, и отсутствие «слабых» ключей.

Ключи с длинами, отличными от указанных и меньшими 256 бит, генерируются посредством дополнения их нулями до следующей большей из упомянутых основных длин.

Алгоритм Twofish использует 16-раундовую сеть Фейстеля (Feistel Network) с биективной (взаимно однозначной) функцией F и дополнительными «отбеливаниями» (Whitenings) на входе и выходе. Единственное отличие от «чистой» фейстелевской структуры заключается в наличии функциональных блоков, выполняющих циклические однобитовые сдвиги вправо и влево.

Преобразование 128-битового блока открытого текста осуществляется за 16 раундов с использованием двух функций. Первая (функция F) представляет собой

функцию трех аргументов: двух входных слов и номера раунда шифрования, необходимого для выбора надлежащих раундовых ключей. Вторая является функцией g и составляет основу алгоритма шифрования: входное 32-битовое слово X разбивается на четыре байта, каждый байт проходит S-box преобразование, зависящее от раундового ключа и описывающееся биективной функцией, преобразующей «входной» байт в «выходной».

Анализ алгоритмов блочного симметричного шифрования Mars и TwoFish и моделей их работы, реализованных в среде программирования C++ Builder 10, позволил выделить их основные характеристики и сделать следующие выводы:

1) общая безопасность: сложность алгоритмов реализации и анализа их безопасности;

2) программная реализации: эффективность программных реализаций зависит от процессора, т.к. требуется управлять операциями 32-битного умножения и переменной ротации;

3) окружения с ограничениями пространства: алгоритмы Mars и TwoFish недостаточно соответствует окружениям с ограничениями пространства, т.к. требует большого объема ROM, требования к которому имеют тенденцию роста;

4) аппаратные реализации: алгоритмы Mars и TwoFish имеют средние потребности, их эффективность ниже средней, скорость реализации зависит от используемой длины ключа;

5) шифрование и дешифрование: шифрование и дешифрование с помощью алгоритмов Mars и TwoFish имеют аналогичные функции, поэтому скорость при шифровании и дешифровании в обоих случаях существенно не изменяется;

6) свойства ключа: алгоритм Mars требует вычисления 10 из 40 подключей за один раз, требуя дополнительных ресурсов для хранения этих подключей, что неудобно для окружений с ограниченной памятью. Оба алгоритма требуют также однократного выполнения управления ключом для создания всех подключей до первого дешифрования с конкретным ключом. Вычисление нескольких подключей за один раз требует больше ресурсов памяти, чем при вычислении подключей на лету.

7)

Библиографический список

1. Мао Венбо. Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.

2. MARS и TwoFish – a candidate cipher for AES / Carolynn Burwick, Don Coppersmith, Edward D’Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas Jr, Luke O’Connor, Mohammad Peyravian, David Safford, Nevenko Zunic.

3. Алехина М.А., Лысенко А.М., Мельников Б.Ф. Об одном подходе к моделированию вычислительных устройств // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2007. №2. С. 2□9.

**Бобрышева Галина Владимировна**
Пензенский государственный университет, г. Пенза, Россия
E-mail: g_bobr@mail.ru

**Bobrysheva G.V.**
Penza State University,
Penza, Russia

**Звозникова Анна Олеговна**
Пензенский государственный университет, г. Пенза, Россия
E-mail: anna.zvoznikova.96@mail.ru

**Zvoznikova A.O.**
Penza State University, Penza, Russia