УДК 681.3.06:519.248.681

С.А. Сидченко[1], В.Л. Петров[2], А.А. Белокуров[2]

[1]*Харьковский университет Вооруженных Сил им. И. Кожедуба*
[2]*Объединенный научно-исследовательский институт ВС Украины, Харьков*

МЕТОДИКА ПРОЕКТИРОВАНИЯ И ТЕСТИРОВАНИЯ СИММЕТРИЧНЫХ БЛОЧНЫХ АЛГОРИТМОВ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ

Рассмотрены критерии и показатели оценки качества (безопасности) блочных симметричных криптографических алгоритмов преобразования информации. Предложена методика их проектирования и тестирования.

информационная безопасность, криптоанализ, проектирование, тестирование, симметричные блочные алгоритмы, преобразование информации

Введение

Постановка проблемы. В последнее время в области информационной безопасности разработано и разрабатывается много новых криптографических преобразований информации. Примером могут служить конкурсы на разработку новых стандартов криптографического преобразования AES [1], про-

водимый с 1997 по 2001 годы, и NESSIE [2], проводимый с 2000 по 2003 годы. Наиболее известен конкурс, объявленный Национальным Институтом Стандартов и Технологий (NIST), по созданию улучшенного стандарта шифрования (Advanced Encryption Standard – AES), в котором приняло участие 15 кандидатов (полная информация о ходе конкурса и документация к шифрам-кандидатам – в [1]).

Наибольшее практическое распространение получили блочные симметричные криптографические преобразования информации. Под ними понимаются преобразования, в которых прямое (шифрование) и обратное (расшифрование) преобразования выполняются над блоками фиксированной длины с использованием одного и того же (симметричного) ключа. (Фактически блочные преобразования представляют собой системы подстановки блоков.) Именно такими преобразованиями являются стандарты DES, AES, ГОСТ 28147-89.

Оценка безопасности преобразований этого класса является актуальной задачей, как в практическом, так и в теоретическом плане. NIST рассматривал эту проблему в процессе создания перспективного стандарта шифрования как очень важную, сложную и в значительной степени неопределенную.

Анализ литературы. Сравнению блочных симметричных преобразований информации и оценки их безопасности посвящено большое количество работ отечественных и зарубежных авторов, например, [1 – 7]. Так в [1, 3] рассмотрена концепция создания улучшенного стандарта шифрования AES, обсуждаются требования к нему, накладываются ограничения и проводится сравнительный анализ алгоритмов-кандидатов AES с целью выбора наиболее подходящего. В [4] проведен сравнительный анализ стандартов шифрования ГОСТ 28147-89 и AES-Rijndael с акцентом на технологичность и эффективность реализаций. В качестве вывода бело сделано предложение по оптимизации ГОСТа за счет перехода от замен в 4-битовых группах к байтовым заменам, что должно повысить стойкость алгоритма к известным видам криптоанализа. В [5] проводится анализ методов криптографической защиты информации и рассмотрены алгоритмы преобразования информации, получившие свое развитие до 1996 года. В [6] рассмотрена архитектура блочных криптографических преобразований информации, построенных на основе сети Фейстеля. В [7] и ряде других работ изложены новые результаты в направлении проектирования скоростных алгоритмов криптографического преобразований информации на основе управляемых преобразований.

Цель статьи. Предложить методику проектирования и оценки качества (безопасности) симметричных блочных криптографических преобразования информации с учетом опыта принятия улучшенного стандарта шифрования AES.

Изложение основного материала

При проектировании нового криптографического преобразовании информации, синтезе или выборе одного из уже существующих преобразований необходимо определиться с областью его дальнейшего применения, так как конкретные условия применения могут существенно повлиять на выбор общей схемы построения алгоритма преобразования информации и на этап оценивания его качества.

Критерии и показатели оценки качества криптографических алгоритмов преобразования информации. При проектировании нового криптографического преобразования информации, синтезе одного из уже существующих или оценки безопасности симметричных блочных алгоритмов преобразования информации предлагаются следующие критерии и показатели качества:

1. Удовлетворение минимальным требованиям, предъявляемыми пользователями, к алгоритмам преобразования.
2. Надежность архитектуры и математической базы криптографических преобразований.
3. Выбор длины ключевых элементов и расписания их использования.
4. Статистическая безопасность криптографических преобразований.
5. Реальная защищенность от криптоаналитических атак.
6. Производительность алгоритмов для программной и аппаратной реализаций.
7. Требования к памяти при программной и аппаратной реализациях.
8. “Гибкость” алгоритма.

Все перечисленные критерии можно свести в три большие группы.

Первой из них является стойкость. Она расценивается как самой важный фактор при оценке безопасности криптоалгоритмов. Под стойкостью понимаются следующие свойства преобразования – надежность (прочность) архитектуры преобразования и математической базы цикловой функции и “развертывания” ключа (выработка ключевых элементов); равновероятность выходных данных (статистическая безопасность); устойчивость алгоритма к криптоаналитическому вскрытию.

Ко 2-й группе относятся скорость и стоимость преобразования информации, которые определяются вычислительной эффективностью (скоростью) на разнообразных платформах, и требованием к памяти.

К 3-й группе относятся характеристики алгоритма и его реализации, такие как гибкость, простота, программная и аппаратная реализуемость.

Одна из самых больших проблем при оценке и сравнении разнообразных алгоритмов преобразования информации – это два конфликтующих между собой требования к конструкции преобразования: стойкость

и скорость. Упор на усиление одного из этих параметров неминуемо ослабляет другой. Рассмотрим эти критерии и показатели качества подробней.

Удовлетворение минимальным требованиям. При проектировании или выборе алгоритма преобразования информации пользователь предъявляет минимальные требования, которым он должен отвечать. На практике чаще всего выступают следующие требования:

1. Длина блока криптографического преобразования B (бит). На практике B = 64 или 128 бит.
2. Длины начальных ключей K (бит). На практике чаще всего K = 64, 128, 192 или 256 бит.
3. Гибкость – работа в различных комбинациях B/K.
4. Стойкость преобразования.
5. Скорость преобразования.

При этом стойкость криптографического алгоритма преобразования информации полагается наиважнейшим критерием оценки.

Безопасность симметричной криптосистемы является функцией двух факторов: надежности алгоритма и длины ключа. "Сильный" криптоалгоритм должен быть настолько безопасен, чтобы лучшего способа, чем вскрывать его грубой силой, не существовало.

Надежность архитектуры и математической базы криптографических алгоритмов. Все симметричные блочные преобразования имеют в своей основе следующую идею. Сообщение разбивается на блоки равной длины, и каждый блок преобразуется (шифруется или расшифровывается) с помощью одного и того же криптопреобразования, зависящего от секретного ключа. Для повышения стойкости это преобразование циклически повторяется несколько раз (итерируется).

Криптоалгоритмы этого класса являются предположительно стойкими, основанной на сложности решения частной математической задачи, которая не сводится к хорошо известным задачам (например, криптоалгоритмы DES, AES, ГОСТ 28147-89).

Основные различия алгоритмов, как правило, сводятся к различиям в архитектуре и цикловой функции. Можно выделить три основные группы архитектур криптопреобразований: сети Фейстеля, SP-сети, "неортодоксальные конструкции".

Сети Фейстеля бывают двух типов: классическая [8] и модифицированная. В классической архитектуре – блок разбивается на две равные половины, одна из которых комбинируется с ключом (выполняется цикловая функция), а затем складывается с другой половиной блока, после чего результат и исходная половина блока меняются местами. К модифицированной сети Фейстеля обычно относят конструктивно аналогичные преобразования, манипулирующие субблоками разной длины.

Кнудсен (Knudsen) в [9] определил следующие необходимые условия безопасности для преобразования Фейстеля: отсутствие простых отношений, все ключи одинаково хороши, устойчивость к дифференциальному и линейному анализам.

Среди кандидатов AES к "классической сети Фейстеля" можно отнести алгоритмы DEAL, DFC, E2, LOKI97, MAGENTA, TWOFISH, а "модифицированной сети Фейстеля" – CAST-256, MARS, RC6.

SP-сети ("сети замен-перестановок") – другая общераспространенная архитектура, ориентированная на распараллеленную нелинейную обработку всего блока данных. Цикловое преобразование заключается в прогоне всего блока текста через слои замен и перестановок, зависящие от ключа. К этой архитектуре относятся и два ее варианта часто встречающихся в печати:

– схема "*KASLT*" ("Key Addition – Substitution – Linear Transformation") – цикловая функция заключается в выполнении следующих операций: "прибавление ключевого элемента – подстановка – линейное преобразование";

– "*Квадрат*" (родоначальником архитектуры является алгоритм с аналогичным названием Square) – байт-ориентированная архитектура (блок представляется в форме матрицы байтов) с использованием двух простейших операций – сложения по модулю 2 и индексированного извлечения из памяти.

К этой группе принадлежат такие алгоритмы-кандидаты, как CRYPTON, Rijndael ("Квадрат"), SAFER+ и SERPENT("KASLT").

"*Неортодоксальные конструкции*". На практике это слабая архитектура. Среди AES-кандидатов было два шифра с такой архитектуры (FROG и HPC), которые не удовлетворяют требованиям стойкости, производительности и гибкости.

При проектировании преобразований, по мнению К. Шеннона [10], на практике необходимо использовать два общих принципа: рассеивание и перемешивание. Рассеивание представляет собой распространение влияния одного знака открытого текста на множество знаков шифртекста, что позволяет скрыть статистические свойства открытого текста. Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Шеннон выдвинул идею создания составного преобразования, удовлетворяющего принципам рассеивания и перемешивания, т.е. преобразования, которое может быть реализовано в виде некоторой последовательности простых преобразований, который вносит небольшой вклад в значительное суммарное рассеивание и перемешивание. Все перечисленные выше архитектуры являются составными преобразованиями.

В составных преобразованиях в качестве простых чаще всего используются следующие:

1. Побитовое сложение по модулю 2 (операция XOR – “логическое исключающее ИЛИ”).

2. Сложение с переносом (операция ADD): сложение числа X и Y по модулю 2^N, т.е. ADD: $(X+Y) \bmod 2^N$.

3. Умножение целых (операция MUL) чисел X и Y по модулю (2^N+1), т.е. MUL: $(X \otimes Y) \bmod (2^N+1)$. На практике можно рассматривать как разновидность S-блоков с N-входами и N-выходами.

4. Циклический сдвиг влево на M позиций (операция ROL):

$$\text{ROL: } (x_0, x_1, \ldots, x_{N-1}) \to (x_M, \ldots, x_{M-2}, x_{M-1}),$$

где $1 \le M \le N-1$; $x_i \in \{0, 1\}$; $i \in \overline{0, N-1}$.

Как частный случай выступает операция циклического сдвига влево на одну позицию:

$$(x_0, x_1, \ldots, x_{N-1}) \to (x_1, \ldots, x_{N-1}, x_0),$$

где $x_i \in \{0, 1\}$; $i \in \overline{0, N-1}$.

5. Циклический сдвиг вправо на M позиций (операция ROR):

$$\text{ROR: } (x_0, x_1, \ldots, x_{N-1}) \to (x_{M-2}, x_{M-1}, \ldots, x_{M-3}),$$

где $0 \le M \le N-1$; $x_i \in \{0, 1\}$; $i \in \overline{0, N-1}$.

Как частный случай выступает операция циклического сдвига вправо на одну позицию:

$$(x_0, x_1, \ldots, x_{N-1}) \to (x_{N-1}, x_0, \ldots, x_{N-2}),$$

где $x_i \in \{0, 1\}$; $i \in \overline{0, N-1}$.

6. Функция перестановки BP (byte permutation) и обратная ей BP^{-1}:

$$\text{BP: } (x_0, x_1, \ldots, x_{N-1}) \to (y_0, y_1, \ldots, y_{N-1});$$

$$BP^{-1}\text{: } (y_0, y_1, \ldots, y_{N-1}) \to (x_0, x_1, \ldots, x_{N-1}),$$

где $x_i, y_i \in \{0, 1\}$; $i \in \overline{0, N-1}$. Причем $BP = (BP^{-1})^{-1}$.

7. Функция расширения E, расширяющее l-битное число до d-битного.

8. Подстановка S-блоками (операция XLAT) преобразующая m-битное число в n-битное.

9. Невырожденное линейное преобразование

$$L(x_0, x_1, \ldots, x_{N-1}) = (x_0, x_1, \ldots, x_{N-1}) \cdot A,$$

где A – матрица над GF(2) с ненулевым определителем.

10. Аффинное преобразование

$$L_a(x_0, x_1, \ldots, x_{N-1}) = (x_0, x_1, \ldots, x_{N-1}) \cdot A + (a_0, a_1, \ldots, a_{N-1}),$$

где $a_i \in GF(2)$.

Кроме этого в [7] представлена классификация управляемых примитивов, на основе которых синтезируются новые классы операций, зависящих от преобразуемых данных или ключа, дается описание новых криптографических примитивов. Среди них управляемые битовые перестановки и подстановки, управляемые двухместные операции, операции циклического сдвига влево (вправо) на число бит, зависящих от ключа или преобразуемых данных.

На основе идеи Шеннона о создании составного преобразования в [11] предложен программно-ориентированный метод недетерминированного преобразования на основе комбинирования нескольких разнотипных цикловых функций с возможностью построения большого количества модификаций преобразования.

В [12] Брюс Шнайер отметил, что криптографическая система не может быть надежнее использованных в ней отдельных алгоритмов преобразования. Иными словами, для того чтобы преодолеть систему защиты, достаточно взломать любой из ее компонентов. Использование хороших строительных материалов еще не является гарантией прочности здания. Так и криптографическая система, построенная на основе мощных алгоритмов и протоколов, тоже может оказаться слабой.

Длина ключа преобразования и выработка сеансовых ключевых элементов. Современные преобразования (шифры) базируются на принципе Кирхгофа (“Kirchhoff”), который гласит, что секретность преобразования обеспечивается секретностью ключа, а не секретностью криптографического преобразования. Поэтому компрометация ключа ведет к раскрытию преобразования.

При проектировании преобразования длину ключа выбирают из предположения, что наилучшей атакой на него является полный перебор ключей (при этом сложность перебора всех возможных ключей растет экспоненциально с ростом числа битов ключа) с учетом перспектив развития вычислительной техники. С точки зрения статистики, надо перебрать примерно половину возможных ключей, прежде чем найдется правильный. Поэтому для ключа 128 бит необходимо перебрать 2^{127} возможных вариантов, прежде чем может найтись правильный ключ.

Оценка развития вычислительной техники во времени производится по закону “Мура” (Moore), который гласит, что для заданной стоимости вычислительная мощность увеличивается в 8 раз каждые 3 года. Если закон “Мура” будет продолжать выполняться (увеличение каждые 3 года длины ключа на 3 бита в 8 (2^3) раз больше возможных вариантов ключей), то в 2072 году можно подобрать полным перебором 128-битный ключ так же “легко”, как сейчас 56-битный.

На практике в большинстве алгоритмов длина ключа меньше, чем требуется для осуществления всех раундов преобразования (шифрования или расшифрования), что приводит к необходимости применения функции “расширения” ключей. В основу этих функции положены те же математические операции, которые используются и в цикловых функциях.

При выборе длины ключевого элемента и схемы его “расширения” необходимо исходить из архитектуры построения алгоритма преобразования. Это связано с тем, что ключевой элемент может использоваться и в качестве управляющего вектора для формирования алгоритма преобразования, как это показано в [7, 11]. Кроме разовых сеансовых ключей в криптоалгоритмах могут использоваться и долго-

временные ключи, в качестве которых могут выступать S-блоки (как в ГОСТ 28147-89). Методике их построения и анализу стойкости посвящены следующие работы [13 – 17].

Статистическая безопасность криптографических преобразований информации. Статистическая безопасность криптографических преобразований является основой для оценки безопасности выходных данных преобразования. Она проводится с использованием некоторого стандартного набора статистических тестов, объединенных единой методикой расчета необходимых показателей эффективности криптографического преобразования и принятия решения о случайности формируемых последовательностей. Решению этой задачи были посвящены ряд работ [1, 17 – 19].

За рубежом существуют следующие мощные библиотеки (программы) статистического тестирования NIST STS [20], Crypt-SX [21] и DIEHARD [22]. Наилучшим образом потребностям статистического тестирования симметричных блочных криптографических алгоритмов преобразования отвечает разработанный в 1999 году специалистами NIST (в рамках проекта AES) набор статистических тестов NIST STS (NIST Statistical Test Suite) и предложенная методика проведения статистического тестирования [20].

Основными методами определения статистической безопасности криптографических алгоритмов являются методы, связанные с расчетом связанности (корреляции блоков) криптограмм между собой и с входными блоками открытых текстов, а также определение избыточности криптограмм.

В математической статистике существуют ряд тестов, называемых критериями согласия для проверки функции распределения случайной величины на предмет ее соответствия теоретически ожидаемому закону распределения. Наиболее известным набором статистических тестов является набор из пяти тестов, предложенный Кнутом в [17]. Кроме этого примерами таких критериев согласия являются: Хи-квадрат (критерий Пирсона), критерий Колмогорова-Смирнова, критерий серий, частотный тест, последовательный тест, автокорреляционный тест, универсальный тест, тест повторений, сравнение тестов l-грамм, комбинирование тестов и другие (см. например [23]). Избыточность связана с зависимостью символов сообщений соответствующего алфавита и неодинаковой вероятностью их появления. Существование избыточности в зашифрованных текстах может исследоваться с использованием программ-архиваторов ZIP и RAR.

Криптоанализ (устойчивость к криптоаналитическим атакам). Под криптоанализом понимается наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Он также позволяет обнаружить слабые места в криптосистеме. Криптоанализ проводится с учетом того, что алгоритм преобразования (шифрования) известен криптоаналитику (правило Кирхгофа), он имеет в своем распоряжении шифртексты (преобразованные тексты) всех сообщений и может получить пары открытый текст/шифротекст. Исходя из этого, существуют следующие основные типы криптоаналитических атак:

– атака с известным шифртекстом (ciphertext only attack);

– атака с известным открытым текстом (known plaintext attack);

– атака с выбором открытого текста (chosen plaintext attack);

– адаптивная атака с выбором открытого текста (adaptive chosen plaintext attack);

– атака с выбором шифртекста (chosen ciphertext attack);

– адаптивная атака с выбором шифртекста (adaptive chosen ciphertext attack);

– атака с выбором текста (chosen text attack);

– атака с выбором ключа (chosen key attack).

При этом основными методами криптоанализа классических алгоритмов являются:

– метод встречи посередине;

– метод Полларда;

– дифференциальный криптоанализ (расширения для дифференциального криптоанализа, поиск наилучшей дифференциальной характеристики);

– линейный криптоанализ;

– интерполяционное вторжение;

– вторжение с частичным угадыванием ключа;

– вторжение с использованием связанного ключа;

– вторжение на основе обработки сбоев;

– поиск лазеек и др.

Большинство из перечисленных методов (в том числе линейный или дифференциальный криптоанализ), требуют гигантских вычислительных затрат и/или ресурсов памяти, огромного числа пар открытый/зашифрованный текст, представляя, таким образом, чисто теоретический интерес. От полного перебора ключа отличается лишь минимальным преимуществом, и срабатывают только в условиях ослабленной модели преобразования. Поэтому ни один из шифров-кандидатов AES за период анализа вскрыть не удалось.

Производительность алгоритмов. Оценка производительности работы криптоалгоритма производится на основе анализа числа тактов работы (скорости), необходимых для:

– преобразования (шифрования и расшифрования) одного блока данных;

– разворачивания ключа;

– настройки алгоритма или его части (например, формирования таблиц).

При этом преобразования должны исследоваться на эффективность в оптимизированных реализациях на языках Assembler, C (C++), Pascal и Java на различных платформах программно и аппаратно

(включая смарт-карты и FPGA-чипы).

Требования к памяти при программной и аппаратной реализациях. При аппаратной реализации оценивается числом логических элементов, при программной – количеством необходимой оперативной и постоянной памяти, в том числе для различных платформ и сред.

Гибкость алгоритмов преобразования. Под гибкостью понимается способность алгоритма работать с различными длинами ключей, блоков текста и раундов преобразования изменяя соотношение стойкость/скорость, возможность реализации алгоритма в качестве поточного шифра или генератора случайных чисел, алгоритма хеширования, возможность реализации на различных платформах и сред и т.д.

Большинство криптографических преобразований информации, исходя из архитектуры их построения, могут быть реализованы с переменной длиной блока, ключа и количества раундов (циклов) преобразования. Это актуально при выборе показателя быстродействие/стойкость, когда при получении большей стойкости можно пожертвовать быстродействием и, наоборот, при повышении стойкости пожертвовать быстродействием.

Рассмотрим этот подход применительно к цикловой функции криптографического преобразования ГОСТ 28147-89. Взаимосвязь размера блока преобразования (n), размера ключа (k) и количество раундов (r) преобразования определяется из соотношения

$$k \cdot z = n/s \cdot r, \qquad (1)$$

где n – размер блока преобразования; k – размер ключа преобразования; r – количество раундов преобразования; s – количество полублоков; z – количество раз использования ключа в схеме разворачивания.

Исходя из (1) можно получить соотношения для размера блока преобразования n, ключа k и количества раундов r:

$$n = \frac{k \cdot z \cdot s}{r};\ r = \frac{k \cdot z \cdot s}{n};\ k = \frac{n \cdot r}{z \cdot s}. \qquad (2)$$

Необходимо отметить, что при увеличении размера блока преобразования и увеличения количества полублоков уменьшает лавинный эффект. Но этот недостаток может быть компенсирован за счет увеличения раундов преобразования. Подходы к построению недетерминированного преобразования с возможностью построения большого количества модификаций представлены в [7, 11].

Методика проектирования и тестирования криптографических преобразований. Процесс проектирования, тестирования и выбора криптографического преобразования выглядит таким образом.

1. Изучается область применения криптографического преобразования.
2. Выдвигаются требования, предъявляемые пользователями, к алгоритму преобразования.
3. Выбирается архитектура и математическая база криптографического преобразований.
4. Строится алгоритм преобразования информации.
5. Выбирается схема расписания использования ключа.
6. Выдвигается нулевая гипотеза H_0 о безопасности (качестве), проверяемого алгоритма.
7. Проводится оценка качества по предложенным выше критериям и показателям.

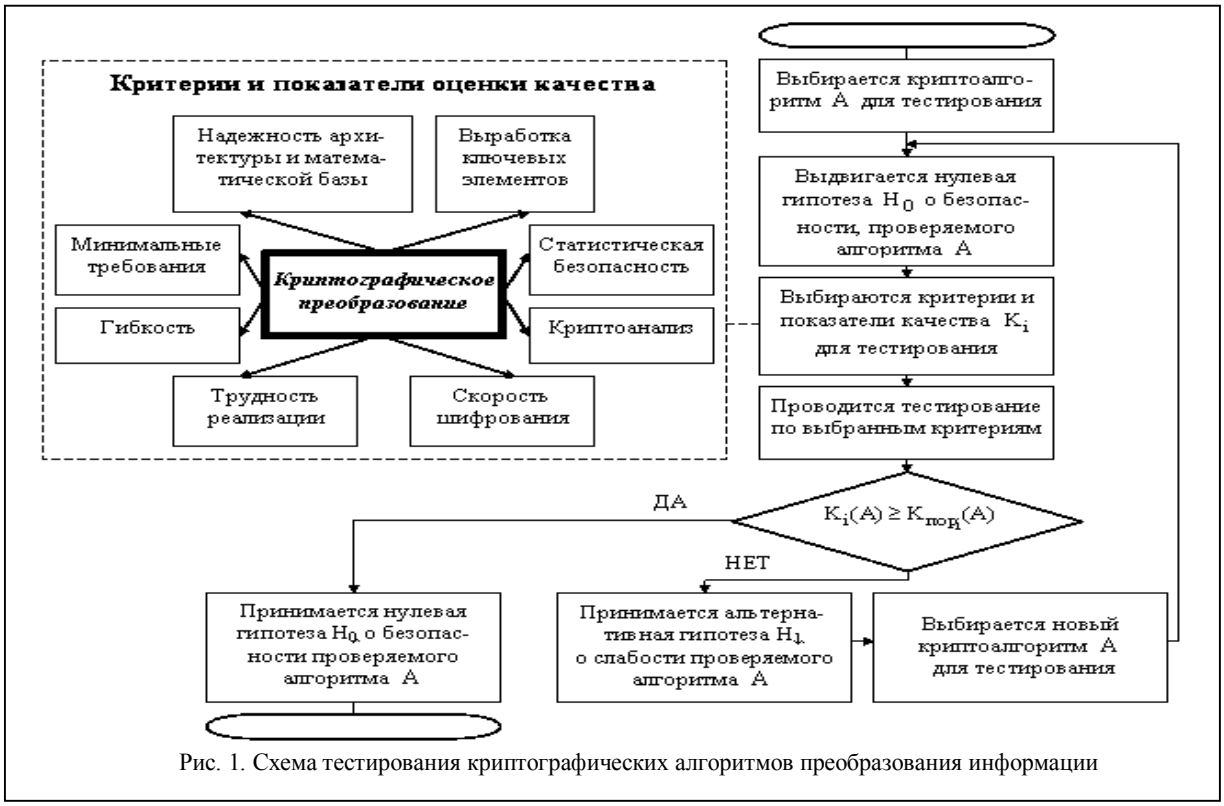

Рис. 1. Схема тестирования криптографических алгоритмов преобразования информации

8. На основе результатов оценки вычисляются значения вероятностей, которые сравниваются с уровнем значимости. В результате их сравнения выдвинутая гипотеза H_0 принимается или отвергается. Если гипотеза H_0 отвергается, то переходим к шагу 3.

9. Реализация предложенного алгоритма в программном и/или аппаратном виде.

Для принятия решения о прохождении тестирования могут использоваться критерии принятия решения на основе заданного порогового уровня, фиксированного доверительного интервала или вероятностного подхода. Значения уровня значимости рекомендуется выбирать из интервала [0,001; 0,01].

При этом этап анализа (тестирования) криптографического преобразования продолжается и в процессе его использования.

Схема тестирования криптографических алгоритмов преобразования информации представлена на рис. 1. Она может использоваться для решения следующих задач: тестирование, изучение, выявление слабых и разработка новых криптоалгоритмов.

Выводы

На практике использование готовой криптосистемы не гарантирует стопроцентного качества обеспечения безопасности. Это связано с тем, что большинство (если не все) криптосистемы, разработанные для частного (личного) использования, снабжены “черными входами”. Так в США в 1992 году был принят Билль S266, обязывавший всех американских разработчиков криптографического оборудования оставлять входы для Агентства национальной безопасности [24].

Для обеспечения безопасности информации необходимо использовать сертифицированные в Украине программно-аппаратные средства криптографической защиты.

Предложенная методика проектирования и оценки качества симметричных блочных алгоритмов преобразований информации может рассматриваться только как первичный анализ преобразования.

Список литературы

1. Computer Security Division [Электронный ресурс]. – Режим доступа: http://www.nist.gov.

2. NESSIE [Электронный ресурс]. – Режим доступа: http://www.cryptonessie.com.

3. Улучшенный стандарт симметричного шифрования XXI века: концепция создания и свойства кандидатов / М.Ф. Бондаренко, И.Д. Горбенко и др. // Радиотехника. – Х.: ХНУРЭ. – 2000. – Вып. 114. – С. 5-14.

4. Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США // Системы безопасности. – М.: Гротэ. – 2001. – №№ 1,2.

5. Schneier Bruce. Applied Cryptography. Second Edition: protocols, algorithms, and Source code // C. Published by John Wiley & SonS. Inc, New York: ChicheSter BriSbane Toronto Singapore, 1996. – 758 p.

6. INFUSED BYTES. Защита информации [Электронный ресурс]. – Режим доступа: http://www.enlight.ru/ib.

7. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – 448 с.

8. Horst Feistel. Cryptography and Computer Privacy // Scientific American. – May 1973. – Vol. 228, No. 5. – P. 15-23.

9. Knudsen L. Practically Secure Feistel Ciphers // Fast Software Encryption, Lecture Notes in Computer Science. – Springer-Verlag, 1993. – Vol. 809. –P. 211-221.

10. Шеннон К.Э. Работы по теории информации и кибернетике. – М.: Иностр. лит., 1963. – 829 с.

11. Сидченко С.А. Метод недетерминированного преобразования информации на основе комбинирования разнотипных цикловых функций. // Системи обробки інформації. – Х.: ХУ ПС. – 2006. – Вип. 6 (55). – С. 158-163.

12. Шнайер Брюс. Слабые места криптографических систем // Открытые системы. – 1999. – № 1. – С. 57-60.

13. Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. Всеукр. межвед. науч.-техн. сб. – Х.: ХНУРЭ. – 1997. – Вып. 103. – С. 121-130.

14. Лисицкая И.В., Олейников Р.В., Головашич С.А., Коряк А.С., Олешко О.И. Анализ стойкости DES подобных алгоритмов шифрования при использовании таблиц подстановок случайного типа. // Радиоэлектроника и информатика. – 1999. – № 1. – С. 111-114.

15. Лисицкая И.В., Головашич С.А., Олешко О.И., Олейников Р.В., Коряк А.С. Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. – 1999. – Вып. 50. – С. 185-194.

16. Горбенко И.Д., Лисицкая И.В., Коряк А.С. Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа. // Радиоэлектроника и информатика. – 1998. – № 1 (02). – С. 39-43.

17. Кнут Д. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т.2. – М.: Мир, 1977. – 700 с.

18. Потий А.В., Орлова С.Ю., Гриненко Т.А. Методика статистического тестирования генераторов случайных и псевдослучайных чисел // Радиотехника. – 2003. – № 3. – С. 57-61.

19. Security requirements for Cryptographic Modules. FIPS 140-1. – U.S. Department of Commerse. – 1994.

20. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // NIST Special Publ. 800-22, National Institute of Standards and Technology. – Gaithersburg, MD, 2000 [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/rng.

21. Gustafson H. et. al. Statistical test suite Crypt-SX. – [Электр. ресурс]. – Режим доступа: http://www.isrc.qut.

22. Marsaglia G. DIEHARD Statistical Tests. – [Электр. ресурс]. – Режим доступа: http://members.home.net.

23. Математический энциклопедический словарь. – М.: Советская энциклопедия, 1988. – 847 с.

24. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.

Поступила в редакцию 16.06.2006

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.