УДК 004.056.55

Маммадов Т.Э., Маммадов Э.Т.
Научно-производственное объединение «СЕЛЕН» НАНА, Баку, Азербайджан
t.e.mammadov@gmail.com

УВЕЛИЧЕНИЕ СТОЙКОСТИ СХЕМ ШИФРОВАНИЯ В СИММЕТРИЧНОЙ КРИПТОГРАФИИ

В работе предлагается новый подход для создания абсолютно стойкой симметричной схемы шифрования, где проблемы, связанные с постоянной генерацией ключей и их распределением, решаются за счет отказа от последних. Их функцию в новой схеме выполняют многочисленные комбинации шифралфавитов.

Ключевые слова: *абсолютная стойкость, симметричная криптография, ключ, одноразовый шифрблокнот, шифралфавит, количество комбинаций шифралфавитов.*

Введение

Во всех областях науки существуют устоявшиеся за многие десятилетия понятия и принципы, основываясь на которые проводятся научные исследования, целью которых является решение задач, вызванных постоянно появляющимися проблемами. Это имеет отношение и к такой области, как криптография, имеющая, как в настоящее время, так и в будущем важнейшее значение для информационной безопасности.

Появление в США суперкомпьютера «СЕКВОЙЯ» фирмы IBM производительностью 16,3 петафлопса (16,3 тысячи триллионов операций в секунду) и постоянные исследования с целью увеличения значения этого показателя в будущем заставляют специалистов, занимающихся вопросами информационной безопасности, самым серьезным образом совершенствовать существующие сегодня шифровальные алгоритмы. Машина с такой производительностью в состоянии вскрывать все существующие сегодня шифры. А это уже угроза государственной безопасности. Решение этой проблемы является важнейшей задачей, стоящей перед разработчиками стойких алгоритмов шифрования.

Как известно, дешифрование сообщений является одной из областей применения суперкомпьютеров. Принимая во внимание, что исследования и разработки по созданию еще более производительных вычислительных машин будут вестись постоянно, необходимо по-новому подходить к созданию новых, более усложненных схем шифрования, используя при этом все доступные методы и средства. Новая задача требует новых, нестандартных решений.

Все современные алгоритмы шифрования в симметричной криптографии являются комбинацией алгоритмов подстановки и перестановки. Результатом их применения является приведение информации в нечитабельную форму и наоборот. И не важно, каким методом это осуществляется. Главное, чтобы процесс шифрования был прост, удобен и обеспечивал высокую стойкость. Это особенно важно сегодня, когда существуют вычислительные машины нового поколения. Работы в этом направлении активно ведутся во всем мире.

Криптографы неустанно работают над своим собственным технологическим чудом – системой шифрования, которая вновь позволит обрести конфиденциальность даже в противостоянии с мощью квантового компьютера. Этот новый вид шифрования должен дать надежду на совершенную стойкость. Другими словами, у этой системы не будет изъянов и слабых мест.

Постановка задачи

Целью данной работы является попытка на основе накопленного многовекового опыта в области криптографии решить проблему недостаточной стойкости существующих современных шифров перед возможностями новых, высокопроизводительных суперкомпьютеров. При этом основное внимание уделяется разработке новой схемы симметричного шифрования, поскольку для этого вида шифрования требуется значительно меньше вычислительных ресурсов по сравнению с асимметричным видом шифрования (шифр RSA).

Метод решения

Условия, делающие шифр абсолютно стойким, а именно полная случайность ключа, равенство длины ключа и длины открытого текста и однократность использования ключа, делают его очень дорогим и непрактичным. Для создания абсолютно стойких, недорогих и удобных в использовании схем шифрования необходимо отойти от устоявшихся понятий и принципов и по-новому подойти к решению этой очень важной задачи, использовав накопленный многовековой опыт в этой области.

Все проблемы связаны с ключом – самым важным и секретным элементом любого криптографического алгоритма, без которого невозможно прочитать шифртекст. Однократность использования ключа при зашифровывании создает необходимость решения задач, связанных с постоянным распределением многочисленных ключей. Проблемы, связанные с этим, также делают шифр непрактичным.

Работа отдельных ключей в многоалфавитных шифрах происходит в двухкоординатной системе, где символы ключа – одна координата, а символы открытого текста – другая. Их комбинации непосредственно взаимодействуют с шифралфавитами. И если принять во внимание, что обычно ключами являются слова, словосочетания либо предложения, то в них, как правило, имеется достаточное количество одинаковых символов, что, в свою очередь, активирует одни и те же шифралфавиты. Это обстоятельство облегчает процесс криптоанализа.

Чтобы избавиться от проблем, связанных с использованием отдельных ключей, можно при разработке абсолютно стойкой схемы шифрования отказаться от них, использовав в качестве ключей запредельное количество комбинаций шифралфавитов. В этом случае для успешной атаки на шифр потребуются недостижимые вычислительные ресурсы.

Эту задачу можно решить, если по-новому использовать схемы шифрования известных полиалфавитных (многоалфавитных) шифров, несправедливо рано, по нашему мнению, отошедших на задний план, став частью истории. Усовершенствовав их, можно добиться абсолютно стойкого шифра без использования многочисленных отдельных ключей и тем самым избавиться от проблем, связанных с ними, в том числе и с их распределением.

Традиционная схема полиалфавитных шифров предусматривает постоянную работу ключа с несколькими шифралфавитами. При этом считается, что ключ является секретным элементом алгоритма, без которого невозможно произвести дешифрование. А разве шифралфавиты, используемые в схеме, публикуются в прессе? Без них, даже зная ключ, также невозможно произвести криптографическое преобразование. Схема шифрования может быть известна, однако секретными должны оставаться и многочисленные комбинации шифралфавитов, в постоянном распределении которых не будет необходимости при новом методе использования полиалфавитных шифров, так как они формируются в процессе криптографического преобразования автоматически, работая в режиме шагового сдвига. Более того, новая схема может обеспечивать зашифровывание каждого символа открытого текста отдельным, неповторяющимся

шифралфавитом только один раз. Не каждого слова, предложения или текста, а каждого символа.

Такая схема шифрования в силу использования запредельного количества комбинаций шифралфавитов скроет видимость циклического применения нескольких моноалфавитных шифров к определенному числу символов шифруемого текста. Именно это обстоятельство, по нашему мнению, сделает такую схему шифрования абсолютно стойкой.

Таким образом, например, если в преобразовании могут участвовать $4{,}8x10^{56.880}$ постоянно генерируемых комбинаций шифралфавитов, то в использовании дополнительных ключей отпадет необходимость, так как и без них провести успешную атаку, дискредитирующую атакуемый шифр, будет невозможно. Такое количество комбинаций алфавитов создаст огромное пространство решений при проведении полного перебора, который может не дать положительных результатов в течение нескольких лет или даже столетий.

В принципе такая схема шифрования не исключает использования и отдельного, даже самого простого, ключа, постоянная генерация которого для обеспечения абсолютной стойкости схемы шифрования не обязательна. Просто время, затрачиваемое на преобразование, будет увеличиваться.

Впервые в современной симметричной криптографии, вопреки устоявшимся правилам, схема может стать алгоритмом шифрования, не являющимся комбинацией двух алгоритмов – подстановки и перестановки, ибо новый способ сложной подстановки настолько увеличивает стойкость алгоритма, что в дополнительном применении второго алгоритма отпадает необходимость.

Как было отмечено выше, в новой схеме шифрования не используются отдельные ключи. Их роль выполняют постоянно обновляющиеся шифралфавиты. Другими словами, схема использует в качестве сверхдлинного ключа, состоящего из нескольких десятков тысяч символов (34.720), последовательность всех шифралфавитов, участвующих в процессе зашифровывания.

Это означает, что на практике длина ключа всегда будет больше длины сообщения. Эта последовательность используется не целиком, а частями, что существенно облегчает преобразование. Такой ключ состоит из десятков так называемых ключевых носителей (в нашем случае их число составляет 31), каждый из которых, в свою очередь, также состоит из десяти базовых шифралфавитов (ключевых составляющих), комбинации которых представляют собой абсолютно случайную последовательность 112 символов.

Схема такого ключевого носителя показана на рис.1. Ни одна комбинация этих алфавитов не повторяется ни в одном ключевом носителе. Один рабочий ключевой носитель в режиме шагового сдвига может зашифровывать один и тот же открытый текст по-разному 112 раз в зависимости от того, с какой начальной позиции и с какого шифралфавита начинается замена при заданной последовательности активирования последних.

Если учесть, что количество комбинаций последователь-ности из десяти шифралфавитов составляет 3.628.800, то один и тот же текст один рабочий ключевой носитель в состоянии зашифровать по-разному 3.628.800 x 112 = 406.425.600 раз.

Фактически каждый такой носитель, являющийся частью сверхдлинного ключа, представляет собой комплект из 406.425.600 ключей одноразовых шифрблокнотов, являющихся единственной известной нераскрываемой формой шифрования, с той лишь разницей, что он сам постоянно генерирует свои шифралфавиты, а потому очень удобен в работе.

Последовательность активирования шифралфавитов задается заранее отправителем, а информация об этом передается получателю с помощью нескольких дополнительных

символов в начале каждого шифртекста. Количество символов в алфавите открытого текста в такой схеме составляет 56.

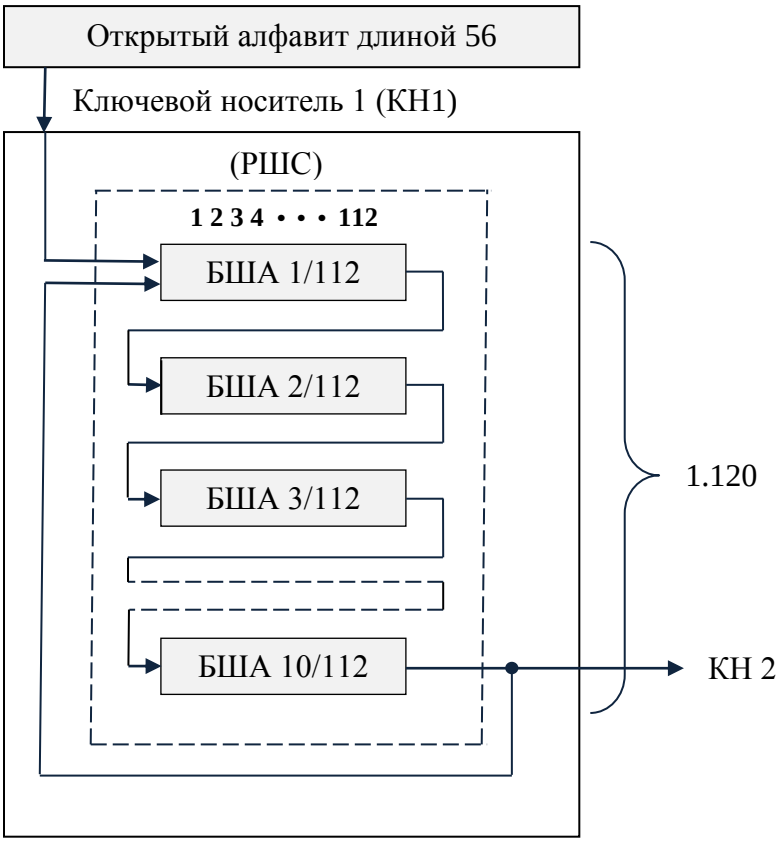

Рис.1. Схема ключевого носителя 1 (КН1)
РШС – режим шагового сдвига,
БША (1–10)/112 – базовые шифралфавиты (1–10) длиной 112

Таким образом, участвуя по выработанной схеме в процессе криптографического преобразования, такой ключ обеспечивает зашифровывание каждого символа открытого текста отдельным шифралфавитом. Возможность оперативной смены ключевых носителей при работе дает возможность увеличения скорости преобразования, так как разные отрезки открытого текста могут зашифровываться параллельно – каждый своим ключевым носителем, а затем объединяться в общий шифртекст и наоборот.

В схеме, в которой каждый ключевой носитель, работая в режиме шагового сдвига, когда каждая из 112 комбинаций, составляющих его десяти базовых шифралфавитов (ключевых составляющих) смещается относительно предыдущего положения на одну позицию, обеспечивая постоянную генерацию последних, каждый символ открытого текста независимо от числа его использования зашифровывается отдельной ключевой составляющей только один раз.

При таком режиме один ключевой носитель в состоянии заменять каждый символ открытого текста на 112 x 10 = 1.120 символов десяти ключевых составляющих. В этом случае замененные символы будут повторяться, однако это никакую путаницу при дешифровании создавать не будет, так как эти символы будут относиться к разным составляющим.

Другими словами, в начале зашифровывания каждого открытого текста отправитель выбирает ключевой носитель (один из 31-го), его начальную позицию (одну из 112), с которой начинается зашифровывание при шаговом сдвиге, и задает конкретную

последовательность активирования шифралфавитов. Что касается проблемы, связанной с распределением ключей, то она решается довольно просто.

С каждым шифртекстом посылаются дополнительно несколько символов, показывающих номер активируемого ключевого носителя, его начальную позицию в режиме шагового сдвига и последовательность активирования шифралфавитов. Разработанная модель шифровального устройства позволяет такую сверхсложную задачу решать просто и удобно. Общая схема шифрования показана на рис.2.

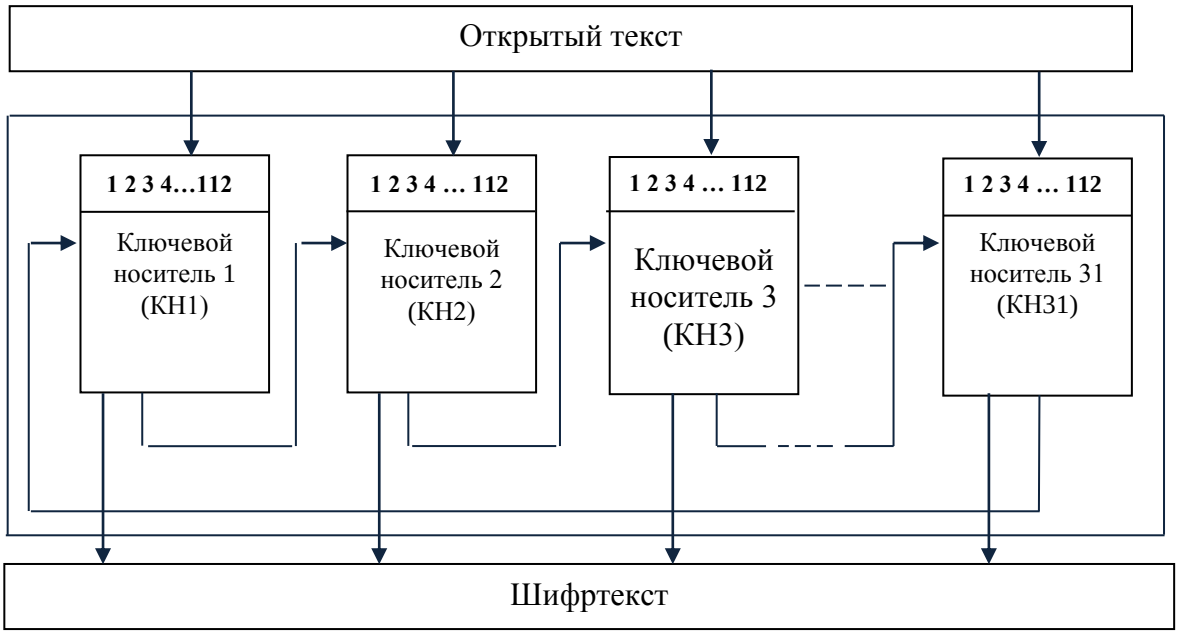

Рис. 2. Общая схема шифрования

Основные параметры шифра:

- используемая функция – подстановка;
- случайность ключа – полная;
- тип ключа – симметричный;
- использование ключа – один раз;
- метод – зашифровывание каждого символа открытого сообщения отдельным ключом;
- длина ключа – 34.720;
- количество комбинаций ключа – $4{,}8 \times 10^{56.880}$;
- мощность алфавита- 142;
- наименее затратный метод анализа – полный перебор ключа.

Потенциал алгоритма чрезвычайно высокий. Увеличивать длину ключа можно не только увеличением числа ключевых носителей и составляющих их шифралфавитов, но и увеличением мощности алфавитов и их длины. В нашем случае длина ключа (последовательность шифралфавитов 31-го ключевого носителя) составляет 34.720. В этом случае количество комбинаций его без учета мощности алфавита составит $4{,}8 \times 10^{56.880}$.

Внедрение полученных результатов

Рассматриваемая схема шифрования в силу исключительной простоты, удобства использования и абсолютной стойкости может быть немедленно внедрена после изготовления на основании действующей модели электромеханического шифровального аппарата. Это будет первым этапом внедрения. Вторым этапом будет создание на базе

разработанного алгоритма программного обеспечения. Это может стать тем случаем, когда очень серьезную и актуальную проблему возможно решить, используя неординарный метод.

Заключение

Таким образом, предложенная в данной работе схема шифрования может создать неразрешимые проблемы для криптоанализа, так как количество комбинаций символов в последовательности всех, используемых в схеме, шифралфавитов, выполняющих роль ключей, равна $4{,}8 \times 10^{56.880}$. Такое количество комбинаций не в состоянии «перемолоть» ни один современный суперкомпьютер. А если учесть, что выбор отправителем ключевого носителя, его начальной позиции и последовательности активирования шифралфавитов абсолютно случайный, то можно смело утверждать, что взломать такой шифр не в состоянии будет даже квантовый компьютер будущего.

Литература

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов.-М.: ДМК Пресс, 2012, 256 с.
2. Зубов А.Ю. Совершенные шифры.- М.: Гелиос АРВ, 2003, 160 с.
3. Сингх С. Книга шифров: тайная история шифров и их расшифровки / пер. с англ. А. Галыгина. М.: АСТ: Астрель, 2009, 447 с.
4. Бернет С., Пейн С. Криптография. Официальное руководство RSASecurity. Изд. 2-е, стереотипное. М.: ООО «Бином-Пресс», 2007, 384 с.
5. Баричев С.Г., Серов Р.Е. Основы современной криптографии: Учебное пособие.-М.: Горячая линия-Телеком, 2002.
6. Риксон Ф. Коды, шифры, сигналы и тайная передача информации / пер. с англ. А. Галыгина. М.: АСТ: Астрель; Владимир: ВКТ, 2011, 656 с.

UOT 004.056.55

Məmmədov Tofiq Ə., Məmmədov Emin T.
AMEA «SELEN» Elmi-istehsalat birliyi, Bakı, Azərbaycan
t.e.mammadov@gmail.com

Simmetrik kriptoqrafiyada şifrləmə sxemlərin davamlığının artırılması

Məqalədə tam davamlı simmetrik şifrləmə sxeminin yaradılması üçün yeni yanaşma təklif olunur. Burada açarların daim generasiyası və onların paylaşdırılması ilə bağlı problemlər onların istifadəsindən imtina etməklə həll olunur. Onların funksiyasını yeni sxemdə şifrəlifbaların çoxsaylı kombinasiyaları yerinə yetirir.

Açar sözlər: tam davamlıq, simmetrik kriptoqrafiya, tək açar, birdəfəli şifrbloknot, şifrəlifba, şifrəlifbaların kombinasiyalarının sayı.

Tofiq E. Mammadov, Emin T. Mammadov
«SELEN» Scientific-production association of ANAS, Baku, Azerbaijan
t.e.mammadov@gmail.com

Resistance increase of the enciphering schemes in the symmetric cryptography

In the article a new approach to the creation of an absolutely resistant symmetric enciphering scheme is suggested. Here the problems related to the constant generation of keys and their distributions are solved by avoiding their use. Their function in the new enciphering scheme has multiple combinations of cipher alphabets.

Key words: *absolute resistance, symmetric cryptology, separate key, one-time cipher pad, cipher alphabet, a number of cipher alphabets combinations.*