УДК 004.056(043.2)

В.А. Марченко

Институт кибернетики им. В.М. Глушкова НАНУ, Киев

КРАТКАЯ МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МЕТОДА КОСВЕННОГО ШИФРОВАНИЯ С ФИКСИРОВАННЫМИ КЛЮЧАМИ

В статье приводится краткая математическая модель косвенного шифрования с применением множества ключей фиксированной длины. Дан анализ современной ситуации в области разработки новых криптографических методов защиты информации, приведены некоторые рекомендации по разработке новых методов шифрования. Показано связь метода косвенного шифрования с классом нераскрываемых шифров. Описаны алгоритмы шифрования и расшифрования, а также некоторые особенности формирования используемого подмножества фиксированных ключей.

Ключевые слова: *шифрование, дешифрование, криптография, косвенное шифрование, нераскрываемые шифры*

Введение

Развитие современных средств вычислительной техники происходит настолько быстрыми темпами, что назрела необходимость изменить подходы к созданию систем защиты информационных систем в частности криптографических систем и протоколов.

Современные криптографические протоколы защиты разрабатываемы для телекоммуникационного оборудования и учитывают ожидаемым период эксплуатации порядка 10-15 лет (например протокол защиты wpa для WI-FI сетей). Но как оказалось появление принципиально новых вычислительных методов распараллеливания обработки информации позволило сократить время взлома ключа шифрования до нескольких часов, таким образом, значительно уменьшив защищенность передаваемой информации [1].

Состояние проблемы

В научной литературе известны два класса криптоалгоритмов:

- имеющих теоретически доказанную криптостойкость;
- имеющих практическую криптостойкость.

Основная масса современных шифров которые используются в информационных системах имеют только практическую криптостойкость которая основывается на нескольких условиях:

- текущим уровнем развития современных средств вычислительной техники;
- линейная интерполяция дальнейшего развития вычислительных средств.
- предполагаемый период эксплуатации криптоалгоритма.

Исходя из этих принципов и разрабатываются современных системы защиты информации, использующие криптографические методы защиты. Как показывает практика такой подход имеет серьезные изъяны.

Например, конкурс, проводимый американским агентством в 2000 на криптостандарт AES подтвердил, что присущее некоторым представленным алгоритмам ненакладное распараллеливания процессов выполнения шифрования и дешифрования не позволил пройти им начальные этапы отбора [2].

В связи с полученными результатами было предложено ряд новых рекомендаций, которые предлагаются для применения при построении современны криптографических систем защиты информации

1) теоретически доказанная криптостойкость;

2) оценка распараллеливания задачи с применением существующих вычислительных средств;

3) оценка криптостойкости с применением квантовых вычислений или других теоретических методов;

4) минимальный период гарантированной эксплуатации системы, составляющий порядка 30-50 лет;

5) применять скачкообразную интерполяцию для учета возможности появления новых средств или алгоритмов взлома.

На данном этапе развития криптологии известен только один класс алгоритмов обладающих теоретической криптостойкостью так называемые нераскрываемые шифры [3]. Самым известным представителем данного класса являются одноразовые блокноты. В известной работе [4] была доказана их информационная криптографическая стойкость соответственно применение этого алгоритма гарантирует нераскрываемость информации в долгий период эксплуатации.

В этой статье изложена краткая математическая модель метода косвенного шифрования [5]. Этот алгоритм имеет схожие свойства с классом нераскрываемых криптоалгоритмов описанных К. Шенноном и достаточно подробно проанализированных позже [6].

Метод косвенного шифрования

Пусть X и Y — конечные множества шифрвеличин и шифробозначений, с которыми оперирует алгоритм шифрования,

$$|X|>1,|Y|>1,|Y|\geq|X|$$

Это означает, что открытые и шифрованные тексты представляются словами в алфавитах X и Y соответственно.

В общем, случаи процесс зашифрования открытого текста $x = x_1..x_t$ заключается в замене каждой шифрвеличины x_t на некоторое шифробозначение y_i, $i=\overline{1,l}$ в соответствии с одним из $n, n>1$ инъективных отображений $e_j : X \to Y$ индексированных числами $j \in K = \{0,1,..,n-1\}$ где K – множество ключей. Каждое слово $x_t \in X$ представляет собой набор $b=\overline{1,s}$ букв формирующих слова из алфавита X.

Согласно [6] для всякого нераскрываемого шифра существует опорный шифр. Для метода косвенного шифрования это представляется совокупностью

$$\sum = (X, K, Y, E, D)$$

$K - \{0,1,\ldots,n-1\}$ – множество ключей;

$E - \{e_j, j \in K\}$ – множество правил зашифрования;

$D - \{d_j, j \in K\}$ – множество правил расшифрования.

Для метода косвенного шифрования

$$|X| = |Y| \neq |K|$$

поэтому он относится к классу нераскрываемых шифров с ограниченным ключом.

Множество ключей определяется как матрица следующего вида

$$K = \begin{Bmatrix} k_0 \\ \vdots \\ k_s \end{Bmatrix} \text{ - набор ключей,}$$

где $k_s = \overline{1,m}$ ключ фиксированной длины.

Длина фиксированного ключа определяется по формуле

$$l = a^w$$

$$a = |X| = \sum b,\ w = \min x_i$$

где w – длина минимальной лексемы алфавита X;

a – количество букв используемого алфавита.

Размер матрицы ключей K определяется как

$$s = \overline{1,n}$$

$$n = \sum_t |x_t|$$

$$|x_t| = \frac{x_t}{w}$$

Сам фиксированный ключ k_s имеет длину $|k_s| = l$ при этом мощность $|K| = A_l^l = l!$. Принцип формирования фиксированного ключа соответствует классической схеме размещения [7] при этом для любого $k_s^m \in k_s$ где $m = \overline{1,l}$

$$p\left(k_s^m\right) = \frac{1}{l},$$

то есть для любого k_s^m априорная вероятность размещения в любой позиции m фиксированного ключа k_s одинаковая для всех позиций.

В общем, случаи из вышесказанного следует что

$$`p\left(k_s^m\right) \neq p'\left(k_s^m\right)$$

где `p – априорная вероятность, а p' – апостериорная вероятность.

Таким образом, априорная вероятность появления заданного символа в заданной позиции неравна апостериорной вероятности его появления в этой же позиции. Но для самих фиксированных ключей k_s

$$`p\left(k_s\right) = p'\left(k_s\right)$$

т.е. априорная вероятность создания фиксированного ключа k_s равна апостериорной вероятности его повторной генерации, так как любое подмножество фиксированных ключей $\{k_{s-1}, k_s, k_{s+1}\} \in K$ никак не связано между собой. Соответственно обладая какой-либо апостериорной информацией о фиксированном ключе k_s нельзя определить априорную информацию для любого ключа k_{s-1} и k_{s+1} из множества K.

Например, для современной вычислительной техники, которая оперирует байтами значение $w = 8$, $a = 2$. Таким образом, длинна фиксированного ключа будет равняться $m = 256$ байт. По-сути каждый фиксированный ключ представляет множество неповторяющихся минимальных лексем используемого алфавита. Поэтому общее количество всевозможных ключей определяется как m!. Для указанного примера это будет определяться как 256!. Исходя из описанных особенностей используемых фиксированных ключей k_s в принципе не существует слабых ключей или ключей не пригодных к использованию при шифровании данных.

Вопросы генерации, передачи и хранения ключей, а также применяемые при этом методы и алгоритмы выборки подходящих ключей выходит за рамки статьи и не рассматриваются в данной работе. В общем, случаи требования к сгенерированным ключам идентичны требованиям, которые выдвигаются для ключей, используемых в алгоритме одноразовых блокнотов.

Следует отметить, что сам алгоритм занимает промежуточное положение между блоковыми и потоковыми криптоалгоритмами. В практическом применении алгоритм позволяет реализовать потоковое шифрование, но при этом будет оперировать для приведенного примера используемого алфавита блоками по восемь бит, а в остальном полностью быть подобным потоковым шифрам с выполнением соответствующих требований. Метод косвенного шифрования характеризируется тем, что оперирует только целыми словами из X и Y.

Алгоритм шифрования

Процесс шифрования происходит следующим образом исходный текст x, предназначенный для шифрования, разбивается на шифрвеличины $x_1,..,x_t$ таким образом, что длинна любой полученной лексемы $x_t = w$. После этого каждая шифровелечина x_t заменяется на соответствующее шифробозначение y_i согласно нижеописанного алгоритма.

Генерируется каким-либо образом множество ключей K. Это множество и представляет собой ключ шифрования, которым должны обладать получатель и отправитель шифрограммы.

Из полученного множества ключей K выбирается такое k_s для которого выполняется условие истинности символа Кронекера

$$\delta_{ts} = \begin{cases} 1, t = s \\ 0, t \neq s \end{cases}$$

где t – порядковый индекс текущего значения x_t относительно начала открытого текста x передаваемого на шифрование; s – порядковый индекс фиксированного ключа k_s относительно начала множества ключей K выбранных для шифрования.

Значение k_s определяется как текущее значение ключа шифрования для текущей лексемы открытого текста x и разбивается на вектор значений $(k_s^0,..,k_s^m)$ где

$$\left|k_s^m\right| = w$$

Находится такое значение k_s^m в выбранном текущем фиксированном ключе k_s для которого выполняется условие $k_s^m = x_t$. В виду применения вышеописанных правил формирования фиксированных ключей такое значение будет единственным в текущем k_s. Полученный индекс m записывается как текущее значение шифробозначения y_i для текущего значение открытого текста x_t.

Данный алгоритм выполняется циклически для всех $x_t \in x$ в виде набора вышеописанных преобразований.

В общем случаи, длинна полученного шифротекста будет равняться длине исходного текста $|x| = |y|$, при этом $|K| = |x| = |y|$.

Алгоритм расшифрования

Процесс расшифрования происходит по схожему алгоритму описанному выше, зашифрованный текст y, разбивается на шифробозначения $y_1,..,y_i$ таким образом, что длинна каждого шифробозначения равна $y_i = w$. После этого каждая y_i заменяется на соответствующую шифрвеличину x_t согласно алгоритма описанного ниже.

Выбирается множество ключей K с помощью которого был зашифрован текст x. Из этого множества выбирается такое значение k_s, для которого выполняется условие истинности

$$\delta_{is} = \begin{cases} 1, i = s \\ 0, i \neq s \end{cases}$$

где i – порядковый индекс текущего значения y_i относительно начала шифротекста y передаваемого на расшифрование; s – порядковый индекс фиксированного ключа k_s относительно начала множества ключей K выбранных для расшифрования.

Значение k_s определяется как текущее значение ключа расшифрования для текущей лексемы шифрограммы y и разбивается на вектор значений $(k_s^0,..,k_s^m)$ где

$$\left|k_s^m\right| = w$$

Находится такое значение k_s^m в выбранном текущем фиксированном ключе k_s, для которого верно условие

$$\delta_{ym} = \begin{cases} 1, y = m \\ 0, y \neq m \end{cases}$$

Так как используемые фиксированные ключи были сформированы согласно вышеописанных правил то такое значение будет единственным в текущем k_s. Полученное значение k_s^m записывается как текущее значение x_t открытого текста x. Данный алгоритм выполняется для всех $y_i \in y$ в виде набора вышеописанных преобразований.

В общем случаи длинна полученного открытого текста будет равняться длине шифротекста $|x| = |y|$, при этом $|K| = |x| = |y|$.

Практические аспекты использования метода

В методе косвенного шифрования используется один базовый алфавит для определения X, Y, K. В

виду чего это свойство имеет важное практическое значение, в частности оно, позволяет говорить, что любое подмножество открытых текстов $x \in X$ одновременно может выступать подмножеством шифробозначений $y \in Y$, а также и подмножеством ключей шифрования $k \in K$ которые используются для шифрования и расшифрования.

Исходя из особенностей формирования множества ключей K при составлении фиксированных ключей $k \in K$ получается избыточность в плане объема генерируемого ключевого потока для шифрования единого входного символа

$$r = \frac{l \cdot w}{w} = l$$

Таким образом, необходимо в r раз больше сгенерировать единичных лексем для построения фиксированных ключей, что бы зашифровать какую-либо лексему x_t. Но эта особенность позволяет утверждать, что информационная энтропия для фиксированных ключей шифрования будет определяться как

$$H(K) = -\sum P(K)\log P(K) = \log l$$

ввиду выполнения условия равновероятносного распределения (1). Такая информационная энтропия характерна для нераскрываемых шифров и является одним из базовых требований к подобным алгоритмам.

Для приводимого алфавита на основе байт необходимо сгенерировать $r = 256$ байт ключа для шифрования одного байта открытого текста. А информационная энтропия ключевого потока $H(K) = \sum \frac{1}{256}\log\frac{1}{256} = 8$.

Выводы

Приведенный метод косвенного шифрования позволяет использовать в различных информационных системах алгоритмы шифрования с доказуемой криптостойкостью, хотя это и связанно с рядом технических трудностей. Так основной проблемой использования подобных алгоритмов является трудность генерации случайного ключевого потока. Основным решением указанной проблемы является использование криптостойких генераторов псевдослучайных чисел (КГПСЧ), что переводит проблему в плоскость разработки таких генераторов. Но описанный метод нетребователен к параметрам подобных генераторов, так как напрямую не использует получаемый ключевой поток.

При использовании алфавитов, таких как байты, получаемые шифрограммы слабоотличымы от исходного шифротекста, что позволяет применять данный метод в задачах стеганографии.

В дальнейшем предполагается разработка новых подходов для применения быстрых КГПСЧ но с относительно низкой криптостойкостью без уменьшения криптостойкости самого метода шифрования.

Список литературы

1. *Tews E., Beck M. Practical attacks against WEP and WPA // Proceedings of the second ACM conference on Wireless network security. – ACM, 2009. – P. 79-86.*
2. *Report on the Development of the Advanced Encryption Standard (AES). – NIST, 2000. – 116 p.*
3. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — М.: "ГелиосАРВ", 2005. – 480 с.*
4. *Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Изд. иностр. лит., 1963. – с. 333 – 369.*
5. *Алишов Н.И., Марченко В.А., Оруджева С.Г. Косвенная стеганография как новый способ передачи секретной информации // Комп'ютерні засоби, мережі та системи: зб. наук. пр. – К.: НАНУ, Ін-т кібернетики, 2009. – № 8. – С. 105–112.*
6. *Зубов А. Совершенные шифры. — М.: Гелиос АРВ, 2003. – 160 с.*
7. *Кофман А. Введение в прикладную комбинаторику.— М.: Наука, 1975. – 480с.*

Надійшла до редколегії 27.03.2012

Рецензент: д-р техн. наук, проф. Н.А. Алишов, Институт кибернетики им. В.М. Глушкова НАН Украины, Киев.

КОРОТКА МАТЕМАТИЧНА МОДЕЛЬ МЕТОДА НЕПРЯМОГО ШИФРУВАННЯ З ФІКСОВАНИМИ КЛЮЧАМИ

В.А. Марченко

У статті приводиться коротка математична модель непрямого шифрування із застосуванням множини ключів фіксованої довжини. Дано аналіз сучасної ситуації в області розробки нових криптографічних методів захисту інформації, наведені деякі рекомендації з розробки нових методів шифрування. Показано зв'язок методу непрямого шифрування із класом шифрів, що не розкриваються. Описано алгоритми шифрування й розшифрування, а також деякі особливості формування використовуваної підмножини фіксованих ключів.

Ключові слова: *шифрування, дешифрування, криптографія, непряме шифрування, шифри що не розкриваються.*

BRIEF MATHEMATICAL MODEL INDIRECT METHOD OF ENCRYPTION WITH A FIXED KEY

V.A. Marchenko

The article summarizes the mathematical model of indirect encryption keys using a set of fixed length. The analysis of the current situation in the development of new cryptographic techniques to protect the information provides some guidance on the development of new methods of encryption. Showing the method of indirect communication with the class of undisclosed encryption ciphers. We describe the encryption and decryption, as well as some features of the formation used by a subset of fixed keys.

Keywords: *encryption, decryption, cryptography, indirect encryption, cipher with the perfect secrecy property*