эффективностями их реализации, с учетом ограничений на суммарную стоимость реализации механизмов защиты, обладает устойчивой сходимостью и может быть применен для решения поставленной задачи.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. Новиков А., Тимошенко А. Построение логико-вероятностной модели защищенной компьютерной системы. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– 2001.– Вип. 3. – с. 101–105. 3. ISO/IEC 7498-1: 1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. 4. О. М. Новіков, А. О. Тимошенко. Логіко-функціональні моделі безпеки інформації в інформаційно-обчислювальних системах з відкритою архітектурою. – Наукові вісті Національного технічного університета України "Київський політехнічний інститут".– 2002.– № 2. 5. Реклейтис Г., Рейвиндран А., Рэгсдел К. Оптимизация в технике: Кн.1. Пер. с англ. – М.: Мир, 1986. 6. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. – М.: Наука. Главная редакция физико-математической литературы, 1984. 7. М. С. Финкельштейн. Надежность и живучесть радиоэлектронных устройств. – М.: Отраслевая система НТИ, 1990. 8. Волкович В. Л., Волошин А. Ф., Заславский В. А., Ушаков И. А. Модели и методы оптимизации надежности сложных систем. – Киев: Наукова думка, 1993. 9. ISO/IEC 7498-2:1989, Information processing systems – Open Systems Interconnection - Basic Reference Model – Part 2: Security Architecture. 10. ISO/IEC 10181-1: 1996, Information technology – Security frameworks for open systems: Overview. 11. ISO/IEC 10181-2: 1996, Information technology – Security frameworks for open systems: Authentication framework. 12. ISO/IEC 10181-3: 1996, Information technology – Security frameworks for open systems: Access control framework. 13. ISO/IEC 10181-4: 1996, Information technology – Security frameworks for open systems: Non repudation framework. 14. ISO/IEC 10181-5: 1996, Information technology – Security frameworks for open systems: Confidentiality framework. 15. ISO/IEC 10181-6: 1996, Information technology – Security frameworks for open systems: Integrity framework.

УДК 681.3.067:681.3.016

ЗОЛОТОЕ СЕЧЕНИЕ В ШИФРОВАНИИ ДАННЫХ

Виктор Мясоедов
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Безопасность информационных технологий начинается с защиты данных в коммуникациях независимо от открытости используемого канала. Безопасность данных в открытых каналов предполагает абсолютную стойкость шифрующего алгоритма. Здесь описан простой и эффективный алгоритм, удовлетворяющий всем необходимым требованиям, обеспечивающий практически неограниченную длину шифрующей последовательности.**
Summary: **Information technologies security begins with data proof in communications regardless open or close channel of communication used. Data security in open channels requires that coding algorithm should be absolutely non-vulnerable. Here is described the simplest and the most effective algorithm with required property, which provides all necessary demands to coding algorithms, and unbounded code key length as well.**
Ключевые слова: **Принцип Кирхгофа, периодичность, невырожденность, нефальсифицируемость, непрогнозируемость, тотальность, золотое сечение, числа Фибоначчи, административный стандарт, интегрированные интеллектуальные системы.**

I Введение

В обзоре алгоритмов шифрования для передачи данных в открытых сетях [1] перечислены формальные и существенные положения шифрования, пригодные для написания "know how". Вместе с тем, в число положений включено требование, не оправданное ни теоретически, ни практически. Речь идёт о реализуемости "know how" [2], выходящего за пределы условия разрешимости уравнения шифрования относительно ключа при известных открытых и зашифрованных данных.

Предметом рассмотрения является генератор Фибоначчи псевдослучайных последовательностей {t}: $u_1=v_1$, $u_2=v_2$; $t=u_1+u_2$, $u_2=u_1$, $u_1=t$, где v_1, v_2 – численно независимые начальные значения ключа, например, математические константы π и e. На деле используются двоичные представления этих констант определённой длины и длинное двоичное сложение. Последний бит переполнения при двоичном сложении игнорируется. Выходным значением генератора является старший байт числа t, применяемый для шифрования/дешифрования байта данных командой "исключающее ИЛИ". Реально используемые начальные

значения получаются из поставленных прокруткой генератора в течение интервала времени, значительно превышающего величину, обратную тактовой частоте процессора.

II Постановка задачи

Требуется исследовать периодичность, прогнозируемость, вырожденность, фальсифицируемость и тотальность порождаемой генератором Фибоначчи последовательности значений ключа и шифрующих байтов при условии максимальной неопределённости начальных значений генератора.

Апериодичность последовательностей псевдослучайных чисел невозможна из-за конечности ресурсов вычислительной техники. На практике это значит, что управляемая периодичность не является недостатком генерируемых последовательностей и должна быть точно оценена, так же как и возможная апериодическая часть. В генераторе Фибоначчи последовательность практически апериодична за счёт произвола в выборе длины ключа l_1.

Невырожденность псевдослучайной последовательности во многих случаях представляет серьёзную проблему из-за известной теоремы Колмогорова о сходимости почти всюду случайных процессов к вероятности 0 или 1, что на практике приводит к генерации одного и того же шифрующего байта, начиная с некоторого момента. Поэтому в процессе генерации необходимо использовать алгоритмы, относительно которых можно доказать иррациональность пределов последовательности какой-либо комбинации операндов с независимостью этого свойства и предела от начальных значений. Таким свойством обладает генератор Фибоначчи $t=u_1+u_2$, $u_2=u_1$, $u_1=t$, так как не усечённые слева числа имеют вид $t_k = f_k v_1 + f_{k-1} v_2$, где f_k – числа Фибоначчи, $f_k = f_{k-1}+f_{k-2}$, $f_0=1$, $f_1=1$. Поэтому последовательность отношений t_k/t_{k+1} не усечённых слева чисел независимо от начальных значений v_1, v_2 сходится к известному иррациональному числу $\left(\sqrt{5}-1\right)/2$, называемому "золотым сечением" [3], так что последовательность Фибоначчи генерируется заново с любого момента псевдослучайного процесса. Поэтому усечение текущего значения ключа при отбрасывании последнего бита переноса в старший разряд не изменяет теоретических свойств генерируемой последовательности псевдослучайных чисел.

III Основная часть

Последовательность всевозможных значений ключа конечна в силу ограничения этих значений усечением слева. Более того, из всего множества чисел 0, 1, 2, 3, … , $2^{l_1+1}-1$, исключены некоторые, но не все, числа, представляющие укороченные ключи ("двоичные нули справа"). Примеры обобщённых последовательностей Фибоначчи, вычисляемых по модулю 2^{l_1+1}, $z_{k+1} \equiv f_k v_1 + f_{k-1} v_2 \pmod{2^{l_1+1}}$, где $f_{k+1} = f_k + f_{k-1}$ – числа Фибоначчи [1], для небольших l_1 показывают, что все они периодичны с периодом $3*2^{l_1-1}$.

Теорема 1. Обобщённая последовательность Фибоначчи, вычисляемая по модулю 2^{l_1+1}, периодична с периодом $3*2^{l_1-1}$.

Доказательство проводится методом математической индукции. Пусть $l_1=1$, $z_1=1$, $z_2=0$, или $z_1=0$, $z_2=1$, или $z_1=1$, $z_2=1$. Случай $z_1=0$, $z_2=0$ исключается из рассмотрения, поскольку означает, что l_1 на деле равно нулю. Очевидно, что во всех остальных случаях период последовательности z_2, z_1 ; z_1+z_2, z_2, z_1, … (mod 2) равен трём.

Предположим, что последовательность $z_k \pmod{2^{l_1}}$, k=1, 2, … , 2^{l_1}, периодична с периодом $3*2^{l_1-1}$, и докажем,что последовательность $x_k \pmod{2^{l_1+1}}$ с начальными значениями $x_1 = w_1 | z_1$, $x_2 = w_2 | z_2$, которые получаются сцеплением пар слов w_1, z_1 и w_2, z_2, где w_1, w_2 – однобитовые слова, периодична с периодом $3*2^{l_1}$. Тогда по принципу математической индукции теорема будет доказана для всех $l_1 \geq 1$.

В самом деле, последовательность $x_k \pmod{2^{l_1+1}}$, k=3, 4, … может быть представлена сцеплениями слов, в которых первый бит вычисляется по модулю 2 с помощью последних битов переполнения λ_k при

двоичном сложении слов z_{k-1}, z_{k-2}, имеющих длину 2^{l_1}:

2 w_2	$\mid z_2$
1 w_1	$\mid z_1$
_____	
3 $w_1 + w_2 + \lambda_3$	$\mid z_3$
4 $w_2 + \lambda_3 + \lambda_4$	$\mid z_4$
5 $w_1 + \lambda_4 + \lambda_5$	$\mid z_5$
6 $w_1 + w_2 + \lambda_3 + \lambda_5 + \lambda_6$	$\mid z_6$
……...	
……...	
……...	
3∗i $w_1 + w_2 + \lambda_3 + \lambda_5 + \ldots + \lambda_{3i-3} + \lambda_{3i-1} + \lambda_{3i}$	$\mid z_{3i}$
3∗i+1 $w_2 + \lambda_3 + \lambda_4 + \ldots + \lambda_{3i} + \lambda_{3i+1}$	$\mid z_{3i+1}$
3∗i+1 $w_1 + \lambda_4 + \lambda_5 + \ldots + \lambda_{3i+1} + \lambda_{3i+2}$	$\mid z_{3i+2}$
……...	
……...	
……...	

Последовательность $z_{k+2} \pmod{2^{l_1}}$ периодична с периодом $3*2^{l_1-1}$, поэтому периодична с той же длиной периода и последовательность битов λ_{k+2}. Так как сложение в битовой части слов x_{k+2} производится по модулю 2, то во втором периоде в текущей битовой части последовательно удваиваются и исчезают из всех последующих битовых частей биты λ_3, λ_4, λ_5, …, так что к концу второго периода восстанавливаются исходные значения последовательности $x_k \pmod{2^{l_1+1}}$:

$3*2^{l_1}$ -2 w_2	$\mid z_2$
$3*2^{l_1}$ -1 w_1	$\mid z_1$.

Поэтому рассматриваемая последовательность слов $x_k \pmod{2^{l_1+1}}$ периодична 2^{l_1+1} с периодом $3*2^{l_1}$, и, значит, утверждение теоремы верно для всех l_1, что и требовалось доказать.

Имеется $2^{l_1+1} - 3*2^{l_1-1} = 2^{l_1-2}$ неиспользуемых возможных значений ключа. Это создаёт резерв для выбора начальных значений.

Вместе с тем, среди намеченных к использованию ключей имеются и короткие ключи ("двоичные нули справа"), периодически появляющиеся в порождаемой последовательности, что в принципе позволяет прогнозировать появление некоторых шифрующих байтов, а это недопустимо. Решением, не затрагивающим стоимость вычислений, является подавление выдачи шифрующих байтов такими значениями ключа, т. е. программа должна иметь три точки входа в практически идентичные секции рабочего модуля. При этом периодичность последовательности шифрующих байтов составит теперь 2^{l_1}.

Теперь можно доказать невырожденность последовательности шифрующих байтов.

Теорема 2. Генератор Фибоначчи с длиной ключа $l_1 > 8$ порождает невырожденную последовательность псевдослучайных шифрующих байтов.

В самом деле, пусть $x_k = t_k - 2^{l_1+1}\varepsilon_k$ – реальные текущие значения ключа, ε_k – последние биты переполнения, 0 или 1, при сложении, тогда для скрытых (отбрасываемых) частей ключа y_k и чисел $d_k = 2^{l_1-9} b_k$, где b_k – шифрующие байты, имеют место соотношения

$$y_k = x_k - d_k$$

$$y_{k+1} = x_{k+1} - d_{k+1}$$

$$y_{k+2} = y_k + y_{k+1} - 2^{l_1-7}\,\mu_{k+2} = (x_k - d_k) + (x_{k+1} - d_{k+1}) - 2^{l_1-7}\,\mu_{k+2},$$

где μ_{k+2} – последние биты переполнения, 0 или 1, при сложении скрытых значений ключа. Так как $x_{k+2} + 2^{l_1+1}\,\mu_{k+2} = x_k + x_{k+1} = y_{k+2} + d_{k+2} + 2^{l_1+1}$, то $d_{k+2} - d_k - d_{k+1} - 2^{l_1-7}\,\mu_{k+2} - 2^{l_1+1}\,\varepsilon_{k+2} = 0$, и поэтому

(*) $$b_{k+2} - b_k - b_{k+1} - 2^8\,\varepsilon_{k+2} = \mu_{k+2}.$$

Если бы в последовательности шифрующих байтов имелись три одинаковых подряд идущих байта b_k, b_{k+1}, b_{k+2}, то из соотношения (*) следовало бы, что при μ_{k+2}=0 эти байты были бы нулевыми ('00000000'), тогда $\varepsilon_{k+2} = 0$, а при μ_{k+2}=1 – единичными ('11111111'). Тогда и байт b_{k-1} был бы тривиальным, т. е. был бы равен 0 или 255 в зависимости от значения μ_{k+2}.

Таким образом, троекратное повторение шифрующего байта означает его тривиальность, и, значит, нетривиальные шифрующие байты могут входить в шифрующую последовательность не более чем два раза подряд.

Максимальная длина последовательности тривиальных байтов конечна, так как эта последовательность прекращается, когда последний бит μ_{k+1} переполнения скрытой части ключа становится равным 1, что обеспечивается ненулевыми начальными значениями скрытых частей ключа, в противном случае было бы $l_1 \le 8$, что противоречит условию теоремы. Поэтому последовательность шифрующих байтов от генератора Фибоначчи не вырождена. Теорема доказана.

Длина последовательности тривиальных байтов не превосходит удвоенной длины ключа $2l_1$, так как между числами 2^{m-1} и 2^m, $2^{m-1} \le f_k < 2^m$, не может быть больше двух чисел Фибоначчи.

Уравнение шифрования неразрешимо относительно начального значения ключа при известных открытых и зашифрованных данных, т. к. значительная часть информации, используемая для вычисления шифрующего байта, не представлена в зашифрованных данных, и, кроме того, за два шага исчезает из процесса вычисления последующих шифрующих байтов, т. е. фактически отбрасывается. Поэтому начальное значение ключа невычислимо, и, значит, текущее (конечное) значение ключа может быть использовано для шифрования следующих данных. При этом одновременное наличие у дешифровальщика открытого и зашифрованного текстов не влияет на криптостойкость последующих текстов при том же начальном значении ключа. Это позволяет неограниченно применять некоторое начальное значение. Соответствующая теорема о возможности фальсификации текущих значений ключа в процессе шифрования легко может быть доказана приёмами из доказательств первых двух теорем.

Разумеется, последовательность шифрующих байтов легко может быть восстановлена по имеющимся открытым и защищённым данным. Однако, это не позволяет даже приблизиться к начальному значению ключа, так как кроме алгебраической невычислимости имеются псевдоцепи Маркова μ_k и ε_k. Поэтому неопределённость текущих значений ключа всегда соответствует длине шифруемых данных, если длина текста не больше, чем $2^{l_1} - 1$. При выполнении этого условия и $l_1 \ge 9$ принцип Кирхгофа удовлетворяется автоматически, а это значит, что алгоритм является абсолютно стойким. При l_1= 64, например, можно зашифровать 8 миллионов терабайтных дисков.

Длинные последовательности тривиальных байтов могут быть исключены из шифрующей последовательности за счёт стоимости вычислений с помощью фальсификации текущих значений ключа.

Потребность в длинном сложении снижается применением архитектуры с длиной машинного слова 64 бита. Целостность данных, поступающих из линии связи, может быть проверена с помощью двух экземпляров контрольной суммы по тексту, случайно размещённых в сообщении. Полезным, в зависимости от очевидных для интегрированных информационных систем требований административного стандарта [2], является использование нескольких независимых начальных значений ключа, оправданное развитием функций защиты данных.

IV Выводы

Таким образом, условие разрешимости уравнения шифрования относительно ключа должно быть ослаблено до условия разрешимости этого уравнения относительно шифрующих байтов (слов).

Генератор Фибоначчи порождает практически апериодическую последовательность шифрующих байтов. Эта последовательность невырождена, нефальсифицируема по открытому и зашифрованноиу экземплярам фрагмента текста. Она легко может быть сделана непрогнозируемой и тотальной с помощью фальсификации текущих значений ключа. По-видимому, имеются возможности обеспечить две последние характеристики без увеличения стоимости вычислений.

Литература: 1. С. Макаренко, А. Брусникин, Алгоритмы шифрования для передачи данных в открытых сетях - В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– Науково-технічний збірник. – Випуск 2. – К.: НДЦ "Тезіс" НТУУ "КПІ".–2001.– 273 с. С. 223. 2. В. В. Мясоедов, Абсолютная защита данных. Know how, © В. В. Мясоедов, Киев, 2000 г, 10 с. 3. Без фамилии авт., Золотое сечение, Математическая энциклопедия, т. 2 Д-КОО – М.: "Советская Энциклопедия",–1979.–110 4стб. С. 466.

УДК 681.3.06

ШЛЮЗ БЕЗОПАСНОСТИ “КРИПТОМАРШРУТИЗАТОР 1.0” С УДАЛЕННЫМ УПРАВЛЕНИЕМ И ЕГО ВОЗМОЖНОСТИ

Иван Горбенко, Александр Волощук*, Виталий Вервейко, Юрий Горбенко, Сергей Полчанинов

*ХНУРЭ, *Укрсоцбанк*

Анотація: **Розглядається задача побудови та реалізації системи захисту міжмережевого трафіку на основі створення тунелів між локальними мережами з використанням шлюзів безпеки.**

Summary: **The task of development and implementation of the network traffic security system is considered. The system based on the inter-LAN tunnels creating using security gateways**.

Ключевые слова: **Системы защиты межсетевого трафика, шлюз безопасности, удаленное управление.**

Введение

Одной из важнейших проблем в организации эффективной системы безопасности компании является определение разделения прав доступа к данным компании. Инструменты, которые позволяют реализовывать такие решения (брандмауэры, шлюзы безопасности), должны интегрироваться непосредственно в корпоративную сеть, используемую компанией, а также в ее отдельные компоненты.

Процесс функционирования корпоративной сети сопровождается циркуляцией потоков информации в локальных или глобальных сетях. Сети, на основе которых строятся современные информационные технологии компаний и корпораций, должны быть достаточно гибкими для того, чтобы обеспечить необходимый доступ к ресурсам или данным и в то же время быть достаточно защищенными для предотвращения нежелательного проникновения в корпоративную сеть. Эта проблема становится более сложной, если компания вынуждена взаимодействовать с общедоступными сетями, такими как Интернет. Когда новые сети и домены становятся доступны со стороны Интернета, добавляются новые серверы или выпускаются новые продукты перед компанией встает проблема их безопасной интеграции и обеспечения сотрудникам компании доступа к ним.

Чтобы построить систему безопасности компания должна в первую очередь разработать политику контроля доступа для внутренних и внешних сетей и сетевых ресурсов. В большинстве компаний считают, что их внутренним сетям (например, локальным сетям внутри здания) можно доверять. При этом считают, что сети вне организации – внешние и им доверять нельзя. Поэтому для изоляции внутренней сети от внешней используются брандмауэры и шлюзы безопасности. Однако, внутренние сети также представляют определенную опасность и должны обеспечивать некоторый уровень защиты, хотя политика безопасности по отношению к внутренним сетям может сильно отличаться от политики безопасности по отношению к внешним сетям, так как в большинстве компаний поток данных внутри рабочей группы обрабатывается по-иному, чем поток данных между рабочими группами.

I Брандмауэры и шлюзы безопасности

Для обеспечения безопасности внутренних и внешних сетей и сетевых ресурсов компании существует множество средств. Одними из основных компонентов таких средств являются брандмауэры и шлюзы безопасности.