Полученные два варианта алгоритма быстрого преобразования Уолша в системе упорядочений Уолша-Пэлли являются симметричными и относятся к «замечательным». А рассмотренный метод извлечения алгоритмов быстрого преобразования Уолша может быть использован в различных системах упорядочений.

Литература

1. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М., «Сов. Радио», 1975.

2. *C. Yen.* Walsh functions and Gray code. IEEE Transactions, 1971, EMC 13, N 3.

ПРИМЕНЕНИЕ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ СКРЫТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ. ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ

Д.Н. Буйновский

Проведен обзор М-последовательностей, а также проанализированы перспективы их использования при передаче информации. В наше время, а также в будущем, данные методы кажутся наиболее перспективными при использовании в технологиях беспроводной передачи данных, хотя, безусловно, их можно использовать для любой среды передачи. Применение М-последовательностей позволяет снизить влияние помех в среде передачи, а также скрытно передавать любую информацию.

М-последовательность — бинарная последовательность импульсов определенной длины, характеризуемая рядом свойств, из которых основные, это то что автокорреляционная функция ее, измеренная на конечный интервал времени, представляет собой один узкий треугольник [2].

Одной из интересных возможностей, которой обладают М-последовательности - является скрытная передача информации, путем передачи через общий канал связи шумоподобного сигнала (ШС), на основе М-последовательности.

В системах с ШС обеспечивается скрытность передачи, если код, определяющий форму ШС, известен только своему корреспонденту, а база ШС выбрана такой величины, при которой уровень полезного сигнала меньше уровня флуктуационного шума, возникающего во входных цепях приемника.

М-последовательности, хоть и в разы повышает объем данных, необходимый для передачи сообщения, и снижается скорость передачи сообщения, существенно повышается вероятность успешного его декодирования.

Таким образом, применение М-последовательностей в современных широкополосных системах передачи позволит улучшить качество передачи потоковых данных (голос и видео).

М-последовательности возможно использовать в системах IP телефонии. В первую очередь, как дополнительные меры, для передачи голоса и видео по нестабильным каналам связи.

Литература

1. М-последовательность [Электронный ресурс] — Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/95625

2. *Клюев Л.Л.* Теория электрической связи. Минск, 2016.

3. М-последовательность [Электронный ресурс] — Режим доступа: https://ru.wikipedia.org/wiki

ШИФРОВАНИЕ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ (NGE)

Д.Н. Буйновский

Проведен обзор нового направления в области криптографии: шифрование следующего поколения. В наше время, а также в будущем, данные методы кажутся наиболее перспективными, так как одиночное использование ни одного из существующих алгоритмов не сможет обеспечить сохранность конфиденциальных данных.

За последние годы, было разработано и использовано множество криптографических алгоритмов во множестве различных протоколов и функций. Однако, криптография не является статической. Устойчивый прогресс в науке и вычислительной технике привели к необходимости использования новых, более безопасных алгоритмов и ключей большего размера. Данная работа посвящена анализу современных методов защиты от угроз информационной безопасности, так называемым методам шифрования нового поколения.

Next generation encryption — новая ветвь развития в области защиты данных. Совершенствование методов анализа данных, прогресс в технике, а также найденные уязвимости

существующих алгоритмов шифрования не дают достаточной степени защиты информации. Поэтому, в наше время, для защиты данных используются NGN методы. Это комплексный подход, представляющий собой комбинирование нескольких алгоритмов защиты данных.

Алгоритмы, составленные NGE являются результатом более чем 30 лет мирового прогресса и эволюции в области криптографии. Каждый составляющий компонент NGE имеет свою историю. NGE состоит из множества всемирно используемых алгоритмов, протестированных на протяжении многих лет, и публично доступных алгоритмов.

При проектировании системы NGN стоит придерживаться еще одного правила: криптостойкость алгоритма должна определяться только криптостойкостью ключей шифрования. Все остальное, например техническое описание самого алгоритма, методы построения системы защиты, должны заведомо считаться известными потенциальному противнику.

Таким образом, система защиты данных, способная обеспечить достаточную защиту от современных угроз, должна представлять собой комплексную систему из различных элементарных методов проверки:

– шифрование с использованием сильного алгоритма и ключа большой длины;
– безопасный обмен ключами;
– аутентификация пользователя;
– авторизация пользователя;
– проверка целостности данных;
– проверка наличия чужого вмешательства;
– сокрытие канала передачи.

Литература

1. Cisco Systems – Next Generation Encryption [Электронный ресурс] — Режим доступа: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html#ftn2

2. Super Cryptography: The Next Generation Encryption [Электронный ресурс] — Режим доступа: http://thehackernews.com/2011/11/super-cryptography-next-generation.html

3. CNG Features [Электронный ресурс] — Режим доступа: https://msdn.microsoft.com/en-us/library/windows/desktop/bb204775(v=vs.85).aspx

ВОПРОСЫ ОБЕСПЕЧЕНИЯ СТОЙКОСТИ КЛЮЧЕЙ ПРИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Г.А. Власова, А.И. Букштынова

Известно, что стойкость криптографической системы определяется стойкостью ключа. Развитие средств вычислительной техники приводит к необходимости увеличения длины ключей для обеспечения требуемого уровня криптостойкости.

До 2002 года стойкими считались RSA-ключи длиной 64 бит (в 1997 г. удалось взломать RSA-шифр с длиной ключа 56 бит за 250 дней). В 2009 году был взломан шифр с длиной ключа 768 бит, а уже в 2010 году — 1024 бит, на что потребовалось всего 100 ч.

В 2015 году появилась информация об успешном взломе 4096-битных RSA-ключей. Однако в дальнейшем было показано, что взломать удалось лишь отдельные отбракованные ключи. Таким образом, на сегодняшний день RSA-ключи длиной 4096 бит можно считать криптостойкими.

Согласно [1], одинаковую криптостойкость имеют ключи симметричных систем с длиной 80 бит и ключи асимметричных систем с длиной 768 бит; ключи длиной 128 бит и 2304 бит соответственно. Анализируя тенденции взлома ключей асимметричного алгоритма RSA, можно сделать вывод, что для симметричного алгоритма AES ключи длиной 128 бит использовать не следует.

Отметим, что наряду с устройствами криптографической защиты по ГОСТ 28147-89 и AES256, встречаются коммерческие предложения с длиной ключа, не обеспечивающие достаточный уровень безопасности (AES128), либо вовсе без информации о длине ключа. Поэтому выбор условий функционирования средств криптографической защиты, в том числе длины ключа, становится необходимым условием обеспечения безопасной работы систем хранения, обработки и передачи информации.

Литература

1. *Деднев М.А., Дыльнов Д.В., Иванов М.А.* Защита информации в банковском деле и электронном бизнесе. М., 2004.