использовать данные с других датчиков, например, акселерометр, гироскоп, магнитометр, которые доступны в современных моделях смартфонов и планшетов с целью повышения точности измерений.

Таким образом, системы, построенные на основе Bluetooth-маячков, являются конкурентоспособной альтернативой другим способам реализации систем навигации внутри помещений, а также могут быть использованы в комбинации с другими технологиями.

Список использованных источников:

1. Kevin Townsend, Carles Cufí, Akiba, Robert Davidson, Getting Started with Bluetooth Low Energy, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.
2. Навигация в помещениях с iBeacon и ИНС [Электронный ресурс] – Режим доступа. – URLhttps://habrahabr.ru/post/245325/ (дата обращения 03.04.2017).
3. BluetoothLowEnergyadoptedspecification [Электронный ресуср] – Режим доступа: – URLhttps://www.bluetooth.org/en-us/specification/adopted-specifications (дата обращения 04.04.2017).

УТИЛИТА ШИФРОВАНИЯ ФАЙЛОВ ДЛЯ WINDOWS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Молчанов И.В.

Жвакина А.В. – канд. техн. наук, доцент

Тема шифрования всегда была крайне важна в программировании, причем не только в больших бизнес-проектах, но и в небольших университетских работах, так как задача по защите данных от несанкционированного вмешательства всегда была, есть и будет актуальна. На данный момент существует большое количество алгоритмов шифрования (от простых перестановочных шифров до стандартизированных асинхронных алгоритмов). В процессе разработки изучены синхронные и асинхронные алгоритмы шифрования среднего уровня сложности, их сильные стороны и уязвимости, также данные алгоритмы реализуются в утилите, созданной для шифрования файлов.

В процессе исследования рассмотрены шифры XOR и RSA, так как являются наиболее простыми из использующихся на практике, но при грамотном использовании и надлежащих модификациях могут быть достаточно эффективными. Материал данной работы предназначен не для профессиональных программистов, давно освоивших более сложные алгоритмы, а для студентов, желающих реализовать какую-либо защиту данных в своих проектах.

Алгоритм шифрования RSA можно представить следующим образом:

- возьмем p, q – достаточно большие простые числа;
- n = p • q;
- выберем случайное d такое, что f = (p – 1) • (q – 1) взаимно просто с d;
- определим e, для которого (e • d) ≡ 1 (modf);
- открытый ключ: {e, n}; закрытый ключ: {d, n};
- блочное шифрование: $F_i = (M_i)^e \mathrm{mod} n$;
- блочная расшифровка: $M_i = (F_i)^d \mathrm{mod} n$.

Основными достоинствами шифра RSA являются:

- использование двух ключей, что позволяет использовать его в клиент-серверных приложениях;
- надежность шифрования при использовании достаточно длинных ключей (512 бит и более).

Основными его недостатками являются:

- необходимость генерации длинных простых чисел, что требует гигантских затрат времени;
- падение криптостойкости при небольших по длине ключах.

Также был проанализирован алгоритм шифрования XOR, описываемый так:

- выбор ключа K (как случайный, так и пользовательский, случайный считается более устойчивым);
- блочное шифрование: Fi = Mi xor K;
- блочная расшифровка: Mi = Fi xor K;

Достоинствами данного шифра являются:

- быстрота шифрования данных;
- простота реализации;
- высокая устойчивость шифра при регулярной смене ключа.

Основными его недостатками являются:

- при использовании чистого XOR и достаточном количестве перехваченных сообщений ключ может быть получен путем анализа зашифрованных данных;
- при известной части текста ключ также может быть получен при перехвате сообщения;
- ключ используется как для шифрования, так и для дешифровки сообщения.

Основной проблемой шифра RSA, по мнению автора, является то, что криптостойкость алгоритма со временем падает (*«По словам исследователей, после их работы в качестве надежной системы шифрования можно рассматривать только RSA-ключи длиной 1024 бита и более. Причём от шифрования ключом длиной в 1024 бит стоит отказаться в ближайшие три-четыре года»*), а для ее повышения

требуется генерация все больших простых чисел, что не является тривиальной задачей. Именно поэтому в первую очередь было решено модифицировать более простой шифр XOR. Для этого мы нашли два способа: компоновка его с перестановочным шифром или добавление битов в зашифрованное сообщение. Из-за тривиальности первого способа, было решено использовать второй.

Возьмем любую реккурентную последовательность вида:

a_1= A> 0; // псевдослучайное число

a_2 = B> 0; // псевдослучайное число

a_{i+1}= α • a_i + β • a_{i-1}; // α и β – также псевдослучайны

На позиции j = a_i добавим псевдослучайные символы или заранее заготовленную информацию, сгенерированную по какому-либо алгоритму. Таким образом, попытка узнать длину ключа путем циклического сдвига (первый шаг по взлому XOR) не осуществима из-за разных дистанций между a_i и a_{i+1}. Таким образом, при надлежащем использовании, данный алгоритм может быть использован для шифрования файлов.

При разработке утилиты особое внимание уделено не только реализации данного алгоритма, но и попытке распространения такой системы на асинхронный алгоритм шифрования.

Исследованиеподдержанопроектом CERES. Centers of Excellence for young RESearchers (Reg.no. 544137-TEMPUS-1-2013-SK-JPHES),

CERES Co-funded by the Tempus Programme of the European Union

Список использованных источников:

1. Алгоритм шифрования RSA. [Электронный ресурс] – Режим доступа: http://www.e-nigma.ru/stat/rsa. – Дата доступа : 28.03.2017.
2. Криптоанализ RSA. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Криптоанализ_RSA. – Дата доступа : 03.04.2017.
3. В. А. Артамонов. Элементы криптологии. [Электронный ресурс] – Режим доступа: http://www.pereplet.ru/obrazovanie/stsoros/1009.html – Дата доступа : 03.04.2017.
4. Шифр XOR: практика взлома. [Электронный ресурс] – Режим доступа: https://russianpenguin.ru/2014/05/04/шифр-xor-практика-взлома/. – Дата доступа : 28.03.2017.

ИСПОЛЬЗОВАНИЕ МАТЕМАТИЧЕСКИХ ЗАКОНОМЕРНОСТЕЙ В ДИЗАЙНЕ САЙТОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сафонова Л. А

Теслюк В.Н. – канд. техн. наук, доцент

В наше время уже довольно сложно удивить человека веб-приложениями. Интернет наполняют множество новостных порталов, блогов, интернет-магазинов и т. д. Одним из основных факторов, влияющих на популярность приложения, является грамотно спроектированный дизайн. На сегодняшний день эффективный веб-дизайн не может быть просто яркой и симпатичной картинкой. Он должен быть интуитивно понятным и как можно более простым. Интересным способом в разработке дизайна веб-приложений является применение математического подхода.

В работе приведены наглядные образцы использования в данной области таких известных математических принципов как «золотое сечение», пропорции Фибоначчи, правило Третей, что доказывает, что применение математики в веб-дизайне поможет обеспечить хорошую основу для дальнейшего развития концептуального дизайна.

Золотое сечение (или золотая пропорция) - это деление в среднем и крайнем отношении или, другими словами, деление непрерывной величины на две части в отношении, при котором меньшая относится к большей, как большая ко всей величине. В этой пропорции отношение частей выражается иррациональной математичской константой (приблизительно равной 1.618033987). Доказано, что объекты, которые содержат в себе «золотое сечение», будут восприниматься людьми как более гармоничные.

Применение данного принципа в дизайне веб-приложения представлено на рисунке 1: