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:

Рис. 1 - Золотое сечение в дизайне

Числа Фибоначчи представляют собой математическую последовательность из ряда чисел. Первые два числа Фибоначчи равны 0 и 1. Далее, каждое последующее - есть сумма двух предыдущих. Ряд из чисел выглядит следующим образом: 0, 1, 1, 2, 3, 5, 8, 13, 21… Числа Фибоначчи обычно используются архитектуре, например, расчет отношения высоты помещения к значению высоты декорирования стен специальными материалами, в музыке, например, для настройки инструментов. Даже расстояние между листьями на стволе деревьев относятся приблизительно как числа Фибоначчи.

В веб-дизайне основной областью применения чисел Фибоначчи является определение размеров контейнеров с основным контентом (содержанием) и боковой панели. Принцип метода заключается в следующем: базовая ширина контейнера, к примеру, 100 пикселей, последовательно умножается на числа из последовательности Фибоначчи. Сетка сайта строится на основании этих вычислений.

Возможный вариант использования пропорций Фибоначчи представлен на рисунке 2:

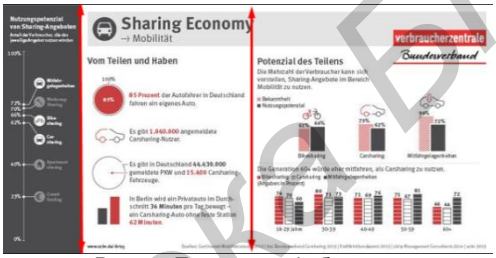

Рис. 1 - Пропорции Фибоначчи

Правило Третей является упрощенной версией Золотого Сечения. Разделение дизайна веб-приложения на трети это наиболее простой путь к достижению божественных пропорций без использования сложных вычислений.

В первую очередь, каждая композиция может быть разделена на девять частей четырьмя линиями: двумя горизонтальными и вертикальными. Сформированные пересечением данных линий четыре точки, рекомендуется использовать для размещения элементов, которым нужно уделить особо важное значение в дизайне. Расстановка композиции по данному правилу создает больше интереса и креатива, чем простое центрирование.

Использовать все четыре точки для акцентирования внимания на наиболее важных функциях и элементах навигации как почти невозможно, так и не полезно. Но при этом можно выгодно использовать некоторые из них для размещения основного послания или функций сайта. Левый верхний угол считается самым важным, так как пользователи просматривают сайты относительно F-фигуры.

Применение Правила третей в веб-дизайне представлено на рисунке 3:

Рис. 1 - Правило третей в дизайне

Таким образом было показано, что математический подход можно применять не только в искусстве и архитектуре, но и в сфере веб-разработки. Однако не стоит забывать о том, что профессиональность дизайна видна тогда, когда он соответствует задачам приложения. Дизайн веб-приложения должен не столько

привлечь, сколько удержать внимание пользователя. Пользователи будут игнорировать дизайн, который игнорирует их.

Список использованных источников:

1. Chris Bank, Jerry Cao, Waleed ZuberiWeb UI design best practices, 2014
2. Adit Gupta // Applying Mathematics To Web DesignЖурнал Smashing Magazine [Электронныйресурс]. Режим доступа: http://4design.xyz/nombre-d-or-suite-de-fibonacci-et-autres-grilles-de-mise-en-page-pour-le-design-web - Дата доступа: 25.01.2017.
3. Bruno Bichet // Nombre d'or, suite de Fibonnacci et autres grilles de misse en page pour le design webПортал 4design [Электронныйресурс]. Режим доступа: https://www.smashingmagazine.com/2010/02/applying-mathematics-to-web-design/ - Дата доступа: 15.01.2017.

МОДУЛЬ ПОЛУЧЕНИЯ ДАННЫХ ИЗ ВНЕШНИХ ОТКРЫТЫХ ИСТОЧНИКОВ

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

Пресняцкий В.Ю., Рожков Д.Н., Дорошкевич П.Е., Свито А.И.

Стержанов М.В. – канд.техн.наук, доцент

Web-crawlers (also known as robots or scrapers) enable the process by following the hyperlinks in web pages to automatically download a fractional snapshot of the web site. This paper describes developed web crawler named MMScraper aimed to process informational web resources for further getting statistical properties and performing data analytics.

В настоящее время в связи с бурным развитием сети Интернет наблюдается обилие электронной неструктурированной информации, представленной текстами на естественных языках. Всё более востребованной становится задача автоматической обработки таких текстов с целью извлечения структурированных данных, которые затем используются при решении различного рода проблем: извлечения фактических данных, поиска информации и т.п. Нами решается задача обработки контента информационно-новостных ресурсов с целью анализа лексико-терминологической информации.

Для сбора требуемых данных требуются специализированные инструменты - поисковые роботы, также называемые «веб-пауками» (web-spider), краулерами (webcrawler) или скребками (webscraper). Поисковый робот — это программный комплекс, который осуществляет навигацию по веб-ресурсам и сбор информации для базы данных приложения-агента [1, 2].

Нами планируется значительная работа по обследованию ряда информационных сайтов, чтобы собрать выборку данных требуемого размера. Анализ имеющихся в свободном доступе решений показал, что открытые реализации зарубежных веб-краулеров слабо приспособлены к решаемой нами задаче, так как требуют весьма трудоемкой настройки, а после нее показывают низкую производительность и существенно нагружают информационный источник. В связи с этим было принято решение разработать собственное решение.

Краулер, названный MMScraper, был разработан нами в соответствии со следующими требованиями:

* Получать список доменных имен сайтов, предназначенных для сканирования, в качестве исходных данных. Предполагается, что имеется некоторое множество заранее определенных для исследования сайтов.

* Делать обход каждого сайта, начиная с главной (индексной) страницы, перемещаясь по внутренним гиперссылкам в заданном порядке обхода «сначала вширь».

* Полученные результаты сохранять в базу данных. Интерес представляют следующие атрибуты: адрес страницы, автор публикации, дата публикации, содержимое публикации.

* Позволять получать данные с сайта через программный интерфейс API.

* Иметь расширяемую архитектуру, чтобы впоследствии развивать функциональность.

* Добавление нового сайта должно быть простым и не требовать привлечения квалифицированного программиста.

Работа разработанного краулера описывается следующим образом: сайт сканируется, начиная с главной страницы, после этого робот обрабатывает ссылки, размещённые на ней, переходя по ним, на другие страницы сайта. Каждая страница проходит анализ на наличие нужной информации, которая в случае обнаружения копируется в соответствующее хранилище. Процесс продолжается тех пор, пока не будет обработано требуемое количество страниц или пока не будет достигнута некая цель. Модуль получения данных разработан на языке программирования Ruby и состоит из трех основных частей: блока сканирования и обработки данных, блока управления краулером (команды вводятся через консоль) и база данных. Информация, которую собирает робот, состоит из ссылочной структуры обрабатываемого ресурса и веб-страниц. В качестве основной базы данных была выбрана бесплатная удобная в использовании СУБД MySQL. Для упрощения взаимодействия с БД нами используется библиотека Sequel, которая позволяет представлять данные в виде объектов.

В работе приводится описание главных требований, общей архитектуры и конфигурации краулера MMScraper, который предназначен для решения довольно узкой, но важной задачи, а именно – сбора различного рода информации о новостных и информационно-аналитических публикациях.