Министерство образования Республики Беларусь

Учреждение образования Белорусский государственный университет информатики и радиоэлектроники

УДК 004.928

Рогов
Максим Геннадьевич

Система управления комплексом городских игр

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-40 80 04 «Математическое моделирование, численные методы и комплексы программ»

_____

Научный руководитель
Егорова Наталья Геннадьевна кандидат физико-математических наук, доцент

_____

Минск 2016

ВВЕДЕНИЕ

Современную жизнь человека тяжело представить без современных компьютерных технологий. Постоянно развивающаяся IT-сфера задает новые тренды и направления развития человеческой деятельности. В последние годы, когда мобильные устройства стали смартфонами, технологии стали неотъемлемой частью любого времяпрепровождения. Однако чем больше технологии упрощают нашу жизнь, тем меньше времени остается для ведения здорового образа жизни.

Современные мобильные системы имеют сотни приложений, направленных на сопровождение занятий спортом. Однако в современном мире, чтобы заинтересовать человека чем-то, уже мало сделать это просто полезным. Любая идея должна быть еще привлекательной и полезной, иначе она не будет пользоваться большим спросом. Так возникли городские игры, сочетающие в себе как простые спортивные занятия, так и не сложную тренировку для мозга.

Информация - это одна из самых ценных вещей в современной жизни. Появление глобальных компьютерных сетей сделало простым получение доступа к информации как для отдельных людей, так и для больших организаций. Но легкость и скорость доступа к данным с помощью компьютерных сетей, таких как Интернет, также сделали значительными следующие угрозы безопасности данных при отсутствии мер их защиты.

Совмещение принципов здорового образа жизни с решением различных криптографических заданий и головоломок является довольно успешно развивающимся направлением современного досуга. Анализ и систематизация современных методов криптографии, совмещение этих методов с исторически обусловленными алгоритмами и способами шифрования является на сегодняшний момент важной особенностью нового формата городских игр, обусловленной повышением требований от пользователей. С точки зрения разработки программного комплекса в рамках данной работы наиболее важным является факт особенности контингента пользователей системы, которые являются студентами БГУИР. Этот факт обуславливает особенные требования к заданиям в сфере информационной безопасности.

На сегодняшний день существует достаточное количество вариантов систем управления городскими играми. Однако в большинстве своем принципы и особенности проведения данных мероприятий приводят к тому, что использование компьютерных технологий, а тем более методов криптографических преобразований, сводится к минимуму. В этом и заключает основное отличие разрабатываемой системы. Комплексный и всеобъемлющий подход к анализу методов криптографических преобразований позволяет не только получить новые данные по результатам научного исследования, но и повысить качество заданий для разрабатываемой системы. Также немаловажным является и тот факт, что периодическая практическая реализация системы и проведение городских игр позволяют обеспечить экспериментальный анализ полученных результатов. Такой анализ, в свою очередь, способен обеспечить новой информацией, позволяющей модернизировать как результаты исследований, так и разрабатываемые задания для системы.

Процесс криптографического сокрытия данных может происходить различными путями. Однако каким бы именно образом этот процесс не проходил, всегда существует ряд обобщенных требований. Наиболее важными из них являются:

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
2. число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
3. знание алгоритма шифрования не должно влиять на надежность защиты;
4. незначительное изменение исходного текста должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
5. структурные элементы алгоритма шифрования должны быть неизменными.

Разработка заданий, используя результаты, полученные в ходе анализа криптографических преобразований, является главной особенностью нового формата городских игр. Основная идея игры, не смотря на разрабатываемые нововведения, остается неизменной и достаточно прямолинейной. В игре участвует определенное количество команд на каждом из этапов игры. У каждой команды имеется маршрут, составленный из мест, находящихся в черте города. Каждая команда получает задание, первая часть которого указывает на определенное место в городе. Прибыв в данное место, команда добывает ключ, обеспечивающий расшифровку второй части задания и получение ответа, который, в свою очередь, приводит команду к новому заданию.

Таким образом, составление заданий, основой которых являются различного рода криптографические преобразования, составляет важную часть основной цели диссертационной работы – разработки программного комплекса для проведения, мониторинга и сопровождения городских игр.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Основной целью работы является разработка программного комплекса для проведения, мониторинга и сопровождения городских игр, изучение, анализ и оценка алгоритмов шифрования для практического использования в программном комплексе, анализ и исследование практической ценности примененных алгоритмов по результатам запуска программного комплекса.

Практическим результатом работы является спроектированная и реализованная на языке программирования C# система управления для комплекса городских мероприятий. Система позволяет пользователям регистрироваться в системе, обеспечивает доступ команд к маршрутам и заданиям, имеет возможность динамического изменения данных в заданиях. Также в рамках проекта были разработаны дополнительные функции системы, включающие в себя дополнительные периодические задания, систему реализации бонусных баллов, графическую реализацию дерева маршрутов.

Для проектирования заданий для городской игры был произведен анализ предметной области, используемых подходов, методов и алгоритмов в области защиты информации. Проект содержит реализованную систему Token-base аутентификации, позволяющую обеспечить более надежную защиту системы во время проведения городских игр. Доступ пользователей к реализованной системе возможен с любых мобильных платформ. Для хранения мультимедийной информации, задействованной в заданиях для городских игр, используется внешнее облачное хранилище, позволяющее оперативно вносить изменения в задания игры во время её проведения.

Для тестирования полученной функциональности была использована библиотека NUnit, которая позволяет с минимальным использованием усилий, реализовать все виды Unit-тестирования приложения. Перед началом общеуниверситетской городской игры программный продукт нужно протестировать на ограниченном круге пользователей, называемых соответственно альфа и бета тестировщиками. Для альфа и бета тестирования программный продукт был предложен небольшой группе студентов БГУИР, которые смогли протестировать систему и оставили свои комментарии и пожелания по модернизации программного продукта.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе произведён обзор предметной области задач, решаемых в рамках данной работы; рассмотрены вопросы о сущности методов криптографических преобразований и принципе их работы; приведены причины использования данных подходов для решения поставленной задачи.

Во второй главе произведено обоснование выбора использованных для реализации технологий. Произведен обзор платформы .NET Framework. Рассказывается о нововведениях в последнюю версию языка C#.

Третья глава посвящена исследованию методов криптографических преобразований. Проанализированы и выявлены наиболее подходящие алгоритмы шифрования для реализации в разрабатываемом программном продукте.

В четвёртой главе представлены центральные объекты системы. Определены базовые сущности и способы расширения функциональности созданной модели. В главе приведены схемы, отражающие взаимоотношения компонентов спроектированной системы.

В пятой главе произведено описание процесса тестирования созданного программного продукта. Произведена оценка практической реализации системы и разработанных заданий. Показан возможный способ расширения разработанной системы.

ЗАКЛЮЧЕНИЕ

В данной работе были рассмотрены вопросы использования различных методов криптографических преобразований. Также была разработана система управления комплексом городских игр. Были проведены анализ и сравнение существующих алгоритмов шифрования с последующим выявлением наиболее подходящих для разработки заданий в рамках существующей системы. Перед непосредственной разработкой программного продукта был проведен анализ предполагаемых технологий разработки, детально изучены возможности платформы Microsoft .NET и языка C#. Основными отличиями разработанной системы от существующих аналогов являются использование современных технологий во время разработки системы, а также более глубокое внедрение компьютерных технологий в принципы и форматы проведения городских игры. Разработанная система при практической реализации проведения игр в рамках БГУИР зарекомендовала себя как качественный программный продукт. Реализованные функции системы смогли должным образом разнообразить проведение мероприятий и обеспечить высокую техническую надежность. С учетом комментариев пользователей был проведен анализ реализованного функционала и разработана дальнейшая схема модернизации системы.

В результате цель работы была достигнута. Был создан программный продукт, с помощью которого осуществляется управление целым комплексом городских игр. Анализ существующих методов криптографических преобразований позволил улучшить качество имеющихся заданий системы и разработать их усовершенствованные варианты. За рамками проделанной работы остались в недостаточной мере рассмотрены вопросы анализа некоторых алгоритмов шифрования. Для разработки имеющегося на данный момент вариант системы, а также проработки заданий, такого рода анализ алгоритмов шифрования не был критически важным. Однако задачи проведения такого рода анализа имеют существенную важность при дальнейшей модернизации системы управления комплексом городских игр.

Разработанная система является готовым программным продуктом. В тоже время существует целый ряд дополнительных функций, которые рассматривались перед началом разработки, однако не были реализованы из-за временных рамок. Разработка данных функций, совершенствование и модернизация разработанной системы являются дальнейшими вариантами работы над программным продуктом.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1 - А.] Рогов М.Г. Анализ методов криптографических преобразований в сфере защиты информационных систем / М.Г. Рогов, А.Г. Шандраков // 51-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР: Тезисы доклада - Минск, 2015.

[2 - А.] Рогов М.Г. Анализ использования методов криптографических преобразований для защиты пользовательских данных / М.Г. Рогов // 52-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР: Тезисы доклада - Минск, 2016.