«Приоритетные направления развития науки, технологий и техники», Италия (Рим), 9–16 апреля 2017 г.

Технические науки

ЗАЩИТА ИНФОРМАЦИИ МЕТОДОМ ШИФРОВАНИЯ

Махамбаева И.У., Бексейтова А.Б., Кабдолдина Н.О.

Кызылординский государственный университет им. Коркыт Ата, Кызылорда, e-mail: ainur.85@list.ru

Наблюдаемое в последнее время прогрессирующее влияние информационных технологий практически на все сферы жизнедеятельности человечества вызывает поступательный рост требований к телекоммуникационным системам и устройствам телекоммуникации. Это объясняется тем, что данные системы являются пока основным средством обмена информацией и качество их функционирования является определяющим фактором эффективности большинства информационных технологий. Важнейшей составляющей качества функционирования телекоммуникационных систем является качество защиты информации. Обеспечение этой составляющей в настоящее время сталкивается с целым рядом проблем, основной из которых выступает противоречие между потенциальными возможностями существующих подходов и постоянно возрастающими требованиями к защите информации. Потенциальная неспособность этих подходов обеспечить выполнение изменяющихся требований объясняет актуальность исследований в направлении поиска принципиально новых подходов, позволяющих решить отмеченную проблему.

Криптографические методы защиты информации – это мощное оружие в борьбе за информационную безопасность.

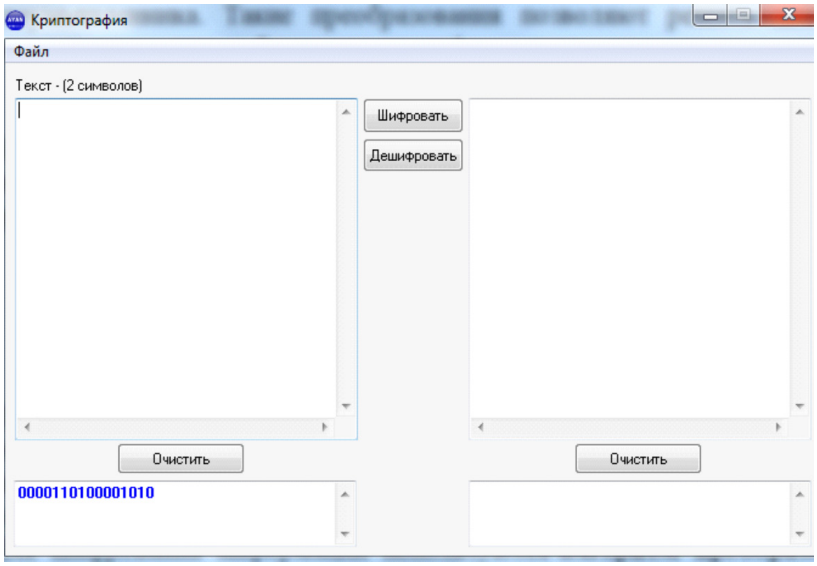
Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.



В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение.

Скрытый файл также может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса кодирование информации является замена исходного смысла сообщения кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Основным видом криптографического преобразования информации в компьютерных сетях является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования.

Список литературы

1. Степанов Е.А. Информационная безопасность и защита информации. – М.: Инфра-М, 2001.

2. Ростовцев А.Г. Элементы криптологии. – М.: Инфра-М, 2000.

3. Теория и практика обеспечения информационной безопасности / под ред. П.Д. Зегжды. – СПб.: Питер, 2000.

МЕТОДЫ УЛУЧШЕНИЯ РАСТРОВЫХ ИЗОБРАЖЕНИЙ: АНТИЭЛАЙЗИНГ И ДИЗЕРИНГ

Турлугулова Н.А., Дюсенбаева Т.Н.

Кызылординский государственный университет им. Коркыт Ата, Кызылорда, e-mail: ainur.85@list.ru

Рассмотрим некоторые из существующих методов, позволяющих визуально улучшать качество растровых изображений. При одних и тех же значениях технических параметров устройства графического вывода может быть создана иллюзия увеличения разрешающей способности или количества цветов. Однако следует иметь в виду, что улучшение одной характеристики может происходить за счет ухудшения другой.

В растровых системах при невысокой разрешающей способности (меньше 300 dpi) существует проблема ступенчатого эффекта (aliasing). Этот эффект особенно заметен на изображении наклонных линий – при большом шаге сетки растра пиксели образуют как бы ступени лестницы.

Рассмотрим это на примере отрезка прямой линии. Растровое изображение объекта определяется алгоритмом закрашивания пикселей, соответствующих площади изображаемого объекта. Можно сформулировать условие корректного закрашивания следующим образом: если в контур изображаемого объекта попадает больше половины площади ячейки растра, то соответствующий пиксель закрашивается цветом объекта (C), иначе пиксель сохраняет цвет фона ($C_ф$).