связано с быстрым увеличением аппаратных мощностей графической системы персональных компьютеров. С другой стороны это развитие связано с потребностями конечных пользователей. Все это позволило трехмерной графике найти широкое применение как в индустрии развлечений, например при создании графики для компьютерных игр, в том числе и браузерных, так и в серьезных системах, которые нашли применение в архитектуре, дизайне, проектировании деталей и целых объектов. Рассмотрим программу 3D графики: 3D Studio MAX, рассмотрим ее возможности, применение в различных сферах а так же рассмотрим практическое применение программы 3D Studio MAX для создания трёхмерной модели фигуры.

3ds Max (3D Studio MAX) — полнофункциональная профессиональная программная система для создания и редактирования трёхмерной графики и анимации, разработанная компанией Autodesk. Содержит самые современные средства для художников и специалистов в области мультимедиа.

Построение трехмерных объектов в программе 3ds Max называется моделированием. 3D-моделирование – это создание 3-х мерной модели мира при помощи формы и цвета. 3D-модель – это не изображение, а именно модель мира. Задача художника максимально ярко, объемно и правдоподобно отразить предмет, и не важно – реальный он или вымышленный. Для отображения простых и сложных объектов 3ds Max использует так называемую полигональную сетку, которая состоит из мельчайших элементов - полигонов. Чем сложнее геометрическая форма объекта, тем больше в нем полигонов и тем больше времени требуется компьютеру для просчета изображения.

УДК 004.932

Криптографические методы защиты информации

Загрецкая Ю.Ю., Минова О.Е.
Белорусский национальный технический университет

Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытые текст или графическое изображение документа. В таком виде сообщение передается по каналу связи, даже и не защищенному. Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным

пользователям. Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (последовательностью бит), обычно называемым шифрующим ключом. Для большинства систем схема генератора ключа может представлять собой набор инструкций и команд либо узел аппаратуры, либо компьютерную программу, либо все это вместе, но в любом случае процесс шифрования (дешифрования) реализуется только этим специальным ключом. Чтобы обмен зашифрованными данными проходил успешно, как отправителю, так и получателю, необходимо знать правильную ключевую установку и хранить ее в тайне.

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом смысле криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации. Взломщик в случае перехвата сообщения будет иметь дело только с зашифрованным текстом, а истинный получатель, принимая сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом - с использованием генератора псевдослучайных чисел. Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом. Надежность шифрования с помощью генератора псевдослучайных чисел зависит как от характеристик генератора, так и, причем в большей степени, от алгоритма получения гаммы. Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для таких серьезных информационных систем, каковыми являются, например, банковские системы.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ,

используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. Знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом. Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA. RSA- это система коллективного пользования, в которой каждый из пользователей имеет свои ключи зашифровывания и расшифровывания данных, причем секретен только ключ расшифровывания.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма - цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений.

Из изложенного следует, что надежная криптографическая система должна удовлетворять ряду определенных требований.

- Процедуры зашифровывания и расшифровывания должны быть «прозрачны» для пользователя.
- Дешифрование закрытой информации должно быть максимально затруднено.
- Содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

УДК 625.7

Методы оценки эксплуатационного состояния автомобильных дорог за рубежом

Москвин Арт. Ю., Москвин Ант. Ю., Мытько Л.Р.
Белорусский национальный технический университет

Автомобильные дороги представляют собой комплекс сооружений, предназначенных для круглосуточного беспрепятственного пропуска транспортных средств с расчетными скоростями и нагрузками в любой период года при любых погодно-климатических условиях.

Система диагностики является необходимым элементом управления надежностью дорожной сети по сигналам о состоянии ее элементов. Если система управления в ответ на сигнал об отказе по транспортно – эксплуатационным параметрам исключает участок дороги из процесса