ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА ПРИМЕРЕ АЛГОРИТМА RSA

Прокопенков Д.С.,
учащийся 4-го курса Оршанского колледжа ВГУ имени П.М. Машерова,
г. Орша, Республика Беларусь
Научный руководитель – ***Юржиц С.Л.,*** *магистр образования, преподаватель*

На данном этапе развития технологий хранения, обработки и передачи информации невообразим отказ от использования различных средств защиты целостности и секретности данных. Одним из аспектов защиты компьютерной информации является шифрование информации, описывающееся обратимым преобразованием некоторых данных на основе ключа. Существует множество различных криптографических систем, наиболее распространённой из которых является система шифрования с открытым ключом, состоящая из группы алгоритмов, основанных на однонаправленных функциях и имеющих два вида ключей: секретный и открытый.

Широтой своего использования асимметричные системы обязаны именно дифференциации ключевой информации, которая позволяет распространять открытый ключ и защищать секретный с большей эффективностью, так как нет фактической необходимости выполнять его передачу, а так как по одному из основополагающих требований асимметричных систем: восстановление секретного ключа из открытого должно быть невозможным, даже при наличии шифртекста и алгоритма преобразования, – то секретная информация более защищена. То же свойство асимметричных криптосистем позволяет использовать их алгоритмы и для создания электронно-цифровых подписей (ЭЦП), что значительно увеличивает их распространённость. Наиболее распространённой на данный момент является криптосистема RSA, поэтому цель исследовательской работы определилась как изучение асимметричных систем шифрования на примере криптосистемы RSA, а также создание программного средства, выполняющего обратимые математические и логические преобразования согласно асимметричному алгоритму шифрования RSA.

Материал и методы. Для выполнения поставленной цели были изучены и подвержены сравнению научные материалы, освещающие сущность асимметричных криптосистем, методов криптоанализа и непосредственно криптосистемы RSA.

Для создания работоспособного алгоритма была необходима реализация нескольких отдельных алгоритмов, например, алгоритма генерации больших чисел, так как выбранный язык (C#) не имел необходимых программных средств; алгоритма теста Ферма для больших целых чисел; алгоритма Евклида для больших целых чисел; а так как алгоритм работает с большими числами, то вероятность возникновения чисел Кармайкла для теста Ферма достаточно велика, следовательно, необходима реализация теста Миллера-Рабина для больших чисел. Алгоритмы вычисления экспоненты и деления по модулю предоставляются языковыми средствами системы программирования.

Разработку было решено производить на основе 10-тичной системы исчисления для более простого понимания работы алгоритма.

Результаты и их обсуждение. Существует несколько наиболее популярных асимметричных алгоритмов, примерами могут служить следующие: RSA, шифр Эль-Гамаля, криптосистема Мак-Элиса и другие.

В основу большинства алгоритмов асимметричного шифрования легли математические функции, обратное решение которых, при настоящих, современных ЭВМ – невозможно или затруднительно настолько, что в итоге его выполнения информация потеряет ценность или актуальность. Такие функции называются однонаправленными [1]. Основная ценность однонаправленных функций заключатся в том, что даже при наличии достаточно простого аналитического обратного решения функции для человека, они не имеют рационального алгоритма его выполнения, так как ЭВМ не имеет мышления и может выполнять лишь описанные некоторым алгоритмом действие. В большинстве своём, именно от различия однонаправленной функции следует дифференциация алгоритмов. Так, наиболее широко используемыми однонаправленными функциями являются: функция нахождения произведения больших чисел, как следствие, обратная задача – разложения большого числа на множи-

тели, которая при произведении порядка 2^{664} требует 10^{23} операции; и функция определения модульной экспоненты по фиксированному основанию, для решение которой необходимо определить значение дискретного логарифма, что не имеет на данный момент эффективного алгоритма (при этом не существует доказательств, что такого алгоритма нет) [2]. Обе из описанных ранее однонаправленных функций используются в алгоритме RSA, что во многом поддерживает его криптостойкость.

Если описывать алгоритм RSA обобщённо, то существует несколько основополагающих логических точек: во-первых, это выбор некоторого множества исходных данных, а именно двух больших простых чисел (вполне логично, что для реализации криптосистемы необходимы алгоритмы генерации больших чисел и тестов на простоту); во-вторых, это нахождение произведения двух больших простых чисел; в-третьих, поиск двух множителей, произведение которых является мультипликативным обратным единице по модулю функции Эйлера для ранее найденного произведения; в-четвёртых, непосредственно шифрование, основанное на нахождение модульной экспоненты.

В ходе исследования было создано программное средство и выполнен сопутствующий этому процессу алгоритмический анализ с точки зрения программирования.

Разработанный шифратор обладает функционалом, необходимым для осуществления обратимого преобразования некоторого текста, а именно: генерация открытого и секретного ключа, причём открытый ключ автоматически заносится в соответствующие поля для шифрования информации; непосредственное шифрование и дешифрование некоторой текстовой информации, а также удаление пробелов открытого текста, для уменьшения объема шифртекста. Для шифрования некоторого текста, необходимо выполнить генерацию ключа или вставить ранее сгенерированный ключ, после чего нажать на кнопку «Encrypt», дешифрование выполняется благодаря использованию секретного ключа и нажатию на кнопку «Decrypt». Шифрование возможно для всех символов как латинского, так и кириллического алфавитов, цифр и всех необходимых пунктуационных и арифметических знаков, что описывает достаточное множество символов для шифрования и дешифрования большинства как русских, так и английских текстов, с возможностью считывания информации из текстовых файлов и занесения в файл.

Заключение. Результатом разработки является программное средство, позволяющее генерировать секретный и открытый ключи шифра, выполняющее обратимое преобразование текста с помощью алгоритма шифрования RSA, в основе которого используются числа 9-того порядка, при избыточности шифртекста 1/15. В ходе исследования были изучены и программно реализованы алгоритмы Евклида, Ферма, Миллера-Рабина для больших чисел. Разработанный шифратор может быть использован для проведения обратимого преобразования небольших текстов с целью создания ЭЦП, шифрования и дешифрования текстов с учётом избыточности шифртекста, а также для изучения принципа асимметричных криптосистем в учреждениях образования в качестве учебного материала.

1. Алфёров, А.П. Основы криптографии [Текст] / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: «Гелиос АРВ», 2002. – 480 с.
2. Романец, Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: «Радио и связь», 2001. – 376 с.

ВОЗМОЖНОСТЬ ПОСТРОЕНИЯ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ ГЕНЕРАТИВНОЙ СОСТЯЗАТЕЛЬНОЙ СЕТИ

Рыльков А.В.,
студент ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Маркова Л.В.,*** *канд. физ.-мат. наук, доцент*

Нейросети умеют распознавать изображения и не только, но генерация самостоятельных решений для них практически не возможна. Однако, относительно недавно, данная проблема была решена исследователями из университета Монреаля. Они разработали генеративную состязательную сеть (далее GAN) [1]. Анализ возможностей сети GAN и области ее применения является актуальной задачей.