

Лабораторная работа №1. Включение общего доступа к папкам на компьютере с Windows 7

При совместной работе с другими пользователями или при желании просто поделиться с друзьями каким-то контентом, расположенным на вашем компьютере, необходимо предоставить общий доступ к определенным каталогам, то есть сделать их доступными для других юзеров.

<http://lumpics.ru/how-enable-folder-sharing-on-windows-7/>

Лабораторная работа №2. Установка Kaspersky Free

Необходимо скопировать на компьютер тестовый вирус, установить антивирус, произвести проверку завирусованного файла или каталога, произвести лечение, восстановить вирусный файл из Карантина и добавить его в исключение антивируса.

<http://blogsadmina.ru/soft/kak-ustanovit-besplatnuyu-versiyu-antivirusa-kaspersky.html>

Лабораторная работа №3. Настройка автоматического резервного копирования на ресурс удаленного доступа

При помощи программы «7-Zip» Необходимо создать сценарий архивирования локальной папки с добавлением пароля к архиву и изменением расширения на одно из системных, а также перемещение созданного архива в папку на компьютере в локальной сети. Настроить расписание выполнение задачи по запуску созданного сценария в «Планировщике заданий».

Лабораторная работа №4. Как посмотреть посты всех ваших соседей в соцсетях

https://pikabu.ru/story/kak_posmotret_postyi_vsekh_vashikh_sosedey_v_sotssetyakh_5737027

Лабораторная работа №5. Ищем людей в сети

<https://vk.com/@myironcomp-kak-dela-u-byvshei-ischem-ludei-v-seti>

Лабораторная работа №6. Шифрование с открытым ключом

1. Теоретическая часть

Главная проблема использования одноключевых (симметричных) криптосистем заключается в распределении ключей. Для того, чтобы был возможен обмен информацией между двумя сторонами, ключ должен быть сгенерирован одной из них, а затем в конфиденциальном порядке передан другой. Особую остроту данная проблема приобрела в наши дни, когда криптография стала общедоступной, вследствие чего количество пользователей больших криптосистем может исчисляться сотнями и тысячами.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Находясь под влиянием работы Ральфа Меркле (Ralph Merkle) о распространении открытого ключа, они предложили метод получения секретных ключей для симметричного шифрования, используя открытый канал. В 2002 году Хеллман предложил называть данный алгоритм «Диффи - Хеллмана - Меркле», признавая вклад Меркле в изобретение криптографии с открытым ключом.

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов - Рон Ривест (Ronald Linn Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman) из Массачусетского Технологического Института (MIT)).

Справедливости ради следует отметить, что в декабре 1977 года была обнародована информация, согласно которой британский математик Клиффорд Кокс (Clifford Cocks), работавший в центре правительственной связи (GCHQ) Великобритании, описал систему, аналогичную RSA, в 1973 году, а несколькими месяцами позже в 1974 году Малькольм Вильямсон изобрел математический алгоритм, аналогичный алгоритму Диффи – Хеллмана - Меркле.

Суть шифрования с открытым ключом заключается в том, что для шифрования данных используется один ключ, а для расшифрования другой (поэтому такие системы часто называют **ассиметричными**).

Основная предпосылка, которая привела к появлению шифрования с открытым ключом, заключалась в том, что отправитель сообщения (тот, кто зашифровывает сообщение), не обязательно должен быть способен его расшифровывать. Т.е. даже имея исходное сообщение, ключ, с помощью которого оно шифровалось, и зная алгоритм шифрования, он не может расшифровать закрытое сообщение без знания ключа расшифрования.

Первый ключ, которым шифруется исходное сообщение, называется **открытым** и может быть опубликован для использования всеми пользователями системы. Расшифрование с помощью этого ключа невозможно. Второй ключ, с помощью которого дешифруется сообщение, называется **секретным** (закрытым) и должен быть известен только законному получателю закрытого сообщения.

Алгоритмы шифрования с открытым ключом используют так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством: при заданном значении аргумента x относительно просто вычислить значение функции (x) , однако, если известно значение функции $y = f(x)$, то нет простого пути для вычисления значения аргумента x . Например, функция **SIN**. Зная x , легко найти значение **SIN(x)** (например, $x = \pi$, тогда **SIN(π)** = 0). Однако, если **SIN(x)** = 0, однозначно определить x нельзя, т.к. в этом случае x может быть любым числом, определяемым по формуле $i * \pi$, где i – целое число.

Однако не всякая необратимая функция годится для использования в реальных криптосистемах. В их числе и функция **SIN**. Следует также отметить, что в самом определении необратимости функции присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к криптосистемам с открытым ключом предъявляются два важных и очевидных **требования**.

1. Преобразование исходного текста должно быть условно необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне.

Все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих **типов односторонних преобразований**.

1. Разложение больших чисел на простые множители (алгоритм RSA).
2. Вычисление дискретного логарифма или дискретное возведение в степень (алгоритм Диффи-Хелмана-Меркле, схема Эль-Гамала).
3. Задача об укладке рюкзака (ранца) (авторы Хелман и Меркл).
4. Вычисление корней алгебраических уравнений.
5. Использование конечных автоматов (автор Тао Ренжи).
6. Использование кодовых конструкций.
7. Использование свойств эллиптических кривых.

Алгоритм RSA. Стойкость RSA основывается на большой вычислительной сложности известных алгоритмов разложения произведения простых чисел на сомножители. Например, легко найти произведение двух простых чисел 7 и 13 даже в уме – 91. Попробуйте в уме найти два простых числа, произведение которых равно 323 (числа 17 и 19). Конечно, для современной вычислительной техники найти два простых числа, произведение которых равно 323, не проблема. Поэтому для надежного шифрования алгоритмом RSA, как правило, выбираются простые числа, количество двоичных разрядов которых равно нескольким сотням.

Описание RSA было опубликовано в августе 1977 года в журнале «Scientific American». Авторы RSA поддерживали идею её активного распространения. В свою очередь, Агентство национальной безопасности (США), опасаясь использования этого алгоритма в негосударственных структурах, на протяжении нескольких лет безуспешно требовало прекращения распространения системы. Ситуация порой доходила до абсурда. Например, когда программист Адам Бек (Adam Back) описал на языке Perl алгоритм RSA, состоящий из пяти строк, правительство США запретило распространение этой программы за пределами страны. Люди, недовольные подобным ограничением, в знак протеста напечатали текст этой программы на своих футболках.

Первым этапом любого асимметричного алгоритма является создание получателем шифрограмм пары ключей: открытого и секретного. Для алгоритма RSA этап создания ключей состоит из следующих операций.

Таблица 1. Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбираются два простых числа ¹ p и q .	p=7, q=13
2	Вычисляется произведение n = p * q.	n=91
3	Вычисляется функция Эйлера ² φ(n) .	φ(n)=(7-1)(13-1)= 91-7-13+1 = 72
4	Выбирается открытый ключ e , как произвольное число (0<e<n), взаимно простое ³ с результатом функции Эйлера (e ⊥ φ(n)).	e=5
5	Вычисляется секретный ключ d , как обратное число ⁴ к e по модулю φ(n) , из соотношения (d*e) mod φ(n) = 1.	(d*5) mod 72 = 1, d = 29
6	Публикуются открытый ключ (e , n) в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике).	

Примечания. **Простое число** – натуральное число, большее единицы и не имеющее других делителей, кроме самого себя и единицы. **Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1 (например, p=3, q=5, n=15, j(n)=8 – взаимно простые с 15 – 1, 2, 4, 7, 8, 11, 13, 14).

Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C = T^e \bmod n, \quad (10)$$

$$T = C^d \bmod n. \quad (11)$$

где T, C - числовые эквиваленты символов открытого и шифрованного сообщения.

Пример шифрования по алгоритму RSA приведен в следующей таблице. Коды букв соответствуют их положению в русском алфавите (начиная с 1).

Таблица 2. Пример шифрования по алгоритму RSA

Открытое сообщение, T	Символ	А	Б	Р	А	М	О	В
	Код	1	2	18	1	14	16	3
Шифрограмма, C = T ⁵ mod 91		1	32	44	1	14	74	61
Открытое сообщение, T = C ²⁹ mod 91		1	2	18	1	14	16	3

Следует отметить, что **p** и **q** выбираются таким образом, чтобы **n** было больше кода любого символа открытого сообщения. В автоматизированных системах исходное сообщение переводиться в двоичное представление, после чего шифрование выполняется над блоками бит, равной длины. При этом длина блока должна быть меньше, чем длина двоичного представления **n**.

В заключении следует отметить стойкость данного алгоритма. В 2003 г. Ади Шамир и Эран Тромер разработали схему устройства TWIRL, которое при стоимости \$ 10 000 может дешифровать 512-битный ключ за 10 минут, а при стоимости \$ 10 000 000 – 1024-битный ключ меньше, чем за год. В настоящее время Лаборатория RSA рекомендует использовать ключи размером 2048 битов.

2. Общая постановка задачи

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

Для вычисления больших чисел можно воспользоваться продвинутым калькулятором: <http://itpride.net/useful/ochen-prodvinutyj-onlajn-kalkulyator.html>