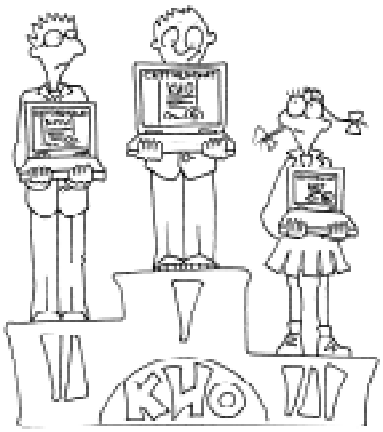
Поздняков Сергей Николаевич,
Степулёнок Денис Олегович

ЭЛЕКТРОННЫЙ СЕРТИФИКАТ

От редакции. В этом году участники конкурса КИО получили электронные сертификаты участника. В статье рассказывается о том, что означает этот термин и чем такой сертификат отличается от обычного – бумажного – документа. Программа «Электронная Россия», объявленная правительством РФ несколько лет назад, подразумевает появление систем оборота электронных документов в управлении государством и электронных денег в банковской системе. В основе этих механизмов лежат те же идеи, на которых был построен электронный сертификат участника. Поэтому редакция считает очень полезным рассмотреть на своих страницах опыт внедрения в обиход электронных документов.

КОД С ОТКРЫТОЙ ЧАСТЬЮ

Выдача официального документа – такого как электронный сертификат – подразумевает наличие на нем электронной подписи, удостоверяющей подлинность документа. Несведущий человек может подумать, что это отсканированная подпись председателя жюри. Но если бы это было так, то любой получатель такого файла смог бы сам «выдавать» подобные сертификаты, копируя на них нужную подпись. Значит, нужен механизм, препятствующий совершению этого действия. Поэтому электронной подписью называют не росчерк руководителя, а такую шифровку документа, которую расшифровать может любой желающий, а зашифровать другой документ тем же шифром – никто. Механизм такой шифровки определяется односторонней функцией. Каждый школьник знаком, по крайней мере, с одной такой функцией – функцией перемножения чисел. Алгоритм умножения «столбиком» знает каждый – он прост и эффективен, то есть работает быстро, даже если числа имеют сотни цифр. В то же время обратная операция – разложение на множители – эффективного алгоритма не имеет (точнее, пока никому не удалось его найти). Разложение на множители связано с подбором делителей. Для небольших чисел это нетрудно, поэтому на школьных уроках эту проблему обычно не замечают. Для больших же чисел эта переборная работа может занять годы у самого лучшего компьютера.



...участники конкурса КИО получили электронные сертификаты участника.

Рассмотрим для примера разложение числа из 100 цифр на два множителя. Для подбора делителя надо перебрать (в худшем случае) все числа от двойки до чисел из 50 цифр (пока частное не станет меньше делителя). Если компьютер перебирает миллиард чисел в секунду, то для такого перебора понадобится число секунд, имеющее в своей записи около 40 цифр (поделили на 1000000000). В часах это будет в 3600 раз меньше, в сутках еще в 24 раза меньше, в годах еще в 365 раз меньше. Но даже если огрубить результат, увеличивая эти делители, то все равно получим число, которое

записывается более чем 30 цифрами: не менее 10000000000000000000000000000000 лет!

Для сравнения на умножение двух чисел из 50 цифр уйдет 2500 элементарных умножений пар цифр и примерно такое же число сложений. Эти действия машина выполнит за доли секунды.

Отличие во времени впечатляющее. Однако такой результат будет в «худшем» случае, то есть для этого надо найти такое число, которое не имело бы маленьких делителей. Лучше всего для этого подойдет произведение двух простых чисел p и q, каждое из которых содержит около 50 цифр.

Пусть мы нашли такие числа (хотя сразу заметим, что это не простая задача). Что делать дальше?

Во-первых, сам буквенный текст надо превратить в последовательность длинных натуральных чисел фиксированной длины (для этого каждый символ шифруется набором цифр, а полученная последовательность разбивается на блоки фиксированной длины).

Обозначим последовательность этих числовых блоков как $x_1, x_2, x_3, ..., x_n$.

Теперь перейдем к шифровке: каждое число зашифруем по формуле

$$y_i = x_i^e \bmod m$$

здесь $m = pq$ – произведение выбранных простых чисел, а e – некоторое число, которое, наряду с p и q, является закрытой (секретной) частью шифра. Эта запись означает, что число x_i возводится в степень e, а затем находится остаток от деления на m полученного результата.

Числа-блоки x_i по величине не должны превышать m, иначе однозначно текст не восстановится.

Как же полученный текст будет расшифровываться?

Все получатели документа (и все желающие) имеют доступ к открытой части кода – числу m и числу d, которое обладает интересным свойством

$$ed = 1 \bmod \varphi(m).$$

Здесь $\varphi(m)$ обозначает число взаимно простых с m чисел, меньших его. Эта функция называется функцией Эйлера. Сама запись говорит о том, что число d должно в

...электронной подписью называют не росчерк руководителя...

некотором смысле быть обратным к e, то есть остаток от деления их произведения на $\varphi(m)$ должен равняться единице. Для нахождения такого числа используется одна из модификаций алгоритма Евклида (см. статью В.А. Петрова, С.Н. Позднякова «Занятие 1. Алгоритмы над целыми числами», журнал «Компьютерные инструменты в образовании», № 1, 1999).

Теперь можно сообщить, что число e выбирается так, чтобы быть взаимно простым с $\varphi(m)$, иначе d не существует.

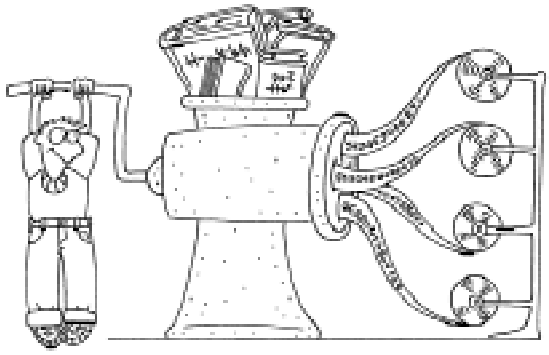
Далее получатели шифровки проделывают с буквами операцию, очень похожую на шифровку: они вычисляют $y_i^d \bmod m$.

Удивительно, но при этом получается x_i!

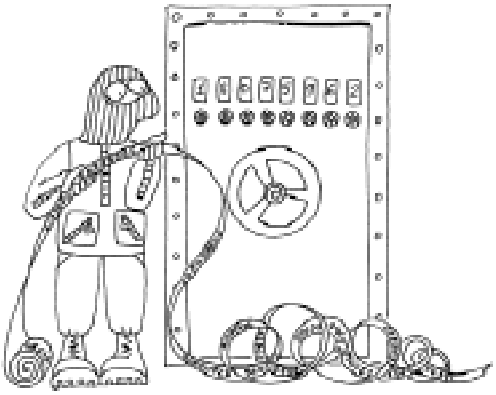
Этот результат объясняется теоремой Эйлера, которая гласит, что

$$x^{\varphi(m)} = 1 \bmod m$$

для всех чисел x, взаимно простых с m. Например, остаток от деления 2^{24} на 35



... буквенный текст надо превратить в последовательность длинных натуральных чисел фиксированной длины...



...почему же трудно «взломать» этот код...

равен 1, так как число взаимно простых с 35 чисел, меньших 35 равно 24. Проверьте!

Проведем доказательство правильности расшифровки.

$$y_i^d \bmod m = (x_i^e)^d \bmod m = x_i^{ed} \bmod m = x_i^{1+k\varphi(m)} \bmod m = x_i\, x_i^{\varphi(m)} \bmod m = x_i$$

Здесь замена ed на $1 + k\varphi(m)$ сделана потому, что ed имеет при делении на $\varphi(m)$ остаток 1 и, следовательно, отличается от 1 на число, кратное $\varphi(m)$ (коэффициент кратности k).

Возникает вопрос, а почему же трудно «взломать» этот код и отыскать число d по известному числу e? Но для этого надо знать $\varphi(m)$, которое в свою очередь не найти без разложения m на множители. Круг замкнулся!

Этот алгоритм носит название RSA. Алгоритм RSA стоит у истоков асимметричной криптографии. Он был предложен тремя исследователями-математиками Рональдом Ривестом (R.Rivest), Ади Шамиром (A.Shamir) и Леонардом Адльманом (L.Adleman) в 1977–78 годах.

В выдаваемом сертификате открытые части шифра находятся в самой оболочке, которая позволяет красиво «отрисовывать» и печатать сертификат. Это избавляет получателей от необходимости вводить длинные числа открытой части шифра (рисунок 1).

Внутри самой оболочки находится инструмент, демонстрирующий работу шифра.

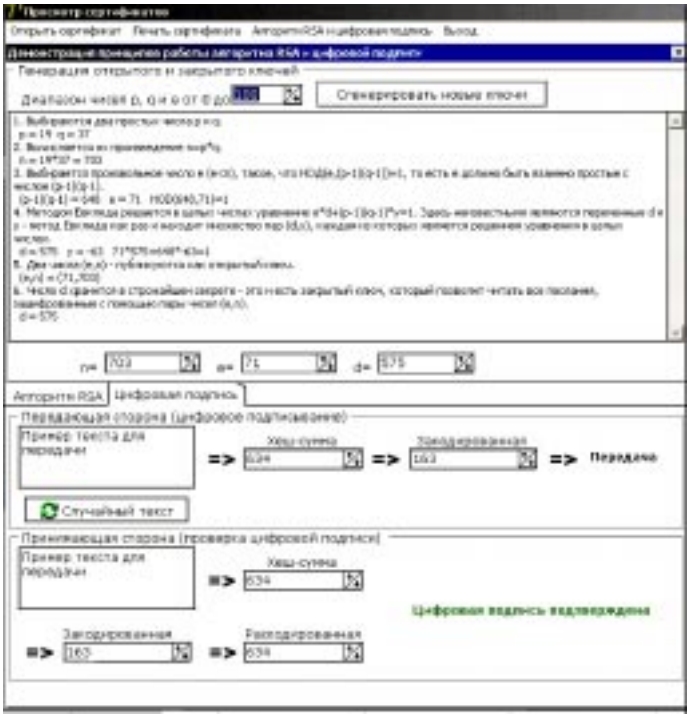


Рисунок 1.

Поздняков Сергей Николаевич,
доктор педагогических наук,
профессор кафедры ВМ-2 СПбГЭТУ,

Степулёнок Денис Олегович,
инженер-программист, выпускник
кафедры АСОиУ СПбГЭТУ.