УКАЗАНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧИ № 27

Любая криптосистема основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в системе, где количество пользователей составляет десятки и сотни управление ключами - серьезная проблема. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации. В этом случае необходимо введение какой-либо случайной величины в процесс шифрования.

Конкретно для реализации алгоритма RSA [4] нас интересуют большие простые числа. Где их взять?

Простых чисел не так мало, как кажется, например, существует приблизительно 10^{151} простых чисел длиною от 1 бита до 512 включительно. Для чисел близких n, вероятность того, что выбранное число окажется простым, равна 1/ln n. Поэтому полное число простых чисел, меньших n равно n/ln n. Считается, что вероятность выбора двумя людьми одного и того же большого простого числа пренебрежимо мала.

Существуют различные вероятностные проверки на простоту чисел, определяющие является ли число простым с заданной степенью достоверности. При условии, что эта степень достоверности достаточно велика, такие способы достаточно хороши. Такие простые числа часто называют «промышленными простыми», т.е. они просты с контролируемой возможностью ошибки.

Повсеместно используемым является алгоритм, разработанный Майклом Рабином по идеям Гари Миллера.

Тест Rabin-Miller

Выберите для проверки случайное число p. Вычислите b как наибольшее число делений p-1 на 2 т.е. 2^b – наибольшая степень числа 2, на которое делится p-1. Затем вычислите m, такое, что $p=1+2^b m$

j Выберите случайное число а, меньшее p.

k Установите $j=0$ и $z=a^m \bmod p$

l Если $z=1$ или если $z=p-1$, то р проходит проверку и может быть простым числом.

m Если $j>0$ и $z=1$, то р не является простым числом.

n Установите $j=j+1$.

Если $j<b$ и $z<p-1$, установите $z=z^2 \bmod p$ и вернитесь на **m**.

Если $z=p-1$, то p проходит проверку и может быть простым числом.

o Если $j=b$ и $z\neq p-1$, то р не является простым числом.

Повторить эту проверку нужно t раз.

Доказано, что в этом тесте вероятность прохождения проверки составным числом убывает быстрее, чем в прочих. Гарантируется, что 75% возможных значений a окажутся показателями того, что выбранное число p составное. Это значит, что вероятность принять составное число p за простое не превышает величины $(¼)^t$.

Генерация простого числа

j Сгенерируйте случайное n-битовое число p.

k Установите его старший и младший биты равными 1. Старший бит будет гарантировать требуемую длину искомого числа, а младший бит обеспечивает его нечетность.

l Убедитесь, что p не делится на небольшие простые числа: 3, 5, 7, 11 и т.д. Наиболее эффективной является проверка на делимость для всех простых чисел, меньших 2000.

m Выполните тест Rabin-Miller минимум 5 раз.

Если p не прошло хотя бы одну проверку из **l** или **m**, оно не является простым.

Проверка, что случайное нечетное p не делится на 3, 5 и 7 отсекает 54% нечетных чисел. Проверка делимости на все простые числа, меньшие 256 отсекает 80% составных нечетных чисел.

Даже, если составное число «просочилось» через этот алгоритм, это будет сразу же замечено, т.к. шифрование и дешифрование не будут работать.