appeared in 2000-03

Countdown to computer security

Two young computer engineers at IIT, Kanpur have made a splash in the field of prime numbers, says **S.Ananthanarayanan**.

Neeraj Kayal and Nitin Saxena, under the guidance of Prof Mahindra Agarwal have developed an elegant and speedy mathematical procedure for testing whether a gigantic number is a prime number or not. The discovery is of immense importance, both in academics and commerce. It has made news over the Internet and has been reported by the New York Times.

Prime numbers?

A prime is simply a number that cannot be divided by anything but the number 1 and itself. Easy examples are the numbers 3, 5, 7, 11, 17.. . We can see that the numbers 9, 15, 21, 221, 5467 are not primes, though for the last two, it would take some effort. We could also check that the numbers, 223, 941, 4561 are actually primes, though this would take a big effort!

This question of how, in the generation of numbers in the world, the sequence of numbers is punctuated by instances that do not relate to the numbers that have gone before, has intrigued mathematicians along the ages. Devices, methods, incantations, to generate consecutive prime numbers, or to be able to say whether or not a given number is a prime have been developed with varying efficacy by mathematical greats, but the subject is still mystifying and remains an uncharted sea.

The few examples cited above might have given the reader a glimpse of how things get difficult when we deal with larger and larger numbers. Now let her just try it with a number like 55555559 or 555555587 or 1260588001 or 1260588281* and she will agree that it becomes positively infernal when we think of numbers with 15, 20, 30, 100 digits!

What good is it?

In financial transactions on the Internet, the interest is in being sure that messages are secret and not tampered with. And also to be sure of the identity of the sender. One way is to use a code that only the two parties to the deal know of. But the

problem with this solution is that codes can be broken with patience and persistence, virtues that computers have in abundance!

But dealing with large primes is difficult even for computers. A code made with two large prime numbers, one known to the sender and the other to the receiver is proving to be just the answer. If the code uses the result of multiplying these two numbers, then the cracking the code would first involve finding the two factors that divide into the product, which amounts to proving that the number is not a prime.

Now if the primes had 33 digits each, then a ‘ham-handed’ method would be for a computer to try out about that many divisions. But even if the computer checked only one in a million of the possibilities and did a million checks a second, the number of seconds needed would have 21 digits! This is thousands and thousands of years!

The real methods are much ‘smarter’, of course, and at the same time, the codes also use more than 33 digits. But the work of the computers scientists at Kanpur is an advance that could help create (and crack) more efficient codes in e-commerce.