Prime Spies

BY DENNIS E. SHASHA

Number theory, once thought an esoteric discipline concerned with curious properties of prime numbers, turns out to form the underpinnings of modern cryptography. The Rivest-Shamir-Adleman public-key cryptography algorithm (RSA, for short) used in most e-commerce transactions relies on the (unproved but widely believed) difficulty of factoring a number that is the product of two primes.

Multiplying two large primes is an example of a so-called one-way function: the multiplication takes only a few milliseconds and is proportional to the length of the binary representations of the numbers; in contrast, discovering the two primes given the product is slow, taking hours for a 512-bit product and continuing a slow exponential climb (in the length of the product) after that. For 2,048-bit numbers, factoring is considered impractical, as far as is publicly known. Fast-factoring algorithms, if they exist, would have untold applications for industrial and even military espionage.

This brings us to a puzzle first posed by John McCarthy (inventor of the programming language Lisp and theoretical Artificial Intelligence) and solved by Michael Rabin (the playful inventor of so many important computer algorithms) in the 1950s. The puzzle goes like this: You have a bunch of spies ready to go into enemy territory. When they return to cross the frontier into your country, you want to avoid getting them shot, while at the same time preventing enemy spies from entering. So each must present a password to the guards, which the guards will verify. Whereas you trust your spies, and your guards are loyal, you believe the guards may loosen their tongues in bars at night. What information should the guards receive, and how should the spies present their passwords, so that only your spies get through and nobody else, even if the guards go out for a couple? Consider the discussion about primes to be a hint.

Dennis E. Shasha's third book of puzzles, Dr. Ecco's Cyberpuzzles, *has just been published.*

Answer to Last Month's Puzzle

If you spread your investments over 10 companies, giving each $1.43 million, the chance that at least seven will yield 10-fold returns is more than 95 percent. If that happens, the total return would be $100.1 million. This strategy leaves $2.7 million in reserve for future investments. For a full explanation, visit www.sciam.com

Web Solution

For a peek at the answer to this month's problem, visit www.sciam.com

CREDIT