Factoring with a TWINKLE

The so-called RSA encryption system is widely used to safeguard electronic mail and credit card payments on the Internet. To unscramble confidential transmitted information, a snoop's computer must factor a large number into its two prime-number components. If the number is large enough, such a task is prohibitively time-consuming (SN: 2/6/99, p. 95). In the RSA scheme, the numbers used in Internet applications typically have about 150 decimal digits (512 bits).

Advances in computer technology and design, however, are quickly bringing such numbers within reach of spies and criminals. Computer scientist Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, has now proposed an ingenious design that takes advantage of existing technology to create a factoring machine for rapidly cracking RSA-based codes. "The main practical significance of such an improvement is that it can make 512-bit numbers easy to crack," says Shamir, who is one of the inventors of the RSA system. To ensure security, numbers much larger than 512 bits will be needed.

The new factoring technique relies on a novel optoelectronic device that Shamir calls The Weizmann Institute Key Locating Engine, or TWINKLE. The device—not yet built—would be housed in an opaque cylinder about 6 inches wide and 10 inches high. An array of light-emitting diodes, driven to flash at various frequencies corresponding to prime numbers, would cover the cylinder's bottom. The cylinder's top would hold a photodetector that measures the total amount of light emitted at any given moment by all the light-emitting diodes. In effect, the array would act like thousands of computers simultaneously running through candidate primes.

A computer would then transform photodetector signals into numbers related to the prime factor being sought. Those numbers then would go into standard mathematical recipes, such as the quadratic sieve or number-field sieve, for factoring large numbers. Adding the optical device promises to make factoring more than 100 times speedier.

"There's no new mathematics in this machine," says cryptographer Bruce Schneier of Counterpane Systems in Minneapolis. "It's just a much faster way of doing existing mathematics."

"Designing and constructing the first prototype of this device [could] cost hundreds of thousands of dollars, but the manufacturing cost of each additional device [would be] about $5,000," Shamir estimates.

"If I were to put a team on it, I would expect it would take 1 to 2 years to . . . build a prototype," Schneier says. —*I.P.*

Data storage on a global scale

The destruction of the famous library in Alexandria at various times in ancient history meant the irrevocable loss of huge collections of texts. Today, the failure or sabotage of a massive computer system storing archival material could present a similar disaster. One way to avoid the problem is to spread information out over the Internet in such a way that programmers could recreate it, even after a large fraction of the participating computers had been disconnected or destroyed.

Peter N. Yianilos of the NEC Research Institute in Princeton, N.J., and his collaborators have now unveiled the prototype of such a dispersed-data-storage system for the Internet. They call it the Archival Intermemory.

The researchers envision breaking up electronic data into memory units, mathematically transforming the files so they contain redundant information, and then parceling out fragments of that material to computers all over the world. At any time, Intermemory software could reassemble complete documents from as few as half of the constituent pieces. —*I.P.*