Hiding in Lattices

An improved mathematical strategy for encrypting data

By IVARS PETERSON

Sending a message over the Internet is like mailing a postcard. It can be read by anyone.

Protecting sensitive information—whether a credit card number, a password, or other data—requires encrypting the message so that no eavesdropper or thief can read the contents in transit. Indeed, many online retailers now use systems that routinely encrypt any information a customer enters to order a product.

In general, the hiding is accomplished in such a way that breaking the code involves solving an extraordinarily difficult mathematical problem—one so hard that even a thief with access to the world's most powerful supercomputers would fail.

For instance, it's easy to multiply two numbers. It's considerably more difficult, given that product, to work out what numbers were multiplied together to generate it. Determining that 57,814,193 is the product of the two prime numbers 7,079 and 8,167 requires much more computer time than multiplying the two primes.

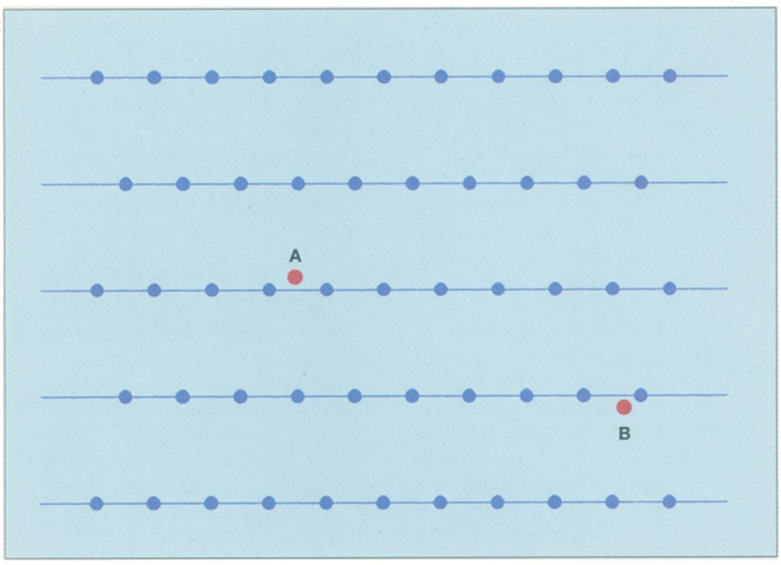
The belief that factoring huge numbers is intrinsically difficult underlies one widely used cryptosystem. Cracking such codes typically requires factoring numbers that are 200 or more digits long (SN: 5/14/94, p. 308).

However, the factoring approach isn't completely foolproof. Computer scientists can't yet guarantee that no one will ever discover a mathematical shortcut that makes factoring quick and easy on a computer.

Moreover, certain numbers turn out to be particularly easy to factor. There's always the danger of inadvertently picking one of these numbers for encryption, making the resulting secret message vulnerable to attack.

Now, Miklós Ajtai and Cynthia Dwork of the IBM Almaden Research Center in San Jose, Calif., have come up with an alternative mathematical basis for protecting confidential information. Moreover, they can prove that breaking a randomly generated instance of their new cryptosystem is equivalent to working out the hardest possible case.

I. Peterson



The Ajtai-Dwork cryptosystem involves the use of randomly oriented lattices in which the rows are much farther apart than points along a row. Encoding 0 means finding a point close to a hyperplane without knowing where the hyperplanes are. In this two-dimensional example of a lattice, the hyperplanes are lines, and two 0s are encoded as points A and B.

In other words, there are no "easy" exceptions that could be exploited to crack the code. "You can't get unlucky and make a bad choice," Dwork says.

The new scheme represents a potentially useful addition to the small handful of cryptosystems now in use. "It's an interesting and important development," says Andrew M. Odlyzko of AT&T Labs–Research in Florham Park, N.J. "People would rather not put all their trust in systems that could fall if a single mathematical problem were to be solved."

Ajtai and Dwork described their cryptosystem at the Association for Computing Machinery's Symposium on Theory of Computing, held earlier this year in El Paso, Texas.

Conventional cryptography typically requires a key—a string of numbers—shared by both sender and recipient. The key can then be used in a series of mathematical operations to scramble the digits representing a message. Deciphering the message involves going through the same procedure in reverse, using the same key (SN: 2/1/97, p. 78).

The trouble with such a scheme is that the two parties must initially communicate in some way to establish the shared key. Such exchanges are cumbersome and potentially insecure, especially when keys are lengthy and regularly changed to increase security (SN: 2/10/96, p. 90).

Public key cryptography offers a way around the key exchange problem. This method requires the use of a pair of complementary keys instead of a single, shared key. One key, which is publicly available, is used to encrypt information; the other key, known only to the intended recipient, is used to decipher the message. Thus, what the public key does, only the secret key can undo.

The security of this type of cryptosystem rests on finding a mathematical procedure to generate two complementary keys such that knowing just the public key and the encryption method is not enough to deduce the private key. The mathematical operation must act like a trap that's much easier to fall into than to escape.

The presumed difficulty of factoring provides such a trapdoor in the RSA cryptosystem, invented by Ronald L. Rivest of the Massachusetts Institute of Technology, Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, and Leonard M. Adleman of the University of Southern California in Los Angeles. The secret key consists of the two prime numbers that were multiplied together to create the lengthier public key.

The sender of an electronic message uses software that automatically scrambles the information by a procedure involving the publicly known numerical key. The recipient's software decrypts the message by using the two prime factors of its private key. The only way an eavesdropper can read an intercepted message is by factoring the public key.

Mathematicians and computer scientists have also proposed public key cryptosystems based on mathematical operations other than factoring. One popular approach involves so-called discrete logarithms.

Another method, based on a mathematical puzzle known as the knapsack problem, initially looked promising, but researchers discovered serious loopholes in many of the different types of knapsack cryptosystems that had been constructed (SN: 11/24/84, p. 330).

The limited number of options available has long been a source of concern among security experts, especially as computers get faster and researchers come up with improved procedures for factoring.

The work of Ajtai and Dwork introduces a new approach to public key cryptography—one based on mathematical constructs called lattices.

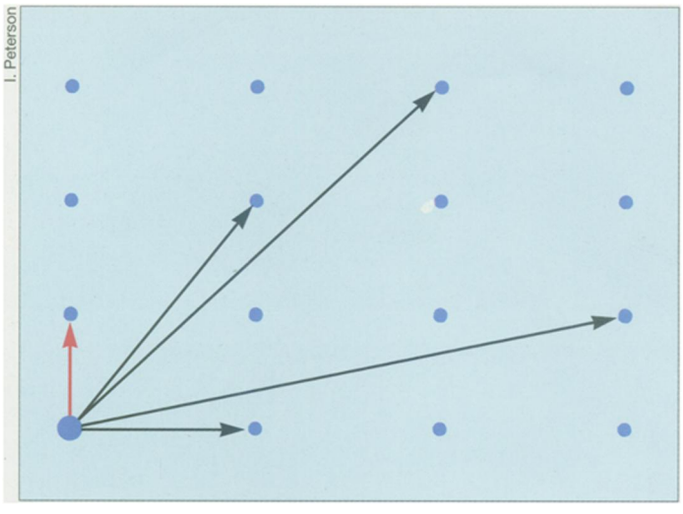
A lattice is a regular array of points, each one specified by a set of coordinates. Two coordinates would designate the location of a point in a two-dimensional lattice; three coordinates, a point in a three-dimensional lattice; four coordinates, a point in a four-dimensional lattice; and so on.

The two- and three-dimensional cases are easy to visualize as orderly arrangements of dots on a sheet of paper or points distributed in space like the atoms of a crystal. By looking at such arrays from different angles, one can see that the points fall into natural groupings—sets of parallel lines or sets of parallel planes. In higher dimensions, such features are called hyperplanes.

In the Ajtai-Dwork cryptosystem, a particular set of hidden hyperplanes constitutes the private key. The public key is a method of generating points that are guaranteed to be near one of those hyperplanes without revealing where any of the hyperplanes is. Even generating a large number of points isn't sufficient to unveil the hyperplanes they trace out.

To send an encrypted message, the user provides the information as a string of 1s and 0s. Software encrypts the message one bit at a time. If the bit is 0, the computer uses the public key to find a point whose coordinates place it very near one of the hidden hyperplanes. If the bit is 1, the computer comes up with a random point somewhere in the high-dimensional space of the lattice.

The private key allows the recipient to determine the distance of each point from the nearest hyperplane. If the distance is sufficiently small, the point is decrypted to represent 0. Otherwise, the point represents 1.



One way to define the position of a point in a lattice is to draw a vector (arrow) from the origin to the point. In this two-dimensional example, it's easy to find the point closest to the origin and, hence, identify the shortest vector. In higher dimensions, however, the problem is much more difficult. In lattices in which the rows are much farther apart than points along a row, finding the "unique" shortest vector is also an extremely difficult computational problem.

There is a tiny chance of error. Once in a long while, a randomly selected point can land close to a hyperplane, so 1 may occasionally be decrypted as 0.

"What we proved, roughly, is that you can't distinguish points that are near the hyperplanes from points that are far from the hyperplanes if you don't already know where those hyperplanes are," Dwork says.

The security of this system rests on the computational difficulty of finding, in effect, the "unique" shortest line segment (or vector) that connects any pair of points in a given lattice. That's easy to do in two or three dimensions. However, there's no quick way of finding the shortest vector in, say, a 100-dimensional lattice, because the number of possible pairs of points that need to be checked becomes exponentially large.

In the Ajtai-Dwork cryptosystem, deducing the private key to find the hyperplanes and decipher a message implies the ability to solve the shortest-vector problem in high dimensions—something that has so far proved extremely difficult to do.

The researchers also proved that breaking a randomly generated instance of their cryptosystem—one that uses a randomly generated set of hyperplanes—is as hard as solving the hardest possible case. Thus, each key is equally difficult to crack.

In effect, our scheme "is more secure than any existing system," Ajtai says.

At present, the cryptosystem developed by Ajtai and Dwork remains more a mathematical exercise than a practical reality. "Quite a bit of work would be required to make the scheme practical," Odlyzko says.

In its current form, for example, the encryption process generates an encoded message that is considerably longer than the original message. "We need to make the system more efficient, and we have ideas on how to do that," Ajtai says.

Ajtai and Dwork are also checking for loopholes and exploring ways to fine-tune their scheme. "It's possible that the system may be secure even for small dimensions," Dwork says.

Other researchers are studying the cryptographic implications of these and related findings. For one thing, some key mathematical results obtained by Ajtai last year may help revive interest in knapsack cryptosystems by suggesting ways to bulletproof those schemes.

"No one yet knows how to prove that any of the underlying problems in use today is absolutely impossible to solve," Ajtai remarks. "Until that happens, the best we can do is to show that randomly generated instances of the new cryptosystem are as hard to crack as the hardest instances of the underlying problem."

Dwork and Ajtai also see possible applications of their technique in generating random numbers on a computer and perhaps for creating a digital signature, which certifies that an electronic document truly belongs to the stated author (SN: 9/7/91, p. 148).

Cryptographers now have a new mathematical field on which to exercise their schemes. □