THE UNPACKING OF A KNAPSACK

Schemes for encrypting messages based on a mathematical puzzle known as the 'knapsack problem' turn out to be less secure than cryptologists had hoped

Robert Bourdeaux

By IVARS PETERSON

It shouldn't take very long for anyone to figure out what the secret message PZFBKZB KBTP says. Each letter of the original message is replaced by a letter that is a fixed number of places away; for example, an A by a C, a B by a D, and so on. Julius Caesar used this kind of simple cipher more than 2,000 years ago to hide military information. Today, encryption is widely used in places like the Department of Defense, where sensitive data must be protected from eavesdroppers and spies. An increasing number of bankers and others concerned about computer security are also turning to cryptography.

Modern encryption schemes are much more elaborate and mathematically complex than Caesar's simple cipher. But are they unbreakable? These cryptosystems are the central figures in a sophisticated mathematical game played by a small group of researchers — mainly mathematicians and computer scientists — who are adept at inventing and solving puzzles. They gleefully pursue the fatal flaws that may lie hidden in rival encryption schemes while trying to come up with new methods that resist such determined attacks.

The latest victim is a group of schemes called "knapsack cryptosystems." They are based on a puzzle known as the "knapsack problem," which goes something like this: Given the total weight of a knapsack and its contents and the weights of the individual items that may be in the knapsack, determine which items are likely to be packed inside so that the total weight adds up to the given amount. Mathematically, the more general problem involves deciding whether some members of a particular collection of positive integers add up to another given integer. If the collection of numbers contains 1, 2, 4, 8, 16 and 32 and the given total is 37, the answer is "yes" because $1 + 4 + 32 = 37$.

Last summer, at the Crypto '84 meeting in Santa Barbara, Calif., Ernest F. Brickell of the Sandia National Laboratories in Albuquerque, N.M., presented an outline of his attack on "iterated knapsacks." Brickell's work eliminates the most important branch of knapsack-based cryptosystems discovered so far.

"I think the traditional approach, which is based on a simple knapsack that is scrambled by iterative multiplication, is for all practical purposes dead," says Adi Shamir of the Weizmann Institute of Science in Israel and co-inventor of several cryptosystems. "It started crumbling some time ago; people were hesitant about using it. But I believe that Ernie Brickell has the last word on this particular scheme, and I don't think it will revive again."

Knapsack cryptosystems are important because they belong to one of only two classes of practical encryption methods that have been proposed as "public-key" cryptosystems. In conventional cryptography, the sender must have a secret key for encrypting messages and the receiver a secret key for decrypting messages. The problem with this method is that the sender must also transmit the secret decrypting key to the receiver in a secure way before any encrypted messages can be sent.

In 1976, Martin E. Hellman of Stanford University and Whitfield Diffie, now at BNR Inc. in Mountain View, Calif., proposed the notion of public-key cryptography to avoid the key exchange problem. In this system, the encryption key is public and available to all senders, while the decryption key is kept secret. The security of this system rests on finding a mathematical way of generating two related keys such that knowing just one of the keys and the encryption method is not enough to recover the second key.

In 1978, two candidate public-key cryptosystems surfaced. One was the RSA scheme, based on the difficulty of factoring large numbers (SN: 1/14/84, p. 20) and named for its inventors, Shamir, Ronald L. Rivest and Leonard M. Adleman, all at the Massachusetts Institute of Technology at the time. The other was the knapsack scheme devised by Hellman and Ralph C. Merkle, now with ELXSI in San Jose, Calif. Initially, knapsack cryptosystems were favored because they offered faster encryption and decryption than the RSA system. At least two companies seriously considered designing special integrated circuit

chips to implement a knapsack cryptosystem.

In a knapsack public-key cryptosystem, the public key is an ordered set of *n* "knapsack weights." To encrypt a message consisting of a sequence of 0s and 1s (for example, data stored in a computer), the message is broken into blocks of *n* bits. Each bit in a block is multiplied by each corresponding number in the public key, and then all these products are added together. The answer is the encrypted message. Whether the method works depends on the proper selection of the "weights" in the knapsack.

Merkle and Hellman's idea was to take an "easy" knapsack problem for which a fast method of solution was known and to disguise it by running it through a "trapdoor" to produce a knapsack that masquerades as a "hard" knapsack, or one that takes an incredibly long time to solve. One simple example of an easy knapsack is the special set of numbers 1, 2, 4, 8, 16 and 32. Each number is one larger than the sum of all the previous numbers. If the encrypted message is 37, it isn't difficult to discover that the actual message is 101001, because the first, third and sixth numbers in the knapsack (or public key) add up to 37.

Merkle and Hellman used a generalization of this example, called a superincreasing knapsack, as their set of "weights." As a trapdoor, they used a "modular multiplication" pair. For the pair of numbers (28, 71), for instance, each original "weight" is multiplied by 28 and then divided by 71. Only the remainders are written down. This turns the key into the numbers 11, 41, 22, 56, 28 and 44. To disguise the knapsack further, the items can also be rearranged into another order. Decryption involves finding another modular multiplication pair (in this case, 33 and 71) that converts the public key back into its original form, and the message is again easy to solve. There happens to be a fast way of finding this reverse modular multiplication pair. More complicated schemes — iterated knapsacks — involve performing several modular multiplications.

"What was apparent early was that it seemed that there might be an attack," says Brickell. "Nobody really knew of one, but we thought there might be one." Somewhere in the patterns of digits in the encrypted messages and public keys were subtle clues that would make it possible to decrypt any message.

Merkle compares the process of determining whether an encryption scheme is breakable with finding one's way out of a maze. "It's like being in the middle of a maze, and you're wandering around in some small piece of it," he says. If someone asks you whether you can get out of the maze, unless you're godlike and can look down on the maze from above, it's very difficult to say either there is or there is not an exit.

In 1982, Shamir made the first successful attack on the simplest form of the knapsack cryptosystem. He found that certain information about superincreasing sequences is not well disguised by a modular multiplication trapdoor. In addition, that information could be recovered rapidly by solving a special kind of mathematics problem (finding a short vector in a lattice). Shamir's method became practical with the invention in the same year of an algorithm for solving this problem quickly. Soon after, using a similar approach, Adleman broke another form of the knapsack cryptosystems known as the Graham-Shamir knapsack.

Meanwhile, Shamir collected $100 from Merkle, who had offered that sum as a prize for anyone who could break his basic scheme. But Merkle, reacting to the publicity surrounding Shamir's feat and the incorrect assertion in TIME magazine and elsewhere that all knapsack cryptosystems were no longer secure, offered a new $1,000 prize for breaking the iterated knapsack. Last month, Merkle conceded that Brickell had won the prize, and Brickell received his check. "The result is very impressive," Merkle wrote.

Says Merkle, "I think the breaking of iterated knapsacks is quite surprising and indicates a degree of insecurity that had not been suspected at all."

Brickell's technique depends on the fact that modular multiplication is the only method being used to hide the knapsack. "With my technique, it doesn't matter how many times you do this [modular multiplication]," says Brickell. "What's really significant is that it's the only technique being used to hide the information."

Almost everyone working in cryptology agrees that Brickell's approach works. "It's a beautiful piece of work," says Shamir. Brickell is now trying to make his mathematical result more rigorous. "I made some assumptions and wrote a computer program to implement it to make sure it worked," he says. "Now, I'm trying to prove those assumptions." In computer tests, his scheme has broken knapsack cryptosystems with up to 100 weights and 20 iterations. The decryption process takes about an hour on a Cray supercomputer.

However, this doesn't rule out the possibility that a secure knapsack cryptosystem exists, Brickell adds. "What this says is that if you use one, you have to use something other than modular arithmetic for hiding it."

Jeffrey C. Lagarias of AT&T Bell Laboratories in Murray Hill, N.J., agrees. "These various attacks do not totally close the door on there being a secure knapsack cryptosystem," he says. "But I would say they cast extremely grave doubts on it." Lagarias, together with Andrew Odlyzko, helped establish some of the basic ideas that led to Brickell's successful attack.

Of course, cryptologists can't resist the challenge of coming up with a cryptosystem that circumvents the flaws pinpointed by Brickell's decryption technique. At Crypto '84, Rivest and Benny Chor were ready with a new knapsack public-key cryptosystem based on arithmetic in mathematical structures called "finite fields."

"This one avoids the dangers that have been revealed [in earlier systems]," says Rivest. "We're hopeful that it'll survive, but we can't tell."

"The jury is still out about the security of the [Chor-Rivest] scheme," says Shamir. "It's based on deep mathematical structures, and you have to give mathematicians a chance to look at it." He adds, "You have to be extremely cautious when claiming that a cryptosystem is strong. The history of cryptography is essentially a history of failures. Lots of cryptosystems, which were invented and then used, proved to be insecure, sometimes with disastrous results."

"The thing that interests me most is that only two serious public-key cryptosystems have been proposed," says Merkle. "One of them has been broken; the other has a complexity that appears to depend on the complexity of factoring, which is still an open question at this time. I think it's surprising that no other fundamentally new techniques have popped up."

"Apparently, it's very difficult to come up with a new scheme," says Shamir. "I think everyone in the field of cryptography has been looking for a new variant, especially when knapsacks seem to be going down the drain. People are quite worried about being left with just one cryptosystem, RSA, and they are frantically looking for new bases for systems."

Even in the case of RSA, some people have their doubts. Says mathematician Ronald L. Graham of AT&T Bell Laboratories, "There is a general feeling in the air, although it's not solid, that factoring may not be as hard as people thought." Adds Merkle, "I think it's the uncertainty that fascinates people and draws them to the problem."

"You can never prove that something is secure," says Brickell. "All you can say is that a lot of people have looked at this for several years, and nobody's figured out a way to attack it."

"The most intriguing question is whether you can develop proof techniques that will show the security of cryptosystems," says Shamir. "If you could do this, it would be the biggest breakthrough in cryptography because at last you would be able to show that concrete cryptosystems just will not be broken in the future unless there is a certain amount of time."

Current mathematical techniques are good enough to put a fence around a problem to show where security lies, says Shamir. They can show that the only way in is through a particular gate. "But how strong is the lock on that gate?" he asks. "We still do not have good techniques for answering that remaining question." □