Secret Bits

How Codes Became Unbreakable

Encryption in the Hands of Terrorists, and Everyone Else

September 13, 2001. Fires were still smoldering in the wreckage of the World Trade Center when Judd Gregg of New Hampshire rose to tell the Senate what had to happen. He recalled the warnings issued by the FBI years before the country had been attacked: the FBI's most serious problem was "the encryption capability of the people who have an intention to hurt America." "It used to be," the senator went on, "that we had the capability to break most codes because of our sophistication." No more. "The technology has outstripped the code breakers," he warned. Even civil libertarian cryptographer Phil Zimmermann, whose encryption software appeared on the Internet in 1991 for use by human rights workers world-wide, agreed that the terrorists were probably encoding their messages. "I just assumed," he said, "somebody planning something so diabolical would want to hide their activities using encryption."

Encryption is the art of encoding messages so they can't be understood by eavesdroppers or adversaries into whose hands the messages might fall. De-scrambling an encrypted message requires knowing the sequence of symbols—the "key"—that was used to encrypt it. An encrypted message may be visible to the world, but without the key, it may as well be hidden in a locked box. Without the key—exactly the right key—the contents of the box, or the message, remains secret.

What was needed, Senator Gregg asserted, was "the cooperation of the community that is building the software, producing the software, and building the equipment that creates the encoding technology"—cooperation, that is, enforced by legislation. The makers of encryption software would have to enable the government to bypass the locks and retrieve the decrypted messages. And what about encryption programs written abroad, which could be shared around the world in the blink of an eye, as Zimmermann's had been? The U.S. should use "the market of the United States as leverage" in getting foreign manufacturers to follow U.S. requirements for "back doors" that could be used by the U.S. government.

By September 27, Gregg's legislation was beginning to take shape. The keys used to encrypt messages would be held in escrow by the government under tight security. There would be a "quasi-judicial entity," appointed by the Supreme Court, which would decide when law enforcement had made its case for release of the keys. Civil libertarians squawked, and doubts were raised as to whether the key escrow idea could actually work. No matter, opined the Senator in late September. "Nothing's ever perfect. If you don't try, you're never going to accomplish it. If you do try, you've at least got some opportunity for accomplishing it."

Abruptly, three weeks later, Senator Gregg dropped his legislative plan. "We are not working on an encryption bill and have no intention to," said the Senator's spokesman on October 17.

On October 24, 2001, Congress passed the USA PATRIOT Act, which gave the FBI sweeping new powers to combat terrorism. But the PATRIOT Act does not mention encryption. U.S. authorities have made no serious attempt to legislate control over cryptographic software since Gregg's proposal.

Why Not Regulate Encryption?

Throughout the 1990s, the FBI had made control of encryption its top legislative priority. Senator Gregg's proposal was a milder form of a bill, drafted by the FBI and reported out favorably by the House Select Committee on Intelligence in 1997, which would have mandated a five-year prison sentence for selling encryption products unless they enabled immediate decryption by authorized officials.

How could regulatory measures that law enforcement deemed critical in 1997 for fighting terrorism drop off the legislative agenda four years later, in the aftermath of the worst terrorist attack ever suffered by the United States of America?

No technological breakthrough in cryptography in the fall of 2001 had legislative significance. There also weren't any relevant diplomatic breakthroughs.

No other circumstances conspired to make the use of encryption by terrorists and criminals an unimportant problem. It was just that something else about encryption had become accepted as more important: the explosion of commercial transactions over the Internet. Congress suddenly realized that it had to allow banks and their customers to use encryption tools, as well as airlines and their customers, and eBay and Amazon and their customers. Anyone using the Internet for commerce needed the protection that encryption provided. Very suddenly, there were millions of such people, so many that the entire U.S. and world economy depended on public confidence in the security of electronic transactions.

The tension between enabling secure conduct of electronic commerce and preventing secret communication among outlaws had been in the air for a decade. Senator Gregg was but the last of the voices calling for restrictions on encryption. The National Research Council had issued a report of nearly 700 pages in 1996 that weighed the alternatives. The report concluded that on balance, efforts to control encryption would be ineffective, and that their costs would exceed any imaginable benefit. The intelligence and defense establishment was not persuaded. FBI Director Louis Freeh testified before Congress in 1997 that "Law enforcement is in unanimous agreement that the widespread use of robust non-key recovery [i.e., non-escrowed] encryption ultimately will devastate our ability to fight crime and prevent terrorism."

Yet only four years later, even in the face of the September 11th attack, the needs of commerce admitted no alternative to widespread dissemination of encryption software to every business in the country, as well as to every home computer from which a commercial transaction might take place. In 1997, average citizens, including elected officials, might never have bought anything online. Congress members' families might not have been regular computer users. By 2001, all that had changed—the digital explosion was happening. Computers had become consumer appliances, Internet connections were common in American homes—and awareness of electronic fraud had become widespread. Consumers did not want their credit card numbers, birthdates, and Social Security numbers exposed on the Internet.

Why is encryption so important to Internet communications that Congress was willing to risk terrorists using encryption, so that American businesses and consumers could use it too? After all, information security is not a new need. People communicating by postal mail, for example, have reasonable assurances of privacy without any use of encryption.

The answer lies in the Internet's open architecture. Bits move through the Internet not in a continuous stream, but in discrete blocks, called *packets*. A packet consists of about 1500 bytes, no more (see the Appendix). Data packets are not like envelopes sent through postal mail, with an address on the

outside and contents hidden. They are like postcards, with everything exposed for anyone to see. As the packets move through the Internet, they are steered on their way by computers called *routers,* which are located at the switching points. Every data packet gets handled at every router: stored, examined, checked, analyzed, and sent on its way. Even if all the fibers and wires could be secured, wireless networks would allow bits to be grabbed out of the air without detection.

If you send your credit card number to a store in an ordinary email, you might as well stand in Times Square and shout it at the top of your lungs. By 2001, a lot of credit card numbers were traveling as bits though glass fibers and through the air, and it was impossible to prevent snoopers from looking at them.

The way to make Internet communications secure—to make sure that no one but the intended recipient knows what is in a message—is for the sender to encrypt the information so that only the recipient can decrypt it. If that can be accomplished, then eavesdroppers along the route from sender to receiver can examine the packets all they want. All they will find is an undecipherable scramble of bits.

In a world awakening to Internet commerce, encryption could no longer be thought of as it had been from ancient times until the turn of the third millennium: as armor used by generals and diplomats to protect information critical to national security. Even in the early 1990s, the State Department demanded that an encryption researcher register as an international arms dealer. Now suddenly, encryption was less like a weapon and more like the armored cars used to transport cash on city streets, except that these armored cars were needed by everyone. Encryption was no longer a munition; it was money.

The commoditization of a critical military tool was more than a technology shift. It sparked, and continues to spark, a rethinking of fundamental notions of privacy and of the balance between security and freedom in a democratic society.

"The question," posed MIT's Ron Rivest, one of the world's leading cryptographers, during one of the many debates over encryption policy that occurred during the 1990s, "is whether people should be able to conduct private conversations, immune from government surveillance, even when that surveillance is fully authorized by a Court order." In the post-2001 atmosphere that produced the PATRIOT Act, it's far from certain that Congress would have responded to Rivest's question with a resounding "Yes." But by 2001, commercial realities had overtaken the debates.

To fit the needs of electronic commerce, encryption software had to be widely available. It had to work perfectly and quickly, with no chance of

anyone cracking the codes. And there was more: Although encryption had been used for more than four millennia, no method known until the late twentieth century would have worked well enough for Internet commerce. But in 1976, two young mathematicians, operating outside the intelligence community that was the center of cryptography research, published a paper that made a reality out of a seemingly absurd scenario: Two parties work out a secret key that enables them to exchange messages securely—even if they have never met and all their messages to each other are in the open, for anyone to hear. With the invention of *public-key cryptography*, it became possible for every man, woman, and child to transmit credit card numbers to Amazon more securely than any general had been able to communicate military orders fifty years earlier, orders on which the fate of nations depended.

Historical Cryptography

Cryptography—"secret writing"—has been around almost as long as writing itself. Ciphers have been found in Egyptian hieroglyphics from as early as 2000 B.C. A *cipher* is a method for transforming a message into an obscured form, together with a way of undoing the transformation to recover the message. Suetonius, the biographer of the Caesars, describes Julius Caesar's use of a cipher in his letters to the orator Cicero, with whom he was planning and plotting in the dying days of the Roman Republic: "... if he [Caesar] had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others." In other words, Caesar used a letter-by-letter translation to encrypt his messages:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC
```

To encrypt a message with Caesar's method, replace each letter in the top row by the corresponding letter in the bottom row. For example, the opening of Caesar's Commentaries "Gallia est omnis divisa in partes tres" would be encrypted as:

Plaintext: `GALLIA EST OMNIS DIVISA IN PARTES TRES`

Ciphertext: `JDOOLD HVW RPQLV GLYLVD LQ SDUWHV WUHV`

The original message is called the *plaintext* and the encoded message is called the *ciphertext*. Messages are decrypted by doing the reverse substitutions.

This method is called the *Caesar shift* or the *Caesar cipher*. The encryption/decryption rule is easy to remember: "Shift the alphabet three places." Of course, the same idea would work if the alphabet were shifted more than three places, or fewer. The Caesar cipher is really a family of ciphers, with 25 possible variations, one for each different amount of shifting.

Caesar ciphers are very simple, and an enemy who knew that Caesar was simply shifting the plaintext could easily try all the 25 possible shifts of the alphabet to decrypt the message. But Caesar's method is a representative of a larger class of ciphers, called *substitution ciphers*, in which one symbol is substituted for another according to a uniform rule (the same letter is always translated the same way).

There are a great many more substitution ciphers than just shifts. For example, we could scramble the letters according to the rule

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

XAPZRDWIBMQEOFTYCGSHULJVKN
```

so that A becomes X, B becomes A, C becomes P, and so on. There is a similar substitution for every way of reordering the letters of the alphabet. The number of different reorderings is

$$26 \times 25 \times 24 \times \cdots \times 3 \times 2$$

which is about 4×10^{26} different methods—ten thousand times the number of stars in the universe! It would be impossible to try them all. General substitution ciphers must be secure—or so it might seem.

Breaking Substitution Ciphers

In about 1392, an English author—once thought to be the great English poet Geoffrey Chaucer, although that is now disputed—wrote a manual for use of an astronomical instrument. Parts of this manual, which was entitled *The Equatorie of the Planetis*, were written in a substitution cipher (see Figure 5.1). This puzzle is not as hard as it looks, even though there is very little ciphertext with which to work. We know it is written in English—Middle English, actually—but let's see how far we can get thinking of it as encrypted English.
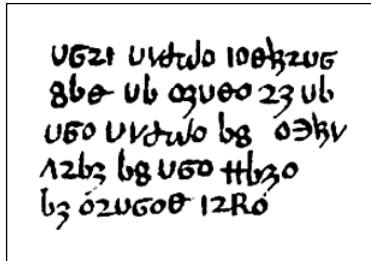
Folio 30v of Peterson MS 75.1, *The Equatorie of Planetis*, a 14th century manuscript held at University of Cambridge.

FIGURE 5.1   Ciphertext in *The Equatorie of Planetis* (1392).

Although this looks like gibberish, it contains some patterns that may be clues. For example, certain symbols occur more frequently than others. There are twelve ●s and ten ∪s, and no other symbol occurs as frequently as these. In ordinary English texts, the two most frequently occurring letters are E and T, so a fair guess is that these two symbols correspond to these two letters. Figure 5.2 shows what happens if we assume that ● = E and ∪ = T. The pattern ∪ᏧᎧ appears twice and apparently represents a three-letter word beginning with T and ending with E. It could be TIE or TOE, but THE seems more likely, so a reasonable assumption is that Ꮐ = H. If that is true, what is the four-letter word at the beginning of the text, which begins with TH? Not THAT, because it ends with a new symbol, nor THEN, because the third letter is also new. Perhaps THIS. And there is a two-letter word beginning with T that appears twice in the second line—that must be TO. Filling in the equivalencies for H, I, S, and O yields Figure 5.3.
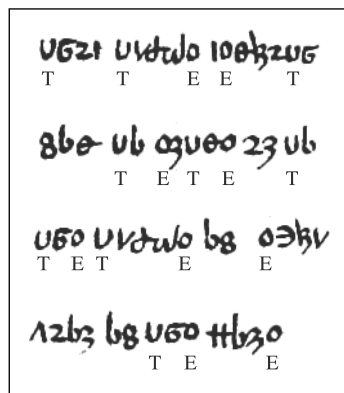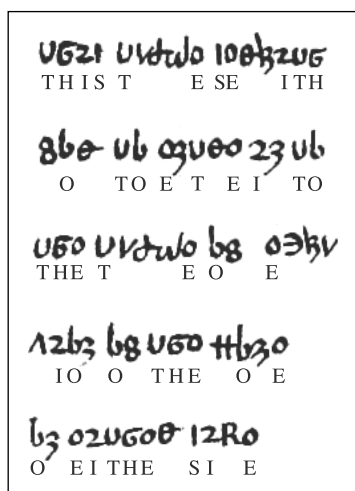

FIGURE 5.2   *Equatorie* ciphertext, with the two most common symbols assumed to stand for E and T.

FIGURE **5.3** *Equatorie* ciphertext, with more conjectural decodings.

At this point, the guessing gets easier—probably the last two words are EITHER SIDE—and the last few symbols can be inferred with a knowledge of Middle English and some idea of what the text is about. The complete plaintext is: *This table servith for to entre in to the table of equacion of the mone on either side* (see Figure 5.4).
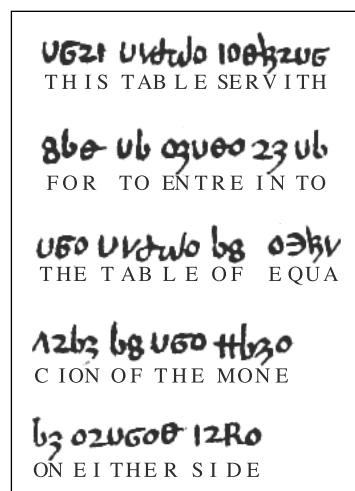
FIGURE **5.4** *Equatorie* ciphertext, fully decoded.

The technique used to crack the code is *frequency analysis*: If the cipher is a simple substitution of symbols for letters, then crucial information about which symbols represent which letters can be gathered from how often the various symbols appear in the ciphertext. This idea was first described by the Arabic philosopher and mathematician Al-Kindi, who lived in Baghdad in the ninth century.

By the Renaissance, this kind of informed guesswork had been reduced to a fine art that was well known to European governments. In a famous example of the insecurity of substitution ciphers, Mary Queen of Scots was beheaded in 1587 due to her misplaced reliance on a substitution cipher to conceal her correspondence with plotters against Queen Elizabeth I. She was not the last to have put too much confidence in an encryption scheme that looked hard to crack, but wasn't. Substitution ciphers were in common use as late as the 1800s, even though they had been insecure for a millennium by that time! Edgar Allen Poe's mystery story *The Gold Bug* (1843) and A. Conan Doyle's Sherlock Holmes mystery *Adventure of the Dancing Men* (1903) both turn on the decryption of substitution ciphers.

Secret Keys and One-Time Pads

In cryptography, every advance in code-breaking yields an innovation in code-making. Seeing how easily the *Equatorie* code was broken, what could we do to make it more secure, or *stronger*, as cryptographers would say? We might use more than one symbol to represent the same plaintext letter. A method named for the sixteenth-century French diplomat Blaise de Vigenère uses multiple Caesar ciphers. For example, we can pick twelve Caesar ciphers and use the first cipher for encrypting the 1st, 13th, and 25th letters of the plaintext; the second cipher for encrypting the 2nd, 14th, and 26th plaintext letters; and so on. Figure 5.5 shows such a Vigenère cipher. A plaintext message beginning SECURE... would be encrypted to produce the ciphertext *llqgrw*..., as indicated by the boxed characters in the figure—S is encrypted using the first row, E is encrypted using the second row, and so on. After we use the bottom row of the table, we start again at the top row, and repeat the process over and over.

We can use the cipher of Figure 5.5 without having to send our correspondent the entire table. Scanning down the first column spells out *thomasbbryan*, which is the key for the message. To communicate using Vigenère encryption, the correspondents must first agree on a key. They then use the key to construct a substitution table for encrypting and decrypting messages.

When SECURE was encrypted as *llqgrw*, the two occurrences of E at the second and sixth positions in the plaintext were represented by different

ciphertext letters, and the two occurrences of the ciphertext letter *l* represented different plaintext letters. This illustrates how the Vigenère cipher confounds simple frequency analysis, which was the main tool of cryptanalysts at the time. Although the idea may seem simple, the discovery of the Vigenère cipher is regarded as a fundamental advance in cryptography, and the method was considered to be unbreakable for hundreds of years.

Harvard University Archives.

FIGURE **5.5** A Vigenère cipher. The key, *thomasbbryan*, runs down the second column. Each row represents a Caesar cipher in which the shift amount is determined by a letter of the key. (Thomas B. Bryan was an attorney who used this code for communicating with a client, Gordon McKay, in 1894.)

CRYPTOGRAPHY AND HISTORY

Cryptography (code-making) and cryptanalysis (code-breaking) have been at the heart of many momentous events in human history. The intertwined stories of diplomacy, war, and coding technology are told beautifully in two books: *The Code-Breakers*, revised edition, by David Kahn (Scribner's, 1996) and *The Code Book* by Simon Singh (Anchor paperback, 2000).

Cryptographers use stock figures for describing encryption scenarios: Alice wants to send a message to Bob, and Eve is an adversary who may be eavesdropping.

Suppose Alice wants to send Bob a message (see Figure 5.6). The lock-and-key metaphor goes this way: Alice puts the message in a box and locks the box, using a key that only she and Bob possess. (Imagine that the lock on Alice's box is the kind that needs the key to lock it as well as to open it.) If Eve intercepts the

box in transit, she has no way to figure out what key to use to open it. When Bob receives the box, he uses his copy of the key to open it. As long as the key is kept secret, it doesn't matter that others can see that there is a box with something in it, and even what kind of lock is on the box. In the same way, even if an encrypted message comes with an announcement that it is encrypted using a Vigenère cipher, it will not be easy to decrypt, except by someone who has the key.
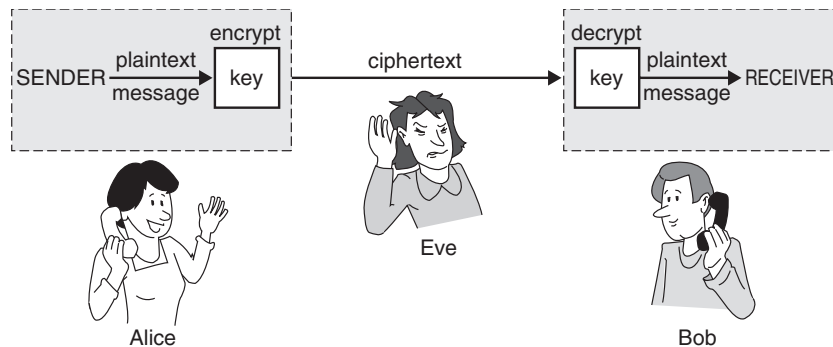

FIGURE **5.6** Standard cryptographic scenario. Alice wants to send a message to Bob. She encrypts it using a secret key. Bob decrypts it using his copy of the key. Eve is an eavesdropper. She intercepts the coded message in transit, and tries to decrypt it.

Or at least that's the idea. The Vigenère cipher was actually broken in the mid 1800s by the English mathematician Charles Babbage, who is now recognized as a founding figure in the field of computing. Babbage recognized that if someone could guess or otherwise deduce the length of the key, and hence the length of the cycle on which the Vigenère cipher was repeated, the problem was reduced to breaking several simple substitutions. He then used a brilliant extension of frequency analysis to discover the length of the key. Babbage never published his technique, perhaps at the request of British Intelligence. A Prussian Army officer, William Kasiski, independently figured out how to break the Vigenère code and published the method in 1863. The Vigenère cipher has been insecure ever since.

The sure way to beat this attack is to use a key that is as long as the plaintext, so that there are no repetitions. If we wanted to encrypt a message of length 100, we might use 100 Caesar ciphers in an arrangement like that of Figure 5.5, extended to 100 rows. Every table row would be used only once. A code like this is known as a *Vernam cipher*, after its World War I-era inventor, AT&T telegraph engineer Gilbert Vernam, and is more commonly referred to as a *one-time pad*.

The term "one-time pad" is based on a particular physical implementation of the cipher. Let's again imagine that Alice wants to get a message to Bob. Alice and Bob have identical pads of paper. Each page of the pad has a key written on it. Alice uses the top page to encrypt a message. When Bob receives it, he uses the top page of his pad to decrypt the message. Both Alice and Bob tear off and destroy the top page of the pad when they have used it. It is essential that the pages not be re-used, as doing so could create patterns like those exploited in cracking the Vigenère cipher.

One-time pads were used during the Second World War and the Cold War in the form of booklets filled with digits (see Figure 5.7). Governments still use one-time pads today for sensitive communications, with large amounts of keying material carefully generated and distributed on CDs or DVDs.

National Security Agency.

FIGURE **5.7**   German one-time pad used for communication between Berlin and Saigon during the 1940s. Encrypted messages identified the page to be used in decryption. The cover warns, "Sheets of this encryption book that seem to be unused could contain codes for messages that are still on their way. They should be kept safe for the longest time a message might need for delivery."

A one-time pad, if used correctly, cannot be broken by cryptanalysis. There are simply no patterns to be found in the ciphertext. There is a deep relation between information theory and cryptography, which Shannon explored in 1949. (In fact, it was probably his wartime research on this sensitive subject that gave birth to his brilliant discoveries about communication in general.) Shannon proved mathematically what is obvious intuitively: The one-time

pad is, in principle, as good as it gets in cryptography. It is absolutely unbreakable—in theory.

But as Yogi Berra said, "In theory, there is no difference between theory and practice. In practice, there is." Good one-time pads are hard to produce. If the pad contains repetitions or other patterns, Shannon's proof that one-time pads are uncrackable no longer holds. More seriously, transmitting a pad between the parties without loss or interception is likely to be just as difficult as communicating the plaintext of the message itself without detection. Typically, the parties would share a pad ahead of time and hope to conceal it in their travels. Big pads are harder to conceal than small pads, however, so the temptation arises to re-use pages—the kiss of death for security.

The Soviet KGB fell victim to exactly this temptation, which led to the partial or complete decryption of over 3000 diplomatic and espionage messages by U.S. and British intelligence during the years 1942–1946. The National Security Agency's VENONA project, publicly revealed only in 1995, was responsible for exposing major KGB agents such as Klaus Fuchs and Kim Philby. The Soviet messages were doubly encrypted, using a one-time pad on top of other techniques; this made the code-breaking project enormously difficult. It was successful only because, as World War II wore on and material conditions deteriorated, the Soviets re-used the pads.

Because one-time pads are impractical, almost all encryption uses relatively short keys. Some methods are more secure than others, however. Computer programs that break Vigenère encryption are readily available on the Internet, and no professional would use a Vigenère cipher today. Today's sophisticated ciphers are the distant descendents of the old substitution methods. Rather than substituting message texts letter for letter, computers divide the ASCII-encoded plaintext message into blocks. They then transform the bits in the block according to some method that depends on a key. The key itself is a sequence of bits on which Alice and Bob must agree and keep secret from Eve. Unlike the Vigenère cipher, there are no known shortcuts for breaking these ciphers (or at least none known publicly). The best method to decrypt a ciphertext without knowing the secret key seems to be brute-force exhaustive search, trying all possible keys.

The amount of computation required to break a cipher by exhaustive search grows exponentially in the size of the key. Increasing the key length by one bit doubles the amount of work required to break the cipher, but only slightly increases the work required to encrypt and decrypt. This is what makes these ciphers so useful: Computers may keep getting faster—even at an exponential rate—but the work required to break the cipher can also be made to grow exponentially by picking longer and longer keys.