Chapter 4

Diffuse and Confuse: How Cryptographers Win the End Game

Historian James Burke, creator of the PBS television series *Connections*, has repeatedly shown that great inventions are the result of the efforts of a number of people coming together to form a single powerful, useful tool. The same thing happened as a result of the centuries-long focus by many sharp-edged minds on cryptography. Although substitution and transposition ciphers became more complex, they could be attacked using statistical methods.

Substitution cryptanalysis

The statistical weakness in substitution ciphers is that they don't change the frequency of alphabetic letters. For example, a cryptanalyst might count the number of times each letter appears in ciphertext. Looking at the letter count of ciphertext `CFGPSF GJWF` (see Figure 4-1), a cryptanalyst typically guesses that the most frequent ciphertext letter (`F`) is really a disguised `E`. If that guess is correct, the cryptanalyst is on the road to cracking the ciphertext. But if the `F` is not an `E`, the cryptanalyst may guess it's a `T`. Given a somewhat longer ciphertext message, the cryptanalyst may guess the most frequent two-letter pattern is *TH*; and so forth.

Computers do statistical analysis very quickly.

Eventually the cryptanalyst will discover clues that uncover what's disguised by the substitution cipher. With the help of computers, that eventuality happens much sooner than the cryptographer would like.

CFGPSF GJWF

Letter Counts of Ciphertext

C : 1 P : 1 F : 3 S : 1 G : 2 W : 1 J : 1

Figure 4-1 Counting ciphertext letters.

Diffusion

Diffusion = substitution + transposition

Ideally, ciphertext should look as if it's a random string of letters keystroked by a chimpanzee. The cryptographer wants to eliminate any clues in the ciphertext that help the cryptanalyst to reclaim plaintext. Mathematically speaking, this

means eliminating statistical relationships between the ciphertext and the underlying plaintext.

Combining transposition and substitution *diffuses* (distributes or disperses) the statistical structure of plaintext over the ciphertext. Not surprisingly, this method is referred to as *diffusion*.[1]

With much of science and technology, little of what we think of as "new discovery" is really new; rather, our current understanding is built on the musings of previous generations. Even Sir Isaac Newton gave credit to others. "If I have seen further than you," he wrote, "it is by standing upon the shoulders of giants." Similarly, diffusion—a technique that current computer cryptography depends on to create a method so unbeatable it can be made public without compromising security—had its beginnings in Greece more than 2,000 years ago.

The Polybius Cipher

Polybius (checkerboard) cipher

Polybius (203–120 BC), a citizen of ancient Greece, is credited with inventing an encoding scheme that converts letters to numbers. Figure 4-2 shows an example of a Polybius square—more commonly known as a *checkerboard* cipher—using the English alphabet. The Polybius square substitutes numbers for plaintext letters. The numbers are the ciphertext.

The first digit in the ciphertext letter is found in the letter row, and the second digit is in the letter column. For example, `A` is converted to 11; `B` is converted to 12; `M` is converted to 32. In a 5 x 5 square, two letters must share the same cell; in Figure 4-2 those letters are `I` and `J`, so they are inferred from the

	1	**2**	**3**	**4**	**5**
1	a	b	c	d	e
2	f	g	h	i / j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Figure 4-2 A Polybius square.

1. Diffusion is actually transposition along with an additional function. The function can be a substitution method or something more elaborate.

Knuckles and Ears

Prisoners made good use of the Polybius square by using their knuckles, or some other hard object, and ears. Russian prisoners developed an audible system, called a *knock* cipher, to turn taps and pauses into letters based on the Polybius square. Later, in World War II, a form of the Polybius square called the quadratic code was used to disguise sensitive information in telephone communications about development of the atomic bomb.

context of the encoded message. Other versions of the Polybius square may have different letters share the same cell.

Polybius hoped to use his square to send messages great distances by means of torches and hilltops. The sender holds a torch in each hand, raising the torch in the right hand the number of times to signal the row and the torch in the left hand the number of times to signal the column. Although one account says there is no known instance of his square being used this way, it was used to turn letters into digits and then into sounds, which came to be known as a knock cipher.

A Polybius secret key square

I	F	W	E	H
A	D	M	O	R
T	U	L	V	N
S	B	K	C	G
J	P	Q	X	Y/Z

In Figure 4-2, letters in the Polybius square are laid out in alphabetical order. But a non-alphabetical grid is more difficult to cryptanlayze. For instance, a non-alphabetical grid could be made with an easily remembered secret key phase, known only to H. X. Mel and Doris Baker—"If we had more time, we would have written a shorter book". The first line of the grid would contain the letters `I F W E H` instead of `A B C D E`, the second line would contain the letters `A D M O R` instead of `F G H I J`, and so on. By the third line letters start to repeat; they're skipped and not used again. So the third line would contain the letters `T U L V N`. Note the secret key phrase does not contain all the letters in the alphabet; specifically, it does not include `C`, `G`, `J`, `P`, `Q`, `X`, `Y`, or `Z`. These letters are placed at the end of the grid.

Let's look at Figures 4-2 and 4-3 to see how letter patterns can be diffused using this method. Figure 4-2 shows a Polybius square that is used in Figure 4-3 to encrypt `JESTER` to `24 15 43 44 15 42` by substituting two numbers for each plaintext letter.

J	E	S	T	E	R
24	15	43	44	15	42

Figure 4-3 The Polybius square in Figure 4-2 is used here to encrypt `JESTER`.

A Useful Cipher Never Used

Almost 2,000 years after Polybius came up with his useful square, Pliny Earl Chase, a Harvard-trained child prodigy and professor of natural science and philosophy, proposed the idea of manipulating the numbered ciphertext from Polybius's square. In 1859 Chase wrote a three-page paper for *Mathematical Monthly* in which he described how he split the numbers in the resulting ciphertext (called *fractionating*) and subjected them to other mathematical operations to further disguise them. Cryptographic historian David Kahn reports that although Chase's techniques were better than many methods, no one has ever used them.

Two numbers for one letter

Can you see that the Es are showing through the ciphertext? After intercepting a few messages and seeing all these 15s (Es), a savvy cryptanalyst will identify this statistical pattern very quickly and crack the cipher. A more secure method will hide all those 15s and other number patterns.

Because each plaintext letter is represented by *two* numbers, you can easily scatter Es by combining a Polybius substitution with a transposition method to transpose some of the numbers. Figure 4-4 rearranges `24 15 43 44 15 42` (JESTER) by splitting apart each number; `24` is separated vertically into a `2` and a `4`; `15` is separated into a `1` and a `5`; and so on.

Now read the numbers along the first and second row: `21 44 14 45 34 52`. The 15s (Es) seem to have vanished. Of course, they're still there. But rearranging the number pairs scatters the ciphertext representation of E. The *top halves* of each number are grouped, as are the bottom halves, forming new number combinations.

We have effectively cut each letter in half and shared its parts with the adjacent ciphertext letter. For example, in Figure 4-5 visualize the first E in JESTER being split into two halves. The top part of the E, represented as a 1, is attached to the top part of the J, represented as a 2; and the bottom half of the E (5) is attached to the bottom half of the J (4).

Transposition is a component of diffusion.

Diffusion dissipates or disperses parts of letters throughout the ciphertext. Our simple Polybius square represented E as two numbers: 1 and 5. Because computers represent each letter as seven (or eight) 0's and 1's, diffusion can dissipate the frequency patterns so well that they cannot be used in the cryptanalysis. The JESTER is still there, so to speak, but he has effectively vanished—except to those who share the secret key.

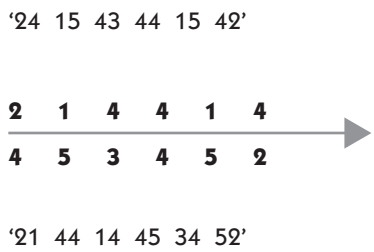

Figure 4-4 Transposing some Polybius square numbers from Figure 4-3.

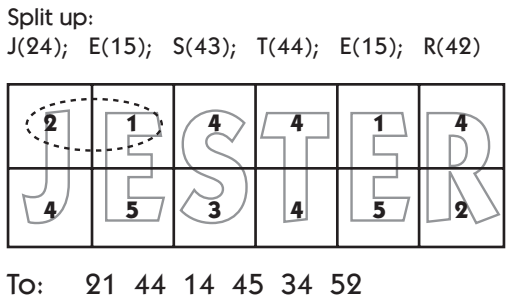

Figure 4-5 In this simple example of diffusion, note how the J and E are mixed together. Diffusion disperses parts of letters throughout the ciphertext.

The Principle of Confusion

Definition: confusion

Diffusion hides the relationship between ciphertext and plaintext.

Confusion hides the relationship between ciphertext and secret key.

The cryptographer assumes that the cryptanalyst has ciphertext and knows the cipher (encryption) method. Diffusion frustrates the cryptanalyst's attempt to use ciphertext patterns to recover plaintext. Because the cryptanalyst doesn't have plaintext, he or she uses ciphertext and the cipher method to try to figure out the encryption key. The principle of *confusion* prevents the cryptanalyst from using ciphertext to figure out the secret encryption key.

In Caesar's cipher, the cryptanalyst can figure out the secret encryption key with very little ciphertext. Even ciphers such as Vigenére's (Chapter 2) aren't strong enough to stop the cryptanalyst from figuring out the secret encryption key.

Confusion usually means that the cryptographer has invented a complex substitution method. Even if the cryptanalyst can figure out some ciphertext patterns, he can't use the cipher method and patterns to figure out the secret key. DES, discussed in Chapter 5, was successful for many years because it uses a complex (nonlinear) substitution method.

Cryptographic Locks and Keys

Definitions: product cipher, round, iterated product ciphers

Ciphers that use confusion and diffusion are called *product ciphers*. Each application of confusion and diffusion is called a *round*. Product ciphers that use many rounds, such as DES, are called *iterated product ciphers*. Historically, effective cryptanalysis tools don't work against correctly designed iterated product ciphers.

A correctly designed iterated product cipher encrypts a message that no one—even the cryptographer who designed the method—can easily decrypt without knowing the secret key.

Definitions: brute force attack, strong method

In other words, with an iterated product cipher, statistical analysis of ciphertext letters is no longer the most practical way to recover the original message. Now the cryptanalyst's best attack is to try each possible secret key, a *brute force* attack. A cryptographic method requiring a brute force attack that also has so many keys that a brute force attack is not feasible is referred to as a *strong* method.

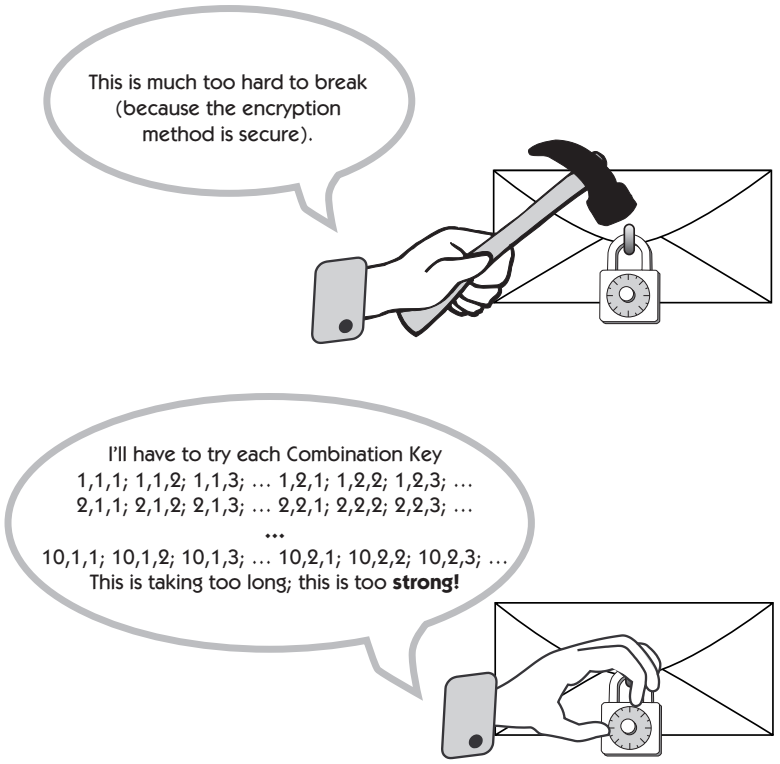

Figure 4-6 A cryptanalyst's most practical attack is to try each possible key.

Modern secure cryptographic methods are strong; the cryptographer can (and arguably should) publish the method for everyone to see and attack (see Figure 4-6). For example, the National Institute of Standards and Technology (NIST)—the U.S. government agency overseeing the next approved secret key encryption standard—mandated that the encryption method of each candidate be openly published.

Always use a published secret key method.

Practically, this means that Alice uses a published secret key method, which has many potential secret keys. If she keeps her secret key secret, her secrets will stay secret, too. But with the rapid pace of technological change, Alice must make sure that she keeps up with the times and periodically assesses whether the method she chose years ago is still secure today.

Chapter 5 discusses the Data Encryption Standard, a previously strong cryptographic secret key method that was published more than 20 years ago. DES has about 70 quadrillion potential keys and is secure against traditional cryptanalysis. But even though DES is less than 30 years old, it's no longer secure (strong) because its 70 quadrillion potential keys aren't enough to stop today's attacks.

Review

Diffusion is a technique that combines transposition and substitution to disperse the statistical structure of plaintext over the ciphertext. A cryptographer uses diffusing techniques to eliminate all clues in the ciphertext that might help an adversary figure out the plaintext of a message. Whereas diffusion hides the relationship between ciphertext and plaintext, confusion hides the relationship between ciphertext and the secret key.

Secret key cipher methods that use diffusion and confusion are called product ciphers. Correctly implemented product ciphers that have great quantities of potential secret keys are called strong. This means that an adversary's best attack is to try each possible secret key, called a brute force attack. But strong cryptographic methods also have enough possible secret keys that a brute force attack is infeasible.

Strong methods are made more secure by being published because they can be scrutinized and tested by cryptanalysts.