Chapter 3

Transposition Ciphers: Moving Around

Definition: transposition ciphers

So far, all the ciphers we've discussed are substitution ciphers, in which plaintext letters are replaced by ciphertext letters. Changing the *positions* of plaintext letters is another enciphering technique. It's called *transposition*, as in transferring position. Many newspapers have transposition puzzles called "jumbles."

Substitution = replacement
Transposition = relocation

A simple transposition of `FIVE AM` moves each letter one position to the left. `FIVE AM` is encrypted to `IVEA MF`. Although the letters have been moved around, all the ciphertext letters are the same as the plaintext letters. There's no replacement or substitution of letters.

To illustrate this ciphering technique, let's look at a more complex transposition: the simple love note `LAST NITE WAS HEAVEN PLEASE MARRY ME`.[1] The table in Figure 3-1 encrypts

L A S T N I T E W A S H E A V E N P L E A S E M A R R Y M E
to
L T E L A A E A E R S W V A R T A E S Y N S N E M I H P M E

L	A	S	T	N	I
T	E	W	A	S	H
E	A	V	E	N	P
L	E	A	S	E	M
A	R	R	Y	M	E

Figure 3-1 A transposition table. The letters are read down the columns.

1. Notice the spelling of "nite." Cryptographers often use nonstandard spelling.

Each plaintext letter transfers to a new position.

Figure 3-1 is like a six-column word processor equipped with word wrapping. It's a 5 x 6 grid. The method used to read letters from the grid is the cipher. This particular cipher reads letters down the first column, then letters down the second column, and so on. The ciphered letters are the same as the plaintext letters except that they are positioned to form a new pattern. The intended receiver must know two things: the length and width of the grid and the way letters are read from the grid.

Patterns and Cryptanalysis

Like substitution ciphers, transposition ciphers can be analyzed for patterns. We choose to show some patterns to others; for example, we might show that we are married by wearing a wedding band. If we want to disguise our marital status, however, we might remove the ring. But a telltale white mark on the ring finger exposes a meaningful pattern to an observant eye.

Looking for patterns

The observant cryptanalyst looks for telltale patterns in substitution and transposition ciphers. The cryptanalyst uses persistence and best guesses, looking for any clue to ferret out patterns.

In Chapter 2, we show how a cryptanalyst uses letter frequency patterns. Just as there are known frequencies of single letters (such as *e* and *t*), there are also known frequencies of two-letter combinations (such as *of* and *in*) and three-letter combinations (such as *the* and *and*). Because transposition ciphers only rearrange plaintext letters, you can try rearranging ciphertext that produces combinations such as *the* and *and*. Also, if you can make guesses about some

Telltale Patterns

Giovanni Battista Porta, a sixteenth-century Italian cryptologist, was one of the earliest cryptographers to divide ciphers into transposition and substitution. His book on cryptography, *De Furtivis Literarum Notis*, is instructive reading even today.

Unlike many people involved in cryptography during the Renaissance, Porta refused to consider polyalphabetic ciphers (such as the Vigenére cipher) invincible. Instead, he proposed some methods of attack. He also offered techniques to improve message disguise, such as using synonyms in plaintext and deliberately misspelling words to avoid the kind of word repetitions and spelling patterns that are used to recover meaning (a modern example: *pa$$word* for *password*).

Porta wrote that knowing the subject matter of the message can speed decryption because the cryptanalyst can look for key words. To keep his readers attentive, he used risqué plaintext examples in his book.

words that might appear in the message, it provides a gateway into decrypting the entire ciphertext.

For example, our plaintext and ciphertext love note,

L A S T N I T E W A S H E A V E N P L E A S E M A R R Y M E

encrypts to

L T E L A A E A E R S W V A R T A E S Y N S N E M I H P M E

Probe for key words.

This may look like mish-mash, but a small clue could give away the secret. If your beloved has a parent who objects to your romance and has an eye peeled for key words[2] such as *marry* or *elope*, your mish-mash could rapidly become meaningful text.

Searching for MARRY, we see that the ciphertext has two Ms and many As. Not much help here. But wait, there are only two Rs, and only one Y. Gotcha. Let's bold those letters and see what emerges.

L T E L **A** A E A E **R** S W V A **R** T A E S **Y** N S N E M I H P **M** E

Using the pattern on ciphertext

Beginning at the Y and going backward five letters is an R; five more letters back is another R, and five letters before that is an A. Six letters before the A (wrapping around) is an M.

Now let's try the pattern to see whether it reclaims more plaintext. Begin below at the first letter L and then skip five, skip five, skip five, skip five, and so on until you reach the end of ciphertext line. Then skip six and wrap around: L, skip to an A, skip to an S, skip to a T, skip to an N, and so on.

L T E L A **A** E A E R **S** W V A R **T** A E S Y **N** S N E M **I** H P M E

If our suspicious parent is a cryptanalyst, he or she may even try skipping letters first—skip one letter, skip two letters—to look for a pattern before looking for key words such as *elope* or *marry*.

Adding Complexity

The following minutia is interesting but not essential to understanding the rest of this text.

You might wonder why transposition ciphers are used if they're so easy to crack. It's because transposition ciphers can be more difficult to crack if they are

2. A guess about key words is often referred to as a *crib*.

repeatedly used on the same plaintext. Figure 3-2 repeats the transposition cipher in Figure 3-1, and Figure 3-3 uses transposition to encipher the output of Figure 3-2. After two transposition cycles the cryptanalyst has a more difficult job unmasking the disguise and reclaiming the original plaintext.

LAST NITE WAS HEAVEN PLEASE **MARRY** ME

Here's the first transposition:

LTEL**A** AEAE**R** SWVA**R** TAES**Y** NSNEM IHP**M**E

Here's the second transposition:

LEVSM TAA**Y**I EE**R**NH L**R**TSP **A**SANM AWEE

Remember that after the first transposition cycle the last four letters of MARRY (ARRY) were five spaces apart. Two transposition rounds make a better disguise. The original plaintext letter ordering has been reversed; the Y in MARRY has been transposed to a new position before the Rs. Although there's still a pattern, it's more difficult to find. Figure 3-2 and Figure 3-3 show the two transpositions of plaintext.

Computerized secret key cryptographic methods use many transposition cycles. The secret key cryptographic method most used currently, the Data Encryption Standard (DES), applies 16 cycles of transposition (and substitution) to each group of about eight letters (see Chapter 5, "DES Isn't Strong Anymore").

Complex transpositions

Before computers were invented, cryptographers often used manual techniques to add complexity to their transposition methods. For example, Figure 3-4 shows another, more complex way of reading text from a grid. Instead of using a transposition method of reading down each column, a diagonal pattern is used. The plaintext message ABCDEFGHIJKL is transposed to AEBCFIJGDHKL.

LAST NITE WAS HEAVEN
PLEASE MARRY ME

L	A	S	T	N	I
T	E	W	A	S	H
E	A	V	E	N	P
L	E	A	S	E	M
A	R	R	Y	M	E

Figure 3-2 The transposition cipher from Figure 3-1.

LTELA AEAER SWVAR
TAESY NSNEM IHPME

L	T	E	L	A	A
E	A	E	R	S	W
V	A	R	T	A	E
S	Y	N	S	N	E
M	I	H	P	M	E

Figure 3-3 The output of Figure 3-2, enciphered.

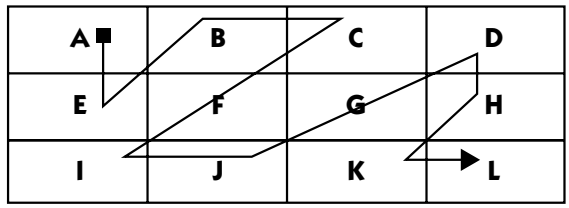


Figure 3-4 An example of diagonal transposition.

Computer Transposition

Transposition ciphers can also be looked at as a set of instructions, one instruction for each letter. Let's quickly review a simple 2 x 3 transposition, shown in Figure 3-5. The message `FIVE AM` is transposed to `FEIAVM` by reading down column 1, then column 2, and then column 3.

Instead of building a transposition table with rows and columns, it's faster to "tell" each letter its new, transposed location. Figure 3-6 enciphers the `FIVE AM` message without building a transposition table. The first letter, `F`, moves to the first position, that is, from location 1 to location 1. The second letter, `I`, moves to the third position, that is, from location 2 to location 3. The third letter, `V`, moves to the fifth position, that is, from location 3 to location 5, and so forth. Computers do this kind of relocation very fast—millions every second.

Computer programs use transposition maps.

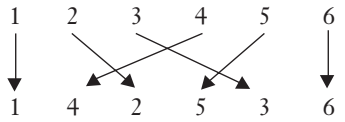
Even a complex transposition cipher, such as the diagonal transposition cipher, has an easy set of instructions, or *transposition map*. Figure 3-7 is a map of the diagonal cipher displayed in Figure 3-4. Row 1 is the beginning position of each letter. Row 2 is the ending position.

F I V E A M

F	I	V
E	A	M

F E I A V M

Figure 3-5 A simple 2 x 3 transposition.



Example:

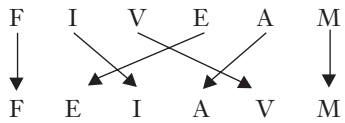


Figure 3-6 This method enciphers `FIVE AM` without the need to build a transposition table.

1	2	3	4	5	6	7	8	9	10	11	12
1	3	4	9	2	5	8	10	6	7	11	12

Figure 3-7 Diagonal transposition map for the cipher in Figure 3-4.

That is, the top row is the initial position of each letter in the message. In our message, in Figure 3-4, `A`, `B`, `C`, and `D` are in the first, second, third, and fourth positions respectively. The bottom row in Figure 3-7 shows their new positions: `A` is moved to the first position, `B` to the third position, `C` to the fourth position, and `D` to the ninth position. Computer programs use this kind of table to rapidly move (encipher) individual bits of the plaintext.

Complex Versus Simple Transposition Ciphers

A transposition cipher that helped the North maintain telegraphic secrecy during the U.S. Civil War was made more complex with the use of key words, code names for important names, and *nulls*, or meaningless letters, symbols, or numbers designed to confuse cryptanalysts. Although the North developed a complex ciphering system, the South was using such a simple cipher that it need not have bothered encrypting messages at all.

In the 1876 U. S. presidential election between Samuel Tilden (D) and Rutherford B. Hayes (R), Democrats communicated the information needed to buy votes using a transposition cipher similar to the one used in the Civil War. But the cipher was simpler, and, when it was broken, the scandal was revealed by the press.

Combining Substitution and Transposition

As cryptographers dug into the mazelike patterns of substitution and transposition cipher methods, they found that using the two types together created much better concealment than either method alone. In fact, using substitution and transposition cipher methods repeatedly on ciphertext does such a good job of disguising patterns that the encoded message is harder to decipher unless the adversary has other kinds of clues, such as those acquired through espionage.

Such a cipher combination nearly defeated the Allied forces in World War I, had it not been for the dogged persistence of Georges Painvin, a French army cryptanalyst whose cutting-edge mind reclaimed meaning from a message

How to Lose 33 Pounds in a Seated Position

French cryptanalyst Georges Painvin lost 33 pounds in his efforts—essential to Allied victory—that cracked ADFGVX, a German cipher used in World War I. Painvin's educated guess was that the cryptographic method used both substitution and transposition. His frequency counts showed that the substitution key changed daily, and he assumed that the same was true of the transposition key. Painvin had to wait for enough messages to be sent on the same day so that he could compare two messages of about the same length that used the same keys. His cipher know-how led him to compare word endings, find repetitions, and make frequency counts to crack the cipher for that day only.

that pinpointed where the Germans planned to attack the French. He broke ADFGVX, one of the toughest field ciphers in cryptographic history.

ADFGVX was so difficult that the Allies never developed a general solution to it during the war. Cracking it nearly always depended on finding, on the same day, two messages of about the same length with similar endings or beginnings. The strength of this cipher lies in its ability to break up plaintext and scatter the text's normal characteristics, which cryptanalysts typically use in reconstructing a transposition cipher.

By itself, simple substitution or simple transposition is not secure, but combining substitution and transposition makes a very secure encryption method.

Modern computer cryptography has made the most of combining transposition and substitution to befuddle even the most brilliant of the brilliant cryptologic minds. How? By doing what computers do well without any mistakes—perform simple operations numerous times. It's just what a computer is good for, and it's also what humans find tedious and error-prone.

As you'll see in Chapter 4, a correctly constructed computer encryption program so completely hides any concealed pattern that cryptanalysts are forced to find new ways to uncover meaning.

Brain Cracking

Sixteenth-century Italian cryptologist Giovanni Battista Porta wrote tellingly of the results of prolonged cryptanalysis, calling it "brain fag" (toil) and advising that such efforts "should not go on uninterrupted."

Seventeenth-century English cryptanalyst John Wallis, while in his seventies, complained about "cracking his brains" spending eight to ten hours a day for seven weeks trying to solve ciphers for England's rulers, William and Mary. Wallis described it as "hard service for one of my years."

Review

Secret key cryptography uses a combination of transposition and substitution to create strong encryption methods. In transposition ciphers, letters or bits are moved from their initial plaintext position to create ciphertext.

A method that uses repeated transpositions makes a cipher more difficult to crack because it obscures the plaintext patterns more effectively. The Data Encryption Standard and Rijndael use multiple combinations of transposition and substitution.

Even before computer cryptography, combinations of transposition and substitution ciphers coupled with frequently changed keys could be very difficult to crack, as illustrated by the ADFGVX cipher used in World War I.