

Let L be the length of the string to be decrypted. Suppose for a moment that L is a multiple of $2(N - 1)$ and let $K = \frac{L}{2(N - 1)}$. One begins by splitting the ciphertext into strings such that the length of the first and last string is K and the length of each intermediate string is $2K$. For the above example with $L = 24$, we have $K = 6$, so we split the ciphertext as follows:

WECRUO ERDSOEERTNE AIVDAC

Write each string on a separate line with spaces after each letter in the first and last line:

W E C R U O
 E R D S O E E R N T N E
 A I V D A C

Then one can read off the plaintext down the first column, diagonally up, down the next column, and so on.

If L is not a multiple of $2(N - 1)$, the determination of how to split up the ciphertext is slightly more complicated than as described above, but the basic approach is the same. Alternatively, for simplicity in decrypting, one can pad the plaintext with extra letters to make its length a multiple of $2(N - 1)$.

If the ciphertext has not been padded, but you either know or are willing to [brute-force](#) the number of rails used, you can decrypt it using the following steps.

As above, let L be the length of the string to be decrypted and let N be the number of rails used during encryption. We will add two variables, x and y , where $x + 1$ = the number of diagonals in the decrypted Rail Fence, and y = the number of empty spaces in the last diagonal.

$$1 = \frac{L + y}{N + ((N - 1) * x)}$$

Next solve for x and y algebraically, where both values are the smallest number possible. This is easily done by incrementing x by 1 until the denominator is larger than L , and then simply solving for y . Consider the example cipher, modified to use 6 rails instead of 3.

W V O
 . E O . E T . N
 . . A C . . R A . . C
 . . . R . . . S E . . N E

```

. . . . . E . I . . . . . D . U . . . . .
. . . . . D . . . . . R . . . . .

```

The resulting cipher text is:

```

WVO EOETN ACRAC RSENE EIDU DR

```

We know that $L = 24$, and if we use $N = 6$ we can solve the equation above.

$$1 = \frac{24 + y}{6 + (5 * x)}$$

$$1 = \frac{18 + y}{5 * x} \text{ Simplify the fraction.}$$

$$1 = \frac{18 + y}{5 * 4} \text{ Solve for } x$$

$$1 = \frac{18 + 2}{20} \text{ Solve for } y$$

We now have $N = 6$, $x = 4$, and $y = 2$. Or, **6 rails**, **5 diagonals (4+1)**, and **2 empty spaces at the end**. By blocking out the empty spaces at the end of the last diagonal, we can simply fill in the Rail Fence line by line using the ciphertext.

```

-           -           -
-           - -         - -
-           -   -       -   -
-   -       -   -       -
-   -       -   -       X
-           -           X

```

```

W           V           O
E           O E         T N
A           C   R       A   C
-           -           -   -       -
-   -       -   -       X
-           -           X

```

Cryptanalysis

The cipher's key is N , the number of rails. If N is known, the ciphertext can be decrypted by using the above algorithm. Values of N equal to or greater than L , the length of the ciphertext, are not usable, since then the ciphertext is the same as the plaintext. Therefore, the number of usable keys is low, allowing the brute-force attack of trying all possible keys. As a result, the rail-fence cipher is considered weak.

Zigzag cipher

The term *zigzag cipher* may refer to the rail fence cipher as described above. However, it may also refer to a different type of cipher described by [Fletcher Pratt](#) in *Secret and Urgent*. It is "written by ruling a sheet of paper in vertical columns, with a letter at the head of each column. A dot is made for each letter of the message in the proper column, reading from top to bottom of the sheet. The letters at the head of the columns are then cut off, the ruling erased and the message of dots sent along to the recipient, who, knowing the width of the columns and the arrangement of the letters at the top, reconstitutes the diagram and reads what it has to say."^[1]

See also

- [Scytale](#)

References

1. Pratt, Fletcher (1939). *Secret and Urgent: The story of codes and ciphers*. [Aegean Park Press](#). pp. 143–144. ISBN 0-89412-261-4.
- [Helen Fouché Gaines](#), *Cryptanalysis, a study of ciphers and their solution*, Dover, 1956, ISBN 0-486-20097-3

External links

- [American Cryptogram Association \(https://web.archive.org/web/20120105152732/http://cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf#RAILFE\)](https://web.archive.org/web/20120105152732/http://cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf#RAILFE)
- [Black Chamber page for encrypting and decrypting the Rail Fence cipher \(https://web.archive.org/web/20110518125721/http://www.simonsingh.net/The_Black_Chamber/railfence.html\)](https://web.archive.org/web/20110518125721/http://www.simonsingh.net/The_Black_Chamber/railfence.html)