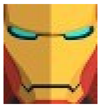
(/cs/) (https://www.baeldung.com/cs/)

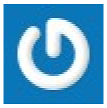
(/bael-search)

Cryptography: Rail Fence Cipher Technique

Last updated: March 18, 2024



Written by: Piyush Adhikari
(https://www.baeldung.com/cs/author/piyushadhikari)



Reviewed by: Korbin Brown
(https://www.baeldung.com/cs/editor/korbinbrown)

Security (https://www.baeldung.com/cs/category/security)

Cryptography (https://www.baeldung.com/cs/tag/cryptography)

1. Overview

(/cs/) (https://www.baeldung.com/cs/)

(/bael-search)

Since the importance of privacy and security has grown, several cryptographic methods and techniques have been developed to protect our sensitive data. As a result, cryptography (/cs/introduction-to-cryptography) did not arise immediately. Rather, it evolved through time, from classical cryptography (/cs/cryptographic-algorithm-complexity#1-classical-cryptography) to modern cryptography (/cs/cryptographic-algorithm-complexity#2-modern-cryptography).

In this article, we'll look at the rail fence cipher technique, covering its encryption and decryption processes as well as its limitation.

2. What Is the Rail Fence Cipher Technique?

Before understanding rail fence cipher, let's discuss classical cryptography techniques, namely substitution (https://en.wikipedia.org/wiki/Substitution_cipher) and transposition (https://en.wikipedia.org/wiki/Transposition_cipher). In the substitution technique, the original message's characters are replaced with different characters, numbers, or symbols. The Caesar cipher (/java-caesar-cipher) is an example of the substitution technique. Conversely, the transposition technique involves rearranging the plaintext through permutation.

Rail fence cipher falls into the category of transposition techniques where we change the position of each plaintext letter. The term "Rail-Fence" is attributed to the resemblance of this technique to a cluster of zigzagging rails.

3. How Does Rail Fence Cipher Work?

This section will provide an in-depth explanation of how the rail fence cipher operates, covering both its encryption and decryption procedures.

3.1. Encryption

The rail fence cipher's encryption process requires choosing the number of rails, writing the message diagonally in a zigzag pattern determined by the selected number of rails, and then combining the characters along each rail from left to right to obtain the encrypted message. Below, we'll explain each step with an example.

First, consider "RAILFENCE" as a plain text. Next, let's take the number of rails or fences as three, which can also be referred to as a key. The key will determine the height of the zigzag pattern. Subsequently, we can write the message diagonally in a zigzag pattern from left to right:

R				F				E
	A		L		E		C	
		I				N		

Lastly, we'll combine individual rows to generate the cipher text, which in this case will be "RFEALECIN".

3.2. Decryption

To begin with decryption, we first need to know the number of rows and columns in the cipher text. The number of columns is equal to the length of the cipher text. Then, we have to figure out the number of rows, which serves as the key, that was used for encryption. **After determining the number of rows and columns, we can construct the table and identify suitable positions for letters, as the rail fence cipher encrypts the text diagonally from left to right in a zigzag pattern**:

*				*				*
	*		*		*		*	
		*				*		

The * represent the positions where letters from the ciphertext are placed to form the plaintext. **We begin by filling in letters from the first "rail" (the top row) and move from left to right. Then, we continue this pattern on the next**

rail and so forth, until all the asterisk positions are filled with letters from the ciphertext:

(/cs/) (https://www.baeldung.com/cs/) (/bael-search)

R				F				E
	*		*		*		*	
		*				*		

Let's complete the above table:

R				F				E
	A		L		E		C	
		I				N		

At last, **we can combine the characters from top to bottom and left to right to obtain the plain text**, which is "RAILFENCE".

4. Limitation

The rail fence cypher's encryption can be easily broken using frequency analysis (https://mathstats.uncg.edu/sites/pauli/112/HTML/secfrequency.html). The key of the encryption is a number that is less than or equal to the length of the cipher text. As a result, it is extremely susceptible to brute-force attacks.

5. Conclusion

In a nutshell, the rail fence technique isn't the best choice for keeping our secrets safe today. Its limitations make it suitable for educational purposes rather than safeguarding sensitive data. **So, in this digital era, we rely on modern encryption techniques such as AES (/java-aes-encryption-decryption#aes-algorithm), RSA (/java-rsa#introduction), and others to protect our information and privacy.**

CATEGORIES

SERIES

ABOUT

(/cs/) (https://www.baeldung.com/cs/)

(/bael-search)