Rail Fence Ciphers

Rail fence ciphers are examples of *transposition ciphers:* The characters in the plaintext message are permuted to create the ciphertext. In the rail fence cipher, the permutation is obtained from a very simple pattern. Other transposition ciphers use other manipulations to permute the characters.

The encryption key for a rail fence cipher is a positive integer.

Suppose we want to encrypt the message “buy your books in August” using a rail fence cipher with encryption key 3. Here is how we would proceed.

i. Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows), forming a zig-zag pattern:

```
b - - - o - - - o - - - i - - - g - - -
- u - y - u - b - o - s - n - u - u - t
- - y - - - r - - - k - - - a - - - s -
```

ii. Then concatenate the non-empty characters from the rows to obtain the ciphertext:

BOOIGUYUBOSNUUTYRKAS

For practice, try encrypting the plaintext “a new semester begins with football and moving vans” using a rail fence cipher with key 5 and see if you obtain the ciphertext

ASNODANETISOTNMVNEMEGWFBAOGSWEREIHALVNSBTLI

The following ciphertext was produced with a rail fence cipher with key 4.

EOCSNYUWLEJYREASONS

See if you can decrypt it.

Because transposition ciphers permute the letters of the plaintext, the plaintext and ciphertext will share the same frequency distribution of characters. Because the frequencies of characters in English (and other languages) are well-known, with messages of sufficient length a transposition cipher can be identified with reasonable confidence using frequency analysis.

If a rail fence cipher is suspected, it is feasible to test it by exhaustive search: In order to avoid undesirable results, the choice of key for a rail fence cipher is quite restricted. Of course, if one were to choose 1 as the key, the plaintext and ciphertext would coincide. The reader should consider the following questions about other possible key choices: What happens if the key is roughly the same as (or larger than) the number of characters in the plaintext? What does this tell you about the number of viable keys for a given message?

The rail fence cipher is a very old encryption scheme, pre-dating the Middle Ages. It was used as a field cipher by both sides in the US Civil War.