National Mathematics Day Activity

Title of activity	Rail-fence cipher
Author(s)	The Australian Association of Mathematics Teachers (AAMT) Inc.
Copyright owner	The Australian Association of Mathematics Teachers (AAMT) Inc.
Year of publication	2012

Each cipher and code activity has a suggested level: lower primary, upper primary or junior secondary. However, many of the activities can be enjoyed by students (and teachers!) of all ages.

For more information about this resource, please contact:

The Australian Association of Mathematics Teachers Inc.
ADDRESS GPO Box 1729, Adelaide SA 5001
PHONE +61 8 8363 0288
FAX +61 8 8362 9288
EMAIL office@aamt.edu.au
INTERNET www.aamt.edu.au

Rail-fence cipher

[jprimary/secondary]

In a rail-fence cipher, the letters of the message (called plaintext) are rearranged, effectively creating an *anagram*. It is called rail-fence because the plaintext is written downwards across successive ‘rails’ of an imaginary ‘fence’. It is a form of transposition cipher.

For example, the plaintext ‘Australian mathematics’ can be written as a three rail cipher:

When read left to right, as normal, along the rails, this gives ATLNTMI, followed by URIMHAC and finally SAAAETS.

Putting the rails together, the created ciphertext would read ATLNTMIURIMHACSAAAETS.

To decipher, you need to know the number of rails and put the letters into that many groups. Be careful, it’s tricky! For the example above, we know that there are three rails and 21 letters. Twenty-one divided by 3 is 7 so the ciphertext must be split into groups of seven. Cut out the groups of 7 letters and arrange one above the other, keeping them in the correct order. Then read down the rails.

- Can you solve this three-rail cipher?

ANTSTILMHOUNAAINRG

(Clue: 2012 is the centenary celebration of the life and scientific impact of this very famous code breaker.)

- Can you write your own three-rail message? (Hint: to make it easier make sure that the number of letters is a multiple of three.)
- A type of rail-fence cipher is called the *zig-zag cipher*. Can you work out how a zig-zag cipher might be constructed? Investigate and see if you are correct.
- What happens if the number of letters is not a multiple of the number of rails?
- Can you write a four-rail message?