National Mathematics Day Activity

Title of activity	Caesar shift 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

Caesar shift cipher

[primary/secondary]

The Caesar shift cipher is said to have been used by Julius Caesar to send coded messages to his generals during his military campaigns.

Caesar simply replaced each letter in a message with the letter three places to the right in the alphabet, looping back around to ‘a’ when he got to ‘x’. For example:

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p
Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	q	r	s	t	u	v	w	x	y	z	a	b	c

The Caesar shift cipher is one of the simplest cipher techniques but it would have been reasonably secure 2000 years ago. Many of Caesar’s enemies would have been illiterate or have assumed that the message was written in a foreign language.

Using the Caesar shift cipher, the message The Roman Empire
would read in ciphertext wkhurpdqhpsluh

- What does this message say?

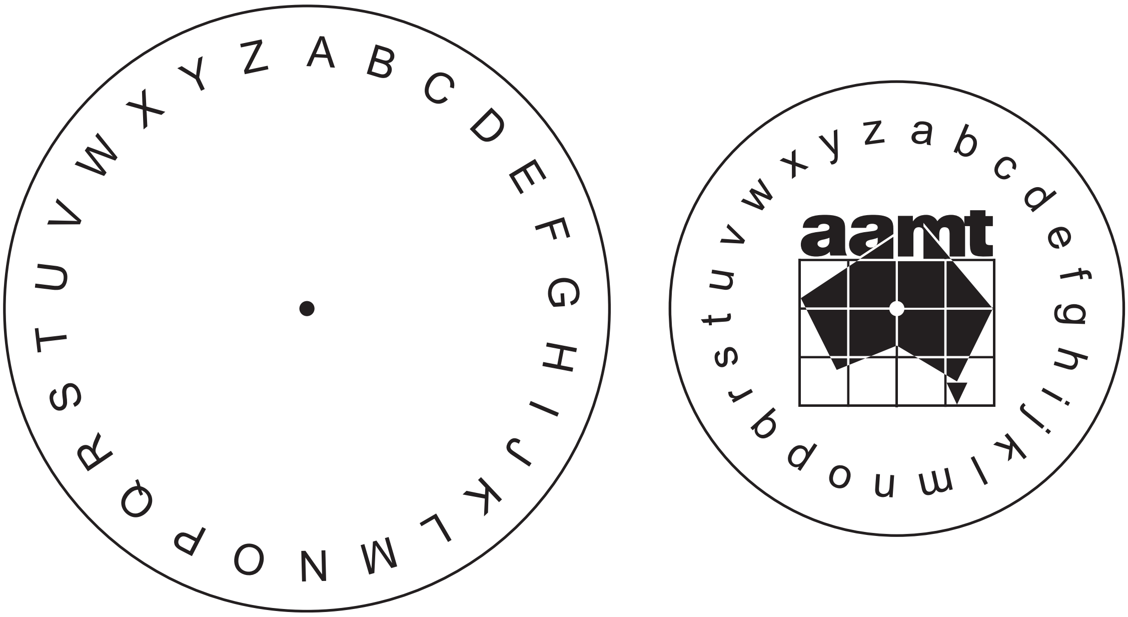
furvvwkhuxelfrqulyhu

- How would this word look if it were written using the Caesar shift?

Cleopatra

- Can you write your own message using the Caesar shift?

- How would your message look if you used a different shift number? You can use a Caesar wheel instead of drawing a table.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z
aamt

Cut out the two circles. Place the smaller over the larger and secure with a split-pin (or similar). Now you can quickly create ciphers using different shift numbers.