Cryptography Worksheet — The Atbash Cipher

Gsv Zgyzhs Xrksvi

The Atbash Cipher is a very old **Substitution Cipher** that was originally developed for use with the Hebrew alphabet. In fact, in the Book of Jeremiah there are several words that have been enciphered using the Atbash Cipher.

It is generally considered one of the easiest ciphers to use as it follows a very simple substitution method. The first letter of the alphabet is replaced with the last letter, the second letter is replaced with the second from last, and so on. In Hebrew, *aleph* (the first letter) is substituted with *tav* (the last letter), *beth* (the second letter) is replaced with *shin* (the penultimate letter). We can see from these letters where the cipher gets its name: the first letter is *aleph*, followed by *tav*, then *beth* and finally *shin*.

Write down what each letter in our alphabet would be substituted with under the Atbash Cipher.

These words have been enciphered using the Atbash Cipher. Decode them.

RHLHXVOVH

ZOTVYIZ

Write a encoded message using the Atbash Cipher. Pass it to the person sitting in front of you to decode.

If someone was to intercept your message, how easy would it be for them to decipher the code, and read the message?

Teacher's Notes — The Atbash Cipher

Start with a discussion of why cryptography developed—to protect valuable or damaging information from being discovered by somebody who was not supposed to know it. There are many ways to hide this information, and one of the earliest methods used was called Steganography. This involved physically hiding the information being sent. There are many ways this has been done through history, but some particularly famous examples are listed below.

1) Herodotus (in 440BC) talks of a method used by Demaratus to send a warning to Greece, whereby he engraved the message on the inside of the wooden backing of a wax tablet, and then applied the wax writing surface. To recover the message, the Greeks had to remove the wax.

2) Herodotus also mentions another method used by Histiaeus to instigate a revolt against the Persians. He shaved the hair off of one of his slaves, and then tattooed the message on the slave's head. When his hair had grown back, the message was hidden, and he was sent to the recipient, who shaved the hair back off to recover the message.

3) A more modern technique is the use of invisible inks.

4) A final more sophisticated method is the use of microdots, which are very small photographs (smaller than a full stop) that are stuck to letters or postcards. They are viewed using a microscope.

As useful as steganography is, if the enemy should find the message, then they can read it easily. This is why cryptography developed, to make it harder for anyone who discovered the secret message to work out what it said.

Ask the pupils if they know of any ways to encipher a message. Lead the discussion towards substitution, where each letter is substituted by another letter or symbol.

The Atbash Cipher is one of the oldest substitution ciphers. It was used in the Book of Jeremiah, where *Sheshakh* (25:26 and 51:41) is written for Babel (or Babylon). This is Atbash, with *beth* being replaced by *shin*, then the same substitution again (since in Hebrew vowels are not written), and finally *lamed* (the twelfth letter) is replaced by *kaph* (the twelfth from last letter).

The substitutions for our alphabet are given by the table below.

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

RHLHXVOVH = Isosceles

ZOTVYIZ = Algebra

Due to the fact that each letter is always enciphered in the same way, this is a very insecure cipher, and very easy for someone who intercepts it to break and find the original message. However, this does not seem to have been a problem in the time it was used, and it seems to have served its purpose well.