**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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 subs tu on 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 le er), *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.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |

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

|  |  |  |
| --- | --- | --- |
| **RHLHXVOVH** |  | **ZOTVYIZ** |

*ISOSCELES ALGEBRA*

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

*HLZKYLG RH GSV YVHG*

*If someone was to intercept your message, how easy would it be for them to decipher the code, and read the message?  
It would be extremely easy to decode and read the messages, as easy as 5 lines of python code and a couple milliseconds*