Bellevue University

Atbash and Baconian Ciphers –

What are they?

Timothy Jelinek

CIS313-T301 Cryptography

8/31/2023

I have grown to be curious about the beginnings of the Bible and how it was written in Hebrew. While I was looking at substitution ciphers, I found the Atbash cipher which was originally used for the Hebrew alphabet but can be used for any alphabet. This cipher uses a specific key where the letters of the alphabet are reversed, where all A's would be replaced with Z's all B's would be replaced with Y's, and so on. With this key, the cipher has little to no security and can be broken very easily. The cipher can be broken so easily that someone who doesn't know that a single piece of the text has been enciphered with Atbash, can solve it by just assuming that it is a substitution cipher and brute forcing their way into knowing the key by hill-climbing. I hope that learning this will help me to learn Hebrew.

Another reason I like this cipher is because of how easy it is to encipher text without using any tools for help. Atbash is interesting as it is a cipher that does not need a stated key. Its ease makes it fun to use to encipher texts to friends and play games with hidden messages. I also see it is possible to use Atbash in Python to encipher messages in your code. Encryption can be used in code to hide code, passwords, links, and other sensitive materials. This cipher appeals to me because it is easy to use, however, it is too easy to use where it is not very secure.

One of my favorite foods is bacon, so it is no surprise that this next cipher stuck out to me. The other substitution cipher I am writing about is the Baconian cipher. Baconian cipher is hiding a secret message instead of just using a cipher. The way to use it is by substituting each letter with a sequence of five characters. The sequence involves A's and B's. The letter D is replaced by aaabb, the letter O is replaced by abbab, and other letters follow this pattern. Two pairs of letters have the same

ciphertexts. These two pairs are I, J, and U, V. This is interesting as each letter is substituted by a sequence of letters instead of just one.

There is a way to incorporate the Baconian cipher into your Python code. To use it you use a dictionary data structure. You use just one dictionary to map out the plaintext-ciphertext pairs as key-value pairs. To encrypt a character, you will need to look for the value using the corresponding plaintext character as a key. You will use this method to find the correct five-character set and retrieve them from the dictionary. This cipher is more complex than the Atbash one, making it more useful in code.

The Baconian cipher is a simple substitution cipher that substitutes a five-character code for each character in a plaintext message. There is a fixed dictionary of 26 codes for each letter in the alphabet. This dictionary can handle spaces and uppercase and lowercase letters. This cipher is not very secure. It can be broken with all of the methods used to cryptanalyze substitution ciphers. The thing this cipher is best used for is hiding the truth of a secret message being sent at all.

After learning about these two ciphers, I learned I prefer the Baconian cipher. This cipher can hide the sending of a secret message. It also is slightly harder to figure out than the Atbash cipher because it uses more characters in substitution. These articles have helped me learn what to look for in enciphered messages to decipher them. The Atbash cipher will also be useful when studying secret messages in Hebrew to learn history. The Baconian cipher is very exciting, however, when given the choice, I will always choose bacon!

Sources:

"Atbash Cipher." Practical Cryptography, practicalcryptography.com, http://practicalcryptography.com/ciphers/atbash-cipher-cipher/. Accessed 31 August 2023.

"Baconian Cipher." GeeksforGeeks, https://www.geeksforgeeks.org/baconian-cipher/. Accessed 31 August 2023.