

Machine Learning for Crypto

by William Gasarch

The following scenario is typical of crypto: Alice wants to send Bob a message. Eve might intercept it. Hence Alice and Bob will agree on a way to encrypt and decrypt the message. For example, they may agree on a shift s : Alice will shift the letters by s to send the message (e.g., if $s = 3$ then a goes to d) and Bob will shift the other direction to decrypt.

The shift cipher, and more sophisticated ciphers, are easy to crack *if you know letter frequencies*. What if you don't (e.g., we need to crack Martian ciphers).

This project will look at using Machine Learning to teach a program to crack a cipher without any prior knowledge. We will start with the shift cipher but then go on to affine ciphers, general substitution cipher, matrix ciphers, and perhaps others.