Ciphers

The Art of Cryptography

Robert Downey Jr.

Ciphers have been around a really long time, and have continued to advance in complexity. They refer to messages that are encoded via substitution of certain letters or symbols for other letters - for instance, a cipher that changes “A” to “B” would turn the word “Cat” to “Cbt”, with the idea that only someone who understands the cipher, the intended recipient of the message, would be able to understand the true meaning.

One of the most famous kinds of ciphers was the Caesar cipher, named after Julius Caesar, in which the encoded alphabet was the normal alphabet shifted three spaces to the left - replacing “abcdef” with “xyzabc”. More advanced ciphers would, instead of shifting the alphabet, use an entirely different alphabet to make it even more unrecognizable. A popular idea that emerged was using a specific word to start their alphabet - if that word were “GATE”, then the alphabet would become “GATEFHIJKL…”, where the alphabet would continue as normal hut spilling those letters.

Both of these kinds of ciphers can be solved the same way though, by using a technique called ‘frequency analysis’. Frequency analysis involves finding the most commonly used letters within encrypted text, and substituting the most commonly used letters with them. If the letter “x” were to be repeated several times in encrypted text, that letter is likely to be one such as e, a, s, or t, which can be further deduced by its placement within words.

Because these kinds of ciphers, substitution ciphers, are all solvable through frequency analysis, more sophisticated methods of encryption were developed. The newer method involves several different ciphers that alternate between a set, known as polyalphabetic substitution. These ciphers typically use a code phrase rather than a code word to determine their alphabets, as each of them requires several. The code phrase “I like cats” may have the alphabets “IJKLMN…”, “LIKEFGH…”, and “CATSUVWX…”, switching between these three each letter.

With the advancement in encryption came an advancement in decryption - people learned to solve polyalphabetic ciphers by searching for repeated patterns within the encrypted text, and then determining the common factor between intervals. If an encrypted text contains the word “FTX” many times, in positions 9, 60, 96, and 102, one could make the assertion that the encryption could be using three alphabets. With this knowledge, they can then split the encrypted text into three texts, each with its own alphabet, and use frequency analysis to determine the most likely letter substitutions. These ciphers are still harder to solve than monoalphabetic ciphers, but can be done if enough encrypted text is provided.