Listen

Classical Cryptosystems

Simple substitution ciphers, although easy to implement, are highly vulnerable to cryptographic attack. The security of these algorithms is dependent on knowledge of a key. By the end of the twentieth century, simple substitution ciphers became easy to break based on letter frequency analysis. In letter frequency analysis, one studies how often each letter occurs in the encrypted message. Every language has a relatively consistent frequency of letters; in English, the most frequently occurring letter is E, whereas the least frequently occurring is Z. Thus, the comparison of frequencies determines the key. This led the way for polyalphabetic ciphers. In a polyalphabetic cipher, a different substitution key is used at different parts of the message, rather than a fixed substitution throughout. Although vulnerable to the same attack, polyalphabetic ciphers require a much greater amount of encrypted text to develop the needed letter frequencies. Examples include the Vigenère cipher and various disk ciphers that used mechanical disks with letters.

Some of the earliest, and simplest, encryption algorithms created by humanity provide a foundation for understanding modern cryptology. These include the shift cipher (also called the Caesar cipher) and the substitution cipher. Underlying these ciphers is the concept that, to encrypt a message, one systematically scrambles the letters of a message. To decrypt the same message, one repeats this process in the reverse order. The strength of such an algorithm lies in a potential adversary not knowing the particular process.

The premise of the shift cipher is to agree upon a key, which is a number between 1 and 25. Every letter of the alphabet is then assigned the letter that is n letters further in the alphabet, wrapping around as necessary. For example, if $n = 3$, then A becomes D, B becomes E, and so on. Typically, the letters are arranged into blocks of the same size to deliberately disguise any two-letter words.

Affine ciphers are similar in nature to shift ciphers. Rather than a single number n, the key for an affine cipher is two numbers (n, m). Also, representing a letter as a number i between 0 and 25, the letter is defined by $ni + m$.

Substitution ciphers are generally encrypted using a keyword or key phrase. As a word has more unknowns than two numbers or a single number, substitution ciphers are more complex to analyze.