27 – Encryption

Tuesday, February 5, 2019 9:48 AM

Plaintext is converted to ciphertext through a process called encryption. The ciphertext is created in such a way that without the key, the message is unreadable. This is really to be able to do when trying to transmit or store data securely.

The Caesar cipher

The Caesar cipher is an example of a shift or substitution cipher in which each character is mapped (e.g. via a dictionary) to another pre-determined character.

This cipher can be extended to a polyalphabetic cipher where the text is passed through many alphabets which means more than one alphabet is needed to decrypt the message which adds an additional layer of security.

Frequency analysis

A Caesar cipher is easily cracked by looking at the frequency of each character in the cipher text. Because each character from the plaintext is mapped to exactly one distinct new character, you can compare the frequencies you would expect in a normal piece of English writing with the cipher text and decipher which letter has been mapped to what.

Transposition cipher

With this type of cipher, letters of the plaintext are rearranged (transposed) to new positions. E.g. with a rail fence cipher or a route cipher. These are still all weak encryption methods as a combination of frequency analysis and anagram deciphering can be used to crack them.

Vernam cipher

The Vernam cipher is a one-time pad technique. The key must be as long as the message. The encryption works by XORing the plaintext with the key to encrypt it and then XORing the ciphertext with the same key again to decrypt the text. As the name suggests, the key can only be used once to ensure full mathematical impossibility of cracking the code. The key must also be generated by a truly random method.

This cipher does still have its weaknesses though. For instance, proof of identity and key-exchange is difficult and random key generation is vital to the algorithm.

General points

Encryption algorithms are ranked based on their computational security or computational hardness.

In general, the following methods are used for cracking codes:

- Identifying commonly used techniques
- Reverse engineering (trying to work out how the code was made)
- Dictionary attacks (checking the guesses plaintext against a dictionary)
- Brute force (tries encrypting random data to see if it matches the cipher text)