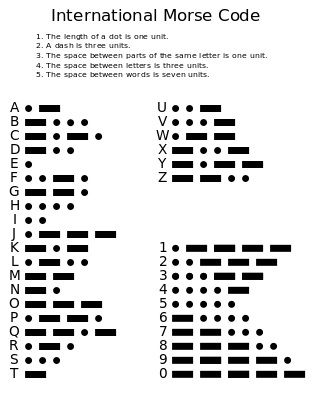
**CIPHER TECHNIQUES**

**Introduction**

Cipher is the technique or the algorithm used to encrypt/decrypt data. It is called a cipher if each and every letter is changed while on the other hand its called code if each word as a whole is converted. The various ciphering/coding techniques are:

**a) Morse Code**

In 1836, the American artist Samuel Morse, with the American physicist Joseph Henry, and Alfred Vail, developed an electrical telegraph system. All the letters of the alphabet, number from 0-9 and some punctuation marks have been replaced by dots, dashes or short and long beeps. For example: A is "▪-". It was not used for concealing message, but transmitting information as a series of clicks, tones or lights. SOS, the most common distress signal, recognized internationally is depicted as three dots, three dashes and three dots.

**Disadvantages:**

* Time Consuming
* You have to learn the morse code
* Easily decipherable

**b) Caesar Shift Cipher**

A cipher was present for each letter of the alphabet, for example ROT1 is one of the ciphers. To decode the message, the person has to be aware which cipher has been used. In G cipher, A becomes G, B becomes H and so on. In Y Cipher, A becomes Y and so on.

**Disadvantages:**

This particular cipher is not very difficult to decipher and hence secret messages do not remain secret for long.

**c) Enigma Code**

The Germans used this sophisticated cipher during the Second World War. It involved using an Enigma machine, which is similar to the type writer. All Germans had the same Enigma machine and the initial wheel configuration of the machine was communicated to all the teams. When a letter was pressed on the machine, a cipher letter lit up on the screen. It got even more difficult when the wheel rotated after certain number of letters, so that the cipher kept on changing. There could be over one hundred trillion possible configurations and hence was difficult to decipher Enigma.

It was broken my Alan Turning ,by using his Bone machine, because one flaw mentioned below!

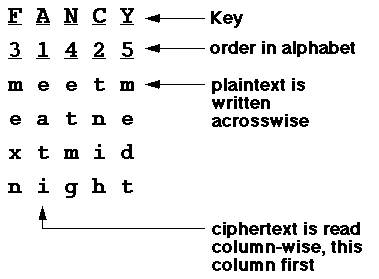
**Flaw:** One letter after being coded never became itself, that is A never was A!

**d) Transposition Cipher**

This particular cipher was used during American Civil War and World War I to communicate sensitive messages. The letters of the alphabet are rearranged based on pre-determined key or rule.

First a keyword is chosen like FANCY. The ordinal values of the letters are written. Over here A is 1, next in order is C which is 2 and so on. The plain text is written in tabular form, as shown and then the cipher text is taken column wise according to how you have numbered the columns.

**Plain Text:** meet me at next midnight



**Cipher Text:** eati tnih mexn etmg medt

**Disadvantage:** The main letters aren’t actually changed so its easily decipherable with current algorithms.

**e) Steganography**

This involves the concealment of a message, image or a file in another message, image or file. The first record of its use is in 1499. Text could be written using invisible ink between visible lines of a text. The benefit of this type is that it does not arouse suspicion like an encrypted message would. There are various ways in which this can be done – physical, digital, social and using puzzles as well. Digital images are used largely for hiding messages as bits. Various modern techniques are available by which steganography can be performed.

**Disadvantages:** Steganography is used for securing data, not concealing it.

By

Nihal Haneef

16CO128