How do you keep a secret: the history of cryptography

History

The paper " How Do You Keep A Secret: the History of Cryptography" is a delightful example of a history essay.

Cryptography has been used for a long time and it has reached the level of encryption now, where the trapdoors are such that it is next to impossible for code breakers to decipher the message without knowing the key.

Secret messages used to either be codes or ciphers. Codes require complete words to be translated and whole notebooks are needed as keys. Ciphers entail having individual letters substituted into other symbols/letters; there are various ways of ciphering, and it is noteworthy that the modern cryptography involves ciphering almost solely.

Earlier, the military used to cipher messages by the skytale method, which involved a leather belt with a code on it and a tapered wooden stick on which the leather belt was wound to decipher it. Julius Caesar used a simple substitution method for his cipher, a technique Emperor Augustus took a liking to as well. However, these ciphers were easy to decode, therefore, new techniques of ciphering were introduced, which included shifting the cipher code regularly, ignoring blanks and shifting letters in a group of a certain number. Moreover, since letters are used in a language in a certain frequency, it is very useful to employ such techniques, as they entail not using the same cipher/code for the same letter. Also, such ciphers have an arithmetic formula as their key which makes it easier to remember for and harder to find on a spy, as against a, say, notebook or a list of ciphers.

Another ciphering technique is the matrix substitution method, whereby a matrix grid is used to cipher letters in groups. In the transposition cipher, a rectangle of a certain dimension is used to write down the message and then only the dimensions of the rectangle are needed to decipher it.

However, the latest technique in the art of ciphering is the trapdoor, whereby it is very easy to track down the code with the key; however, the key is so hard to find that it is next to impossible to crack the cipher without the help of that key. Such encryption is used to encrypt emails, bank accounts details as well as satellite TV broadcasts.