Classical Cryptography Paper-Edgar C. Reinke Summary

Cryptography is a method of secret communication. It can be done in two ways:  
1. Cipher   
a. Transposition- The letters of the message are systematically disarranged   
b .Substitution- We have a fixed key wherein different letters, numbers, symbols used in place of letters in the message  
2.Code- Arbitrary groups of symbols are used in place of whole sentences/phrases.  
  
HISTORICAL EXAMPLES OF CRYPTOGRAPHY  
  
-Many instances have been seen in which steps were taken to avoid detection of unenciphered text(E.g. When Milesian Histiaeus shaved the head of his most trusted slave, and tattooed his message on his scalp. After waiting for his hair to grow back, the slave was sent to his son-in-law, where his head was again shaven so that the message could be seen.)  
  
-Scytale cipher/Plutarch's staff-A scytale is a stick, a piece of wood around which a ribbon (leather) is wrapped and on which a message is written, when the ribbon is unrolled an encrypted message appears (the order of the letters having changed).First recorded use by Spartan generals.  
  
How Cicero, a Roman statesman and philosopher during Julius Caesar's dictatorship might have solved the Scytale cipher: by copying the transcript, cutting it into equal parts, and observing different arrangements by juxtaposition.  
  
Mono-substitution of letters in the message- It provides virtually no security. It can be deciphered by writing the next letter under a row of words in the message. Now do the same with the row of letters we just wrote. Keep continuing this process until plain text is observed.  
  
To add an additional layer of security, choose a keyword, whose letters will represent the first few letters of the English Alphabet. In the given example, the keyword is Libertas.

  
  
To solve such a cipher, we may make use of frequency charts of letters and digraphs (two letters taken together that make a single sound)  
  
To decide whether a cipher is transposed or substituted:  
We can make comparisons between a general frequency table of letters and one of the messages. Thus, the frequencies of the letters may be matched. However, this is not a perfect method, especially for a short message.  
  
In conclusion, cryptography has ancient roots. It can be a fun and stimulating experience. One only needs a pen and paper to get started.