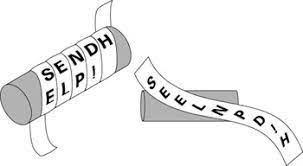
# History of Cryptography

## Techniques of Cryptography

* There are two basic building blocks of all encryption techniques:
  + Substitution
  + Transposition
* Substitution:
  + An encryption technique in which the letters of plaintext are replaced by other letters or by numbers or symbols.
  + If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.
* Transposition
  + An encryption technique that involves performing some sort of permutation on the plaintext letters.

## Classic Cryptography

* Caesar cipher (substitution)
  + involves replacing each letter of the alphabet with the letter standing **3** places further down the alphabet.
  + ****used by Julius Caesar, hence the name
* ROT13 cipher (substitution)
  + similar technique to Caesar cipher, except that letter is shifted **13 places**
  + can be further modified for different amounts of shifts
* Scytale (transposition)
  + a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message.
  + the recipient uses a rod of the same diameter on which the parchment is wrapped to read the message.



* Rail Fence cipher (transposition)
  + plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
  + Example: encode the message ‘meet at the schoolhouse’ with depth 2
    - The message is written as follows (i.e. diagonally)

m1 e3 a5 t e c o l o s

e2 t4 t h s h o h u e

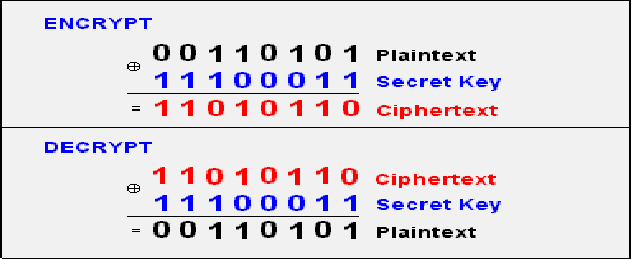
* + - The encoded message is: MEATECOLOSETTHSHOHUE
* Route/Row cipher (transposition)
  + Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
  + The order of columns then becomes the key to the algorithm.

## 1800s Cryptography

* Polyalphabetic ciphers (substitution)
  + uses different monoalphabetic substitutions as one proceeds through the plaintext message.
  + All the techniques have the following features in common:
    - A set of related monoalphabetic substitution rules are used
    - A key determines which particular rule is chosen for a given transformation.
* Vigenere cipher (substitution)
  + Uses the set of related monoalphabetic substitution rules consisting of 26 Caesar ciphers with shifts of 0 through 25.
  + Each cipher is denoted by a key letter (e.g. ‘d’ for shift of 3).
  + Constructing a matrix known as Vigenere tableau helps: each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top.
  + Encryption process: Given a key letter x and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y.
  + To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.
  + e.g. Key = d e c e p t i v e d e c e p t i v e d e c e p t i v e   
    Plain Text = w e a r e d i s c o v e r e d s a v e y o u r s e l f   
    Cipher Text = ZICVTWQNGRZGVTWAVZHCQYGLMGJ
  + Decryption: The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

## One Time Pad Cipher

* Proposed by Frank Miller in 1882
* Mathematically possible to provide “the perfect secrecy” only if
  + The key must be as long as the plain text.
  + The key must be truly random
  + The key must only be used once
  + The key must keep secret
* Nice concept but impractical!
  + requires a very long key which is expensive to produce and expensive to transmit.
  + Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

  
Uses bitwise XOR operation

## During WW2

* Mechanical era: a mechanical device for encrypting messages

  
(a) Rotor machine



(b) Enigma machine

  
(c) Enigma’s inner workings