Ciphers

Ankur Mishra

1/22/2018, 2/6/2017

Contents

1 Columnar Transposition Ciphers

1.1 Simple Columnar Transposition Cipher

General Process: Rearranging letters based on numeric key.

1.1.1 Encoding

To encode, put text in to a matrix, which has c columns, where c = key. Then copy each column from left to right to create your a new encoded message.

1.1.2 Decoding

To decode, first approximate the number of rows (r) by dividing the length of the decoded message by the key. Then write each letter of the encoded message from up to down, till the row length is reached. Keep in mind, if there is a reminder(x) when calculating the number of rows, leave x spaces blank in the last row.

1.1.3 Example

Example:
Text: "REARRANGING LETTERS" | Key: 5
$18/5 = 4R2$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ R & E & A & R & R \\ A & N & G & I & N \\ G & L & E & T & T \\ E & R & S & & \end{bmatrix} \tag{1}$$

Encoded: RAGEENLRAGESRIT RNT

1.2 Keyword Columnar Transposition Cipher

General Process: Rearranging letters based on a keyword and each keyword letter's alphabetical order.

1.2.1 Encoding

To encode, put text in to a matrix, which has c columns, where c = the length of the keyword. Keep each letter of your keyword above each column of the matrix. Then copy each column from based on your keyword's alphabetical order to create your a new encoded message.

1.2.2 Decoding

1.2.3 Example

$$\begin{bmatrix} C & R & Y & P & T & O \\ & & & & & \\ S & L & I & G & H & T \\ L & Y & M & O & R & E \\ C & O & M & P & L & I \\ C & A & T & E & D & \end{bmatrix} \tag{2}$$

2 Playfair Cipher and Railfence Cipher

2.1 Playfair Cipher

2.2 Railfence Cipher

3 ADFGVX Cipher and Vigenere Cipher

3.1 ADFGVX Cipher

3.2 Vigenere Cipher