**Process Description of**

**Decrypting a Permutation Cipher**

Submitted by: Daniel Nedrow

Submitted to: Professor David Wilson

EGR 3350

Date: June 2, 2018

PROCESS DESCRIPTION OF DECRYPTING A PERMUTATION CIPHER

**Introduction**

*Decrypting a permutation cipher* is a decryption process whereby groups of shuffled letters are rearranged back into their original order. For example, the encrypted words “HTE ACT” would be decrypted to “the cat.” The *ciphertext string* is the name for the coded message, and the *plaintext string* is the name for the decoded, readable message. We say *n* is the size of the letter groupings (above, n = 3). The purpose of decrypting a permutation cipher is to uncover the meaning of a coded message. Decrypting a permutation cipher involves the following steps: generating the decryption key, grouping the ciphertext, generating the plaintext, and interpreting the plaintext.

**Discussion**

Assume we are given the encryption key and that n = 8. See Figure 1 for the ciphertext we wish to decode; refer to Table 1 for the encryption key.

***Generating the Decryption Key***

*Generating the decryption key* is a logical process whereby we use a given encryption key to infer the corresponding decryption key. The *encryption key* is a mapping which was used to create the ciphertext. We say *i* is the index of each letter within the ciphertext string. From Table 1, observe that the 1st letter of the ciphertext was the 5th letter of the plaintext, the 2nd letter of the ciphertext was the 7th letter of the plaintext, and so on. Thus, the function *π(i)* tells us from where

EERHLTBEIQNIULSOHRSTTIOENTONSOUD

***Figure 1***

The ciphertext string. Source: Author.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π(i) | 5 | 7 | 4 | 2 | 8 | 1 | 6 | 3 |

***Table 1***

The encryption key. Source: Author.

in the plaintext to get ciphertext letter i. The purpose of generating the decryption key is to begin the decoding process. The method is simple: we look at the indices in the bottom row of the encryption key and map them back to their corresponding indices in the top row. Thus, 1 maps back to 6, 2 maps back to 4, and so on. We say *j* is the index of each letter within the plaintext string, and *π-1(j)* tells us from where in the ciphertext to get plaintext letter j. After reversing the encryption key as described, we generate the decryption key in Table 2. To effectively apply the decryption key, we must next group the ciphertext.

***Grouping the Ciphertext***

*Grouping the ciphertext* is a separation process whereby we divide the entire ciphertext string into groups of n letters. Grouping allows us to apply the decryption key. We were given n = 8 as the group size. We should count the letters of the entire ciphertext string and verify the count is

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| j | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π-1(j) | 6 | 4 | 8 | 3 | 1 | 7 | 2 | 5 |

***Table 2***

The decryption key. Source: Author.

divisible by n. Here, there are 32 letters in the ciphertext, which is indeed divisible by 8. Figure 2 shows the grouping. With our groups in hand, we can now begin generating the plaintext.

EERHLTBE IQNIULSO HRSTTIOE NTONSOUD

***Figure 2***

The ciphertext string in groups of 8 letters. Source: Author.

***Generating the Plaintext***

*Generating the plaintext* is a decoding process whereby the ciphertext letters are arranged back into their original order. The purpose is to retrieve a raw form of the plaintext. Take the first grouping of 8 letters from Figure 2: EERHLTBE. Refer to Table 2 for the decryption key. We see that the 1st letter of the plaintext should come from position 6 in this ciphertext: T. The 2nd letter comes from position 4: H. The 3rd letter comes from position 8, the 4th letter from position 3, the 5th letter from position 1, the 6th letter from position 7, the 7th letter from position 2, and the 8th letter from position 5. For the first group, we get THEREBEL. Using the same process, the next three groups decrypt to LIONISQU ITESHORT ONDONUTS. Since we have our plaintext, we can now interpret it.

***Interpreting the Plaintext***

*Interpreting the plaintext* is an intuitive process of forming words from the plaintext. The purpose is to get the plaintext out of its raw form and into something easily readable. The plaintext was THEREBEL LIONISQU ITESHORT ONDONUTS. It is simply necessary to write this message in its most likely form. We can choose from “The rebel lion is quite short on donuts” and “The rebellion is quite short on donuts.” We choose the second form, and at this point the entire process of decrypting the message is finished.

**Conclusion**

Decrypting a permutation cipher is a decryption process whereby groups of shuffled letters are rearranged back into their original order. We start by using a given encryption function to generate the inverse function, or decryption key. We then group the ciphertext into blocks of n letters. We use the decryption key to decrypt the blocks of letters, generating the plaintext. Finally, we interpret the plaintext as a message in English. Decrypting a permutation cipher is a simple decryption process that is easy to learn.