Permutation Cipher

Math 4175

§2.6.1. Permutation Cipher

All of the criptosystems we have discussed so far involve replacing plaintext characters by different cipher text characters. The idea of a Permutation Cipher (also known as the Transposition Cipher) is to keep the plaintext character unchanged, but to alter their positions by rearranging them using a permutation.

Just like the Substitution Cipher, the Permutation Cipher has also been in use for hundreds of years. In deed, the distinction between these two ciphers was pointed out by Giovanni Porta in 1563.

Recall that we replace the entire plain text in Substitution Cipher by using a permutation. But in the Permutation Cipher, we shuffle (not replace) the plaintext block by block by using a permutation.

§2.6.1. Permutation Cipher

For example, let us say we want to encrypt

`she sells sea shells by the sea shore`

Suppose $m = 6$ and the key is the following permutation π:

i	1	2	3	4	5	6
$\pi(i)$	3	5	1	6	4	2

The first row of the above table lists the values of i, $1 \leq i \leq 6$, and the second row lists the corresponding values of $\pi(i)$.

We first partition the plaintext into groups of six letters:

`shesel     lsseas     hellsb     ythese     ashore`

§2.6.1. Permutation Cipher

Now, rearrange each group of six letters according to the permutation π. We obtain:

EESLSH SALSES LSHBLE HSYEET HRAEOS

So, the ciphertext is:

EESLSHSALSESLSHBLEHSYEETHRAEOS

The cipher text can be decrypted in similar fashion, using the inverse permutation π^{-1}; i.e.,

i	1	2	3	4	5	6
$\pi^{-1}(i)$	3	6	1	5	2	4

Decrypt: ZLPEZU

§2.6.1. Permutation Cipher

Now we are in a position to provide a precise mathematical definition of Permutation Cipher:

Permutation Cipher is a cryptosystem with $\mathcal{P} = \mathcal{C} = \left(\mathbb{Z}_{26}\right)^m$ where m is a positive integer. The key space $\mathcal{K}$ is the set of all permutations on $\{1, 2, \cdots, m\}$. For a key $K \in \mathcal{K}$, we define

$$e_\pi(x_1, \cdots, x_m) = \left(x_{\pi(1)}, \cdots, x_{\pi(m)}\right)$$

and

$$d_\pi(y_1, \cdots, y_m) = \left(y_{\pi^{-1}(1)}, \cdots, y_{\pi^{-1}(m)}\right)$$

where π^{-1} is the inverse permutation of π.

§2.6.1. Permutation Cipher

Now let us describe a special type of Permutation Cipher. Let m and n be positive integers (which divide the number of all (or part of) plaintext characters). Write out the plaintext, by m rows and n columns, in $m \times n$ rectangles. Then form the cipher text by taking the columns of these rectangles.

For example, we would like to encrypt the plaintext **cryptography** by taking $m = 3$ and $n = 4$.

```
cryp
togr
aphy
```

The ciphertext would be CTAROPYGHPRY. The corresponding permutation is

i	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(i)$	1	5	9	2	6	10	3	7	11	4	8	12

§2.6.2. Cryptanalysis of Permutation Cipher

Oscar received the following message which is encrypted by using the above special type of Permutation Cipher. Decrypt it:

```
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
```

It is a long text, and so we first divide them into blocks by finding the length of the block.

Since the cipher text has length 42, the length of each block must be a proper divisor of 42; that is, $2, 3, 6, 7, 14,$ or 21.

Below is the partition of the cipher text in groups of 6 letters:

```
MYAMRA  RUYIQT  ENCTOR  AHROYW  DSOYEO  UARRGD  ERNOGW
```

Hint: Either $m = 2, n = 3$ or $m = 3, n = 2$

§2.6.2. Cryptanalysis of Permutation Cipher

We now show that the Permutation Cipher is a special case of the Hill Cipher. So a cryptanalysis of Hill Cipher can be used for Permutation Cipher.

Given a permutation π on $\{1, 2, \cdots, m\}$, we can define an associated permutation matrix, denoted by $K_\pi = (k_{ij})$ as follows:

$$k_{ij} = \begin{cases} 1 & \text{if } i = \pi(j) \\ 0 & \text{otherwise} \end{cases}$$

Definition: A matrix is called a permutation matrix if every row and column contains exactly one '1', and all other entries are '0'.

§2.6.2. Cryptanalysis of Permutation Cipher

For example, let $m = 6$ and π be given as follows:

i	1	2	3	4	5	6
$\pi(i)$	3	5	1	6	4	2

Then K_π is given by

$$K_\pi = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

§2.6.2. Cryptanalysis of Permutation Cipher

In this case, the inverse matrix is given by

$$K_\pi^{-1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Verify that the above two matrices are inverse to each other.

So cryptanalysis of Permutation Cipher may be done the same way as Hill Cipher.