Classical Cryptography, Part II

Permutation ciphers

In the various kinds of substitution ciphers, the plaintext is encrypted by replacing its characters with other characters. In a permutation cipher, the encryption is done by changing the order of the characters.

A famous ancient example is the *scytale*. It involved taking a ribbon of paper or cloth and wrapping it around a cylindrical tube. You would write your message across the ribbon while it is on the tube and then unwrap the ribbon. The letters of the message after the ribbon is removed will appear to be in a random order, and they will only make sense if the ribbon is again wrapped around a tube of the same thickness.

Rail fence cipher

A simple type of permutation cipher is the *rail fence* cipher. Suppose our message is SECRETMESSAGE. Separate it into the characters at even and odd indices, like below.

S E C R E T M E S S A G E

Then take all the characters at even indices and combine them. Do the same for the characters at odd indices. Put all the evens before the odds, and you get the encrypted message SCEMSAEERTESG, as shown below.

SCEMSAE ERTESG

To decrypt, you can do things in reverse order. A nice visual way to do this is put one half above the other and space out the letters like below. Then read left to right, zigzagging between the rows.

```
S C E M S A E
 E R T E S G
```

Notice that all of the characters of the original message are present in the encrypted message. This is a feature of permutation ciphers. In particular, frequency analysis will show that the letter frequencies match plain English, which is one way people use to recognize permutation ciphers. The rail fence cipher in particular is not at all secure, but it's convenient for demonstrating what permutation ciphers are all about.

Columnar transposition

There are many other types of permutation ciphers. We'll look at just one more: *columnar transposition*. The basic idea is to write the message out in a fixed number of columns, then scramble the columns, and write the message back out again.

Here is an example. Suppose our message is THISISASECRETMESSAGE. Let's use six columns. We write out the message as below.

1	2	3	4	5	6
T	H	I	S	I	S
A	S	E	C	R	E
T	M	E	S	S	A
G	E	Q	R	S	T

Note that the message is too short to fit, so we add some *padding* characters at the end to fill out the last row. Let's say we decide to scramble the columns into the order 5, 2, 4, 6, 3, 1. We then get the following.

5	2	4	6	3	1
I	H	S	S	I	T
R	S	C	E	E	A
S	M	S	A	E	T
S	E	R	T	Q	G

Then write it back out as IHSSITRSCEEASMSAETSERTQG.

Decryption is similar. Take the ciphertext, write it back in columns. Then label the columns with the numbers given in the key. The result would look just like the table above. Then rearrange the columns into numerical order and read the message back out.

Double columnar transposition, where the process is done twice, is a pretty good cipher that was used in World War II and into the 1950s. Combined with a substitution cipher, it is even stronger. Modern ciphers are built on a similar principle of combining substitutions and permutations, just many more of them.

Block ciphers and the Playfair cipher

The last major category of cipher we will talk about are block ciphers. These are a type of substitution cipher where instead of substituting single letters for other single letters, we substitute groups (or blocks) of letters for other groups of letters.

A famous example is the Playfair cipher. It was in use up until World War II. Prior to computers, breaking it usually took enough time that the decrypted text would no longer be useful by the time the cipher was cracked. We'll use an example to describe how it works. For this example, the plaintext is THISISASECRETCHANNEL, and the key is ZOOKEEPER.

Start by writing out the letters of the key in a 5×5 grid. If a letter appears multiple times in the key, only put in the first occurrence. Then fill out the rest of the grid in alphabetical order with the letters that do not appear in the key. Because this grid has 25 spots, there is not enough room for all 26 letters of the alphabet. To deal with this, we will treat I and J as the same letter, using I for both. Here is the grid:

Z	O	K	E	P
R	A	B	C	D
F	G	H	I	L
M	N	Q	S	T
U	V	W	X	Y

Next, go through the plaintext message two letters at a time. If any of those blocks of two letters are ever both the same letter, that will cause a problem with the encryption. To fix this, replace the second letter of the block with an X and move that replaced letter to the start of the next block. For instance, if we have a block NN and the next letter is an E, then the NN block becomes NX and the block after becomes NE. Also, if we get to the end of the message and only have one letter in the final block, add a Q for padding. Shown below is how the message will be broken up. We will explain next how to get the ciphertext.

plaintext	TH	IS	IS	AS	EC	RE	TC	HA	NX	NE	LQ
ciphertext	QL	SX	SX	CN	CI	CZ	SD	GB	SV	SO	HT

For the first plaintext block, TH, draw a box around the T and the H in the table, like below. T should be at one corner and H at another. Each letter gets encrypted to the letter at the *opposite corner in the same row*. So T will be replaced with Q and H will be replaced with L.

Z	O	K	E	P
R	A	B	C	D
F	G	H	I	L
M	N	Q	S	T
U	V	W	X	Y

For the next block, IS, draw a box around those letters, like below. This time they are in the same column, so we

won't be able to do what we did above. When the two letters are in the same column like this, the rule is to replace each letter with the letter directly below it, wrapping around to the top if needed. So here I gets replaced with S and S gets replaced with X.

```
  Z  O  K  E  P
  R  A  B  C  D
- F  G  H  I  L
  M  N  Q  S  T
  U  V  W  X  Y
```

The next block is IS again. It gets replaced with SX again. The fact that the same blocks get encrypted to the same things is a weakness of this cipher. This fact combined with frequency analysis is key to breaking the cipher.

The next block is AS. Again, draw the box around A and S. This is a proper box with letters at all four corners. Just like in the first step, replace each letter with the one in the opposite corner in the same row. So A gets replaced with C and S gets replaced with N. See below.

```
  Z  O  K  E  P
  R  A  B  C  D
- F  G  H  I  L
  M  N  Q  S  T
  U  V  W  X  Y
```

We'll now skip ahead to the block TM. Both letters are in the same row. The rule in this case is to replace each letter with the one immediately to its right, wrapping around if needed. So M gets replaced with N and T gets replaced with M. See below.

```
  Z  O  K  E  P
  R  A  B  C  D
- F  G  H  I  L
  M  N  Q  S  T
  U  V  W  X  Y
```

To summarize, here is the entire encryption procedure:

1. Write out the letters of the key into a 5×5 grid, only writing the first occurrence of each letter. After the letters of the key are used up, then follow with all the remaining letters of the alphabet in order. But leave out J. In the Playfair cipher, any J's in the key or message are replaced with I's.
2. Go through the plaintext message in blocks of two.
3. If the current block has two repeated letters, replace the second letter with an X and move that second letter to the start of the next block.
4. If the very last block only has one letter, make the second letter a Q.
5. To encrypt a block of two letters, draw a box around them in the table. Then
   (a) If the two letters are in different rows and columns, replace each letter with the letter in the same row in the opposite corner of the box.
   (b) If the two letters are in the same row, replace each with the letter immediately to its right in the table, wrapping around to the left of the table if needed.
   (c) If the two letters are in the same column, replace each with the letter immediately below it in the table, wrapping around to the top of the table if needed.

Decryption is very similar to encryption. Steps 5b and c are similar except you move left and up instead of right and down.