CS 4823: Homework #7

Due on March 9, 2018

Christopher Tse

Problem 1

Let w be a string over $\{A, B, ..., Z\}$. Choose two Caesar cipher keys k_1 and k_2. Encrypt the symbols of w having odd index using k_1 and those having even index using k_2. Then reverse the order of the encrypted string.

Show that the above procedure defines a cryptosystem.

Solution

A cryptosystem is defined as a tuple (P, C, K, E, D) such that P is a set for the plaintext space, C is a set for the ciphertext space, K is a set for the key space, E is a family of encryption functions, and D is a family of decryption functions.

The above system is a cyphersystem since there is a plaintext w in the plaintext space $\{A, B, ..., Z\}$ as described. There is also a final encrypted string which is the ciphertext, which corresponds to C. We have a key space K which is defined by k_1 and k_2. Using this key, we can determine the encryption and decryption functions for E and D like we would for a normal Caesar cipher.

Determine the plaintext space, the ciphertext space, and the key space.

Solution

The plaintext and ciphertext space are the same as described in the problem, $\{A, B, ..., Z\}$.

The keyspace for both k_1 and k_2 are any monic degree 1 polynomial since the keys are always in the form of $c = p + n$ for some integer n in a Caesar cipher.

Problem 2

What is the maximum number of different encryption functions of a block cipher over the alphabet $\{0, 1\}$ with block length n?

Solution

Since block ciphers are permutations, we can find the number of different encryption functions by finding the number of unique permutations in some block. Let n be the block length, n_0 be the number of 0's in the block and n_1 be the number of 1's in the block. We then get the number of encryption keys n_e with

$$n_e = \frac{n!}{n_0! n_1!}$$

Problem 3

Read the page on frequency analysis and write a program to calculate the frequencies of English letters (case-insensitive) in the section "History and Usage" (not including the title of the section and the text in the figures).

Solution

```
1  // frequency.js
2  if (process.argv.length < 3) {
3      console.log('Usage: node frequency.js FILENAME');
4      process.exit(1);
5  }
6
7  const fs = require('fs');
8  const filename = process.argv[2];
9
10 // read in input file
11 fs.readFile(filename, 'utf8', (err, data) => {
12     if (err) throw err;
13
14     // make the text all lowercase and remove non-alphabet characters then split into array
           of individual characters
15     let textArr = data.toLowerCase().replace(/[^a-z]/g, '').split('');
16
17     // reduce the array of characters, incrementing count of character if it exists in the
           object or initializing to 1 if it does not exist yet
18     let result = textArr.reduce( (acc, curr) => {
19         acc[curr] ? acc[curr]++ : acc[curr] = 1;
20         return acc;
21     }, {});
22
23     console.log(result);
24 });
```

```
$ node frequency.js input.txt
```

Problem 4

Suppose that we use Caesar cipher with multiplication over $\mathbb{Z}/26\mathbb{Z}$ (i.e. affine cipher):

$$c = 11p + 5.$$

Can you find the formula for decryption?

Solution

To find the decryption formula we simply perform the inverse operations. We first subtract 5 from the cipher text then multiply by the inverse of the multiplicative factor 11, which is 19. Therefore:

$$p = 19(c - 5)$$

What is the ciphertext for "TEXAS"?

Solution

"GXYFV"

What is the plaintext for "OKLAHOMA" if we treat it as ciphertext?

Solution

"PRKJMPDJ"