CS4021D NUMBER THEORY AND CRYPTOGRAPHY

Documentation

Name: JYOTHI SEVAKULA **Section :** A

Roll No: B180359CS

1. Affine cipher

Affine Cipher We can combine the additive and multiplicative ciphers to get what is called the affine cipher□a combination of both ciphers with a pair of keys. The first key is used with the multiplicative cipher; the second key is used with the additive cipher. The affine cipher is actually two ciphers, applied one after another. We could have shown only one complex operation for the encryption or decryption such as C = (P × k1 + k2) mod 26 and P = ((C − k2) × k1 −1) mod 26. However, we have used a temporary result (T) and have indicated two separate operations to show that whenever we use a combination of ciphers we should be sure that each one has an inverse at the other side of the line and that they are used in reverse order in the encryption and decryption. If addition is the last operation in encryption, then subtraction should be the first in decryption.

2. Hill cipher

Another interesting example of a polyalphabetic cipher is the Hill cipher invented by Lester S. Hill. Unlike the other polyalphabetic ciphers we have already discussed, the plaintext is divided into equal-size blocks. The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block. For this reason, the Hill cipher belongs to a category of ciphers called block ciphers. The other ciphers we studied so far belong to the category called stream ciphers. The differences between block and stream ciphers are discussed at the end of this chapter. In a Hill cipher, the key is a square matrix of size m × m in which m is the size of the block. If we call the key matrix K, each element of the matrix is k i,j

3. Shift cipher

The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature. Assume that the plaintext consists of lowercase letters (a to z), and that the ciphertext consists of uppercase letters (A to Z). To be able to apply mathematical operations on the plaintext and ciphertext, we assign numerical values to each letter (lower- or uppercase)

4. Substitution cipher

Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack. After Alice and Bob agreed to a single key, that key is used to encrypt each letter in the plaintext or decrypt each letter in the ciphertext. In other words, the key is independent from the letters being transferred. A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character. Figure 3.12 shows an example of such a mapping.

5. Transposition cipher

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext. A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

Keyless Transposition Ciphers

Simple transposition ciphers, which were used in the past, are keyless. There are two methods for permutation of characters. In the first method, the text is written into a table column by column and then transmitted row by row. In the second method, the text is written into the table row by row and then transmitted column by column.

Keyed Transposition Ciphers

The keyless ciphers permute the characters by using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example). The permutation is done on the whole plaintext to create the whole ciphertext. Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

6. Vigenere cipher

One interesting kind of polyalphabetic cipher was designed by Blaise de Vigenere, a sixteenth-century French mathematician. A Vigenere cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have $1 \leq m \leq 26$. The cipher can be described as follows where (k1, k2, …, km) is the initial secret key agreed to by Alice and Bob. One important difference between the Vigenere cipher and the other two polyalphabetic ciphers we have looked at, is that the Vigenere key stream does not depend on the plaintext characters; it depends only on the position of the character in the plaintext. In other words, the key stream can be created without knowing what the plaintext is.