**RAVI KANT BASIC CRYPTOGRAPHY**

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain-text messages. The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. The problem? If the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's private key will decode it — meaning theft is of no use without the corresponding private key.

**CAESAR CIPHER**

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials. Thus, to cipher a given text we need an integer value, known as shift which indicates the number of positions each letter of the text has been moved down. The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1, … , Z = 25. The procedure is as follows:

* Traverse the given text one character at a time .
* For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
* Return the new string generated.

**TRIFID CIPHER**

The trifid cipher is a classical cipher invented by Félix Delastelle and described in 1902.Extending the principles of Delastelle's earlier bifid cipher, it combines the techniques of fractionation and transposition to achieve a certain amount of confusion and diffusion: each letter of the ciphertext depends on three letters of the plaintext and up to three letters of the key. The trifid cipher uses a table to fractionate each plaintext letter into a trigram, mixes the constituents of the trigrams, and then applies the table in reverse to turn these mixed trigrams into ciphertext letters. Delastelle notes that the most practical system uses three symbols for the trigrams: In order to split letters into three parts, it is necessary to represent them by a group of three signs or numbers. Knowing that n objects, combined in trigrams in all possible ways, give n × n × n = n3, we recognize that three is the only value for n; two would only give 23 = 8 trigrams, while four would give 43 = 64, but three give 33 = 27.

**BIFID CIPHER**

In classical cryptography, the bifid cipher is a cipher which combines the Polybius square with transposition, and uses fractionation to achieve diffusion. It was invented around 1901 by Felix Delastelle. First, a mixed alphabet Polybius square is drawn up, where the I and the J share their position. The message is converted to its coordinates in the usual manner, but they are written vertically beneath. They are then read out in rows. Then divided up into pairs again, and the pairs turned back into letters using the square. In this way, each ciphertext character depends on two plaintext characters, so the bifid is a digraph cipher, like the Playfair cipher. To decrypt, the procedure is simply reversed.

Longer messages are first broken up into blocks of fixed length, called the period, and the above encryption procedure is applied to each block. One way to detect the period uses bigram statistics on ciphertext letters separated by half the period. For even periods, p, ciphertext letters at a distance of p/2 are influenced by two plaintext letters, but for odd periods, p, ciphertext letters at distances of p/2 (rounded either up or down) are influenced by three plaintext letters. Thus, odd periods are more secure than even against this form of cryptanalysis, because it would require more text to find a statistical anomaly in trigram plaintext statistics than bigram plaintext statistics.

**RAIL FENCE CIPHER**

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm. The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

* In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
* When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner.
* After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

As for decryption, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

* Hence, rail matrix can be constructed accordingly. Once we’ve got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively ).
* Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.