Group Project 533

Group Members: Shreeram Murali, Vinay Nori

Simple Cipher

Caesar Cipher:

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

The easiest way to understand how this cipher works is, see the example below:

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   XYZABCDEFGHIJKLMNOPQRSTUVW
```

Reserve Cipher:

The reverse cipher encrypts a message by printing it in reverse order.

So “Hello world!” encrypts to “!dlrow olleH”.

To decrypt, you simply reverse the reversed message to get the original message. The encryption and decryption steps are the same.

The reverse cipher is a very weak cipher. Just by looking at its ciphertext you can figure out it is just in reverse order.

See if you can figure this out:

“syas ti tahw tuo erugif llits ylbaborp nac uoy ,detpyrcne si siht hguoht neve ,elpmaxe roF”

Double Cipher:

This is a hybrid cipher which makes use of both Caesar Cipher and Reserve Cipher.

First the text is reversed my making use of the same logic behind the reverse cipher, then the data is transformed into encrypted data by making use of Caesar cipher.

Best way to understand this cipher is:

Eg:- HELLO -> OLLEH -> PMMFI

Complex Cipher

Transposition Cipher:

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Example:

Data : We are discovered flee at once.

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

The cipher turns the text into data into the above format.

Then it reads the data in below shown format:

```
WECRL TEERD SOEEF EAOCA IVDEN
```

Multiplicative Cipher:

The Multiplicative Cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function (ax + b) mod 26, where b is the magnitude of the shift.

$$E(x)\ =\ (ax + b)\ mod\ m$$

where modulus m is the size of the alphabet and a and b are the keys of the cipher.

The value a must be chosen such that a and m are coprime. The decryption function is

$$D(x)\ =\ a^\wedge - 1(x - b)\ mod\ m$$