Cryptography and Network Security

Akash Singh Sant (20CS60R40)

September 2020

1 Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties.

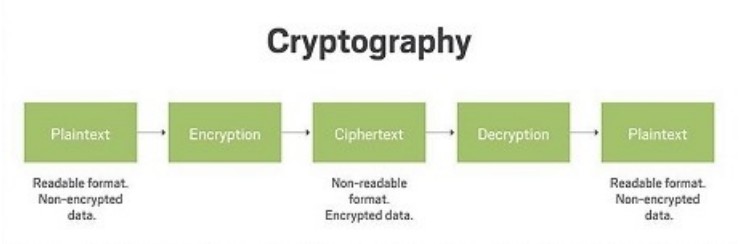
In Cryptography there are 3 major goals :
1.Confidentiality: No third party should be allowed to access the data shared between sender and receiver
2.Integrity: Data shouldn't be modified by unauthorised user.
3.Availability: Data should be easily available to authorized users.

Some of the techniques used to provide Confidentiality and Integrity :
1.Encryption
2.Hash Function
3.Message Authentication Codes.

An important point to note is any technique used to provide confidentiality and integrity shouldn't hinder the availability of data to authorized users.

2 Cryptography Algorithm

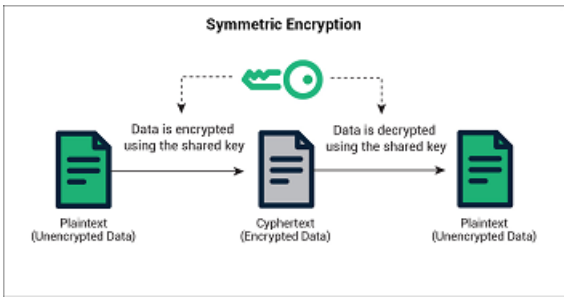
A Cryptography algorithm starts with sender sending the plain text which is then encrypted using a key to produce the encrypted text known as cipher text which is then received at the receiving end is decrypted using the key to get plain text again.



Based on the key , Cryptography can be classified into two classes :
1.Symmetric key Cryptography
2.Asymmetric key Cryptography

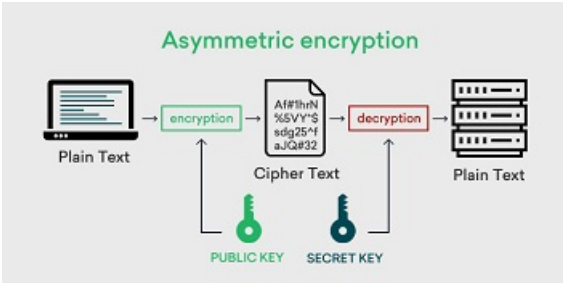
2.1 Symmetric key Cryptography

In symmetric key cryptography both encryption and decryption is done using the same key i.e the key is shared between the sender and receiver.



2.2 Asymmetric key Cryptography

In asymmetric key cryptography encryption is done using the public key and decryption is done using the private key i.e the 2 different keys are used for encryption and decryption.



2.3 Shift Cipher

Consider Plain Text=Cipher text=key=Z_{26},
Here Z_{26} represents the set of english alphabets,where 0 representing A and 25 representing Z Alphabet.
let Key,k be any number in[0,25],i.e there are 26 possibilities for key,
let plain text be x,So the cipher text,y can be obtained in the following way,

$$\mathbf{y=x+k(mod\ 26)}$$

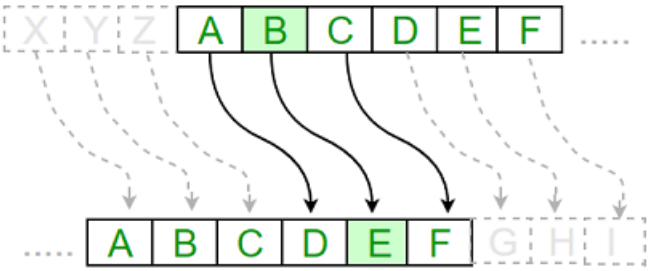
We can get the plain text back from the cipher text as :

$$\mathbf{x=y-k(mod\ 26)}$$

Note : We have used modulo 26 so that the corresponding cipher text value doesnt go out of range.
An example of Shift Cipher is the Caeser Cipher.

2.4 Caeser Cipher

Caeser Cipher uses the key,k=3.So accordingly,
Plain text 'A' is converted into cipher text in the following manner,
Alphabet A corresponds to 0 in Z_{26}
Hence cipher text,y=0+3 mod 26 i.e y=3=C
The same algorithm is applicable to all alphabets and the corresponding cipher is shown in the following figure .



Caeser Cipher uses monoalphabetic substitution.

2.4.1 Monoalphabetic Substitution

A monoalphabetic substitution cipher relies on a fixed replacement structure. That is, the substitution for each letter is done using a particular letter different for each letter. So in this the first letter of plain text have 26 option for a corresponding cipher letter and the next letter will have 25 option and so on.

Max Key Size=26*25.....*1=26!

2.5 Affine Cipher

In affine cipher,Encryption function is given as :

$$e(x)=ax+b(mod\ 26)$$

And,Decryption function is given as :

$$d(y)=a^{-1}(y-b)(mod\ 26)$$

where (a,b) forms the key,In this cipher b can take any value in[0,25]
However a should be co-prime with 26 otherwise the function won't be invertible.