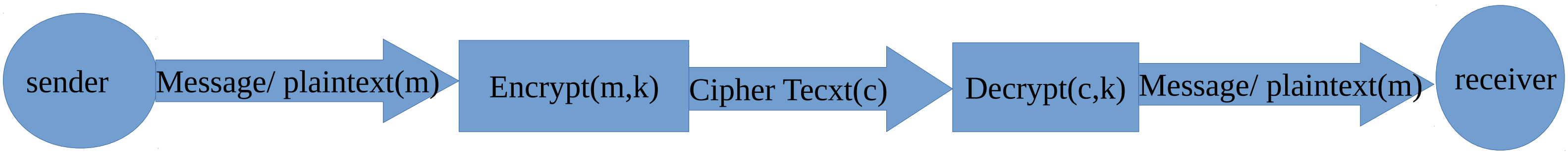
INTRODUCTION TO ENCRYPTION ALGORITHMS:

Definitions of some basic terms:

1. Plain text or message(m) : This is the actual text to be transmitted from sender to Receiver
2. Ciphertext(c): The text generated as a result of encryption algorithm. Sent over the public medium.
3. Key(k):a parameter that determines the functional output of the cryptographic algorithm



1. Ceaser cipher

the shift cipher, Caesar's code or Caesar shift, is one of the simplest and oldest 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 up or down the alphabet. This Fixed number acts a the key.
For example, with a left shift of 3, D would be replaced by A, E would become B, and so on and with a right shift of 3 , D would become G and so on. The method is named after Julius Caesar, who used it in his private correspondence.

For instance, here is a ceaser cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key)-

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line which is 3

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Deciphering is done in reverse, with a right shift of 3.

The encryption can also be represented using modular arithmetic by first mapping the letters to numbers i.e A → 0, B → 1, ..., Z → 25.

Then Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x)=(x+n) \bmod 26$$

Decryption is performed similarly,

$$D_n(x)=(x-n) \bmod 26$$

Before we move on to other encryption schemes, let us see what is symmetric and unsymmetric key encryption:

1. *<u>Secret key cryptography or Symmetric-key cryptography:</u>* the sender and the receiver know the same secret key. And the same key is used to encrypt messages by sender and decrypt by receiver.

There are 2 major types of Symmetric-key encryption :

1. *Stream cipher* – which encrypts the digits of a message one at a time.
2. *Block cipher* -which takes a number of bits (blocks) and then encrypt them as a single unit. 64 bits blocks have been commonly used.

On sender side say Alice:
Encrypt(plaintext, key)=ciphertext
on Receiver's side a.k.a Bob:
Decrypt(ciphertext,key)=plaintext

2. *<u>Public key cryptography or Asymmetric-key cryptography:</u>*

Two keys are used- private keys and public keys. For encryption public key is used and for decryption private key is used . Public key (known to the public) is used to encrypt the message by the sender. The message is decrypted my recieverusing the private key (known only to the user)

On sender side say Alice:(has the public key of Bob)
Encrypt(plaintext, public key of Bob)=ciphertext
on Receiver's side a.k.a Bob:
Decrypt(ciphertext,Private key of Bob)=plaintext

2.One-time pad

The One -time pad is a famous symmetric encryption algorithm which is a stream cipher.

How it works:

Alice(sender) and Bob(receiver) agree upon a secret key k = 10110 (say)

message/plaintext m= 01100

Encryption involves XOR the key k with the plain text.

Thus Encrypt(m,k)=10110 XOR 01100 = 11010 which is the cipher text c.

On Bob's end, to retrieve the m, c is XOR with key again

Decrypt(c,k) = 11010 XOR 10110 =01100 which is the original message

3. RSA

The RSA (Rivest-Shamir-Adleman) is an assymetric encryption algorithm.

It is based on the fact that finding the factors of a large composite number is difficult: especially when the factors are random prime numbers.

Hence even if the public key is known it is difficult to find the private key.

Algorithm:

1.choose two large prime numbers p and q

2.calculate n=p*q which is the modulus for private and public keys

3.claculate phi=(p-1)*(q-1)

4.choose a random integer e such that

i) 1<e<phi

ii) e is not a factor of n

iii) e and phi are co-prime

Now the public key : (n,e) is released into the public

5.choose an integer d which satisfies the relation (d*e)mod n=1 i.e d=(K*phi +1)/e where k is any random integer

The private key: (n,d) is kept a secret and is with only the receiver

if m is the messsage and c is the ciphertext

The sender knows the public key (n,e) of the receiver.

Thus, to encrypt side the formula used is:

$c=m^{e}$ mod n

The private key is a secret known only to the receiver.

Thus, to decrypt the formula used is:

$m=c^{d}$ mod n

Now, d depends on the factor phi = (p-1)(q-1). Thus though n is known , finding its prime factors p, q is a hard problem. Thus it is nearly impossible to get the private key from just the knwledge of the public key. This is the reason for the robustness of the algorithm.