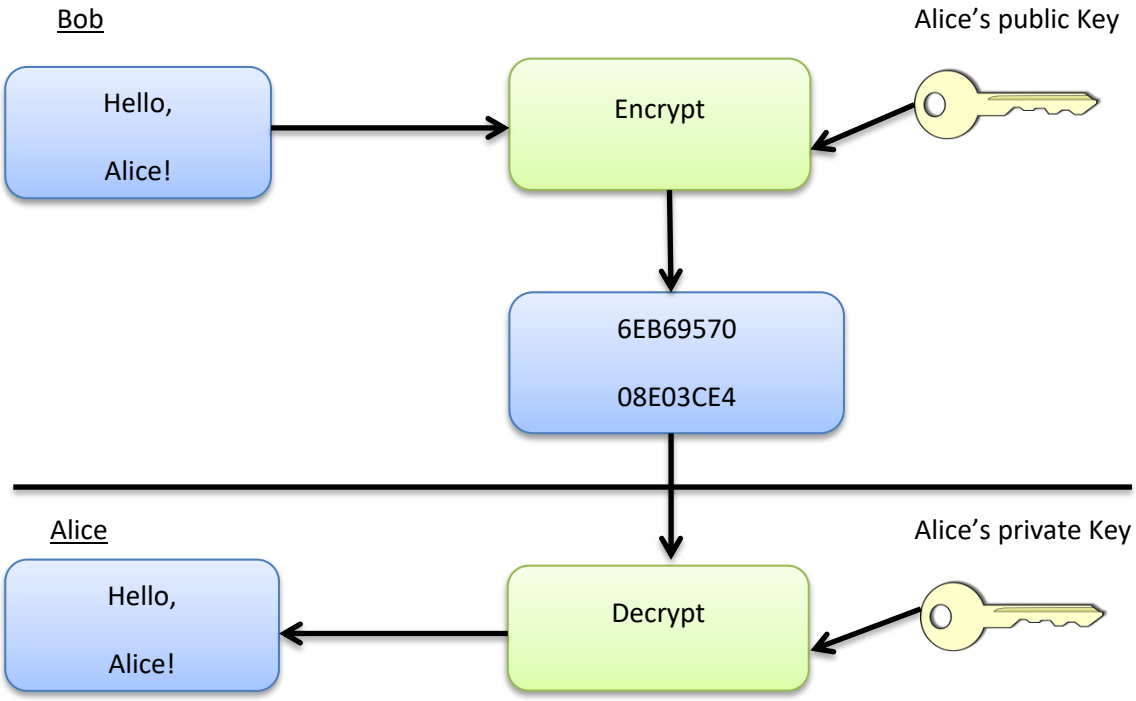
Cryptography

Ankur Pal

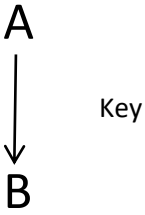
March 10/2018

- Cryptography can be defined as the science of coding or decoding.
- Encrypting data (message/information) in a format such that only authorized parties can read it and extract the information out of it.

The plain text encrypted and gets converted into cipher text (can't be understood by any unauthorized personnel) which gets decrypted and again gets converted to plain text.

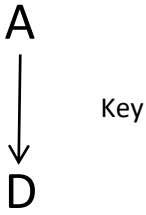


Caesar Cipher: Substituting a letter with another letter through a Key.



Key 1

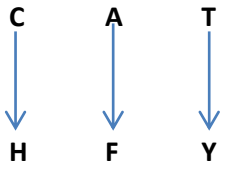
(A shifts 1 position down the alphabets)



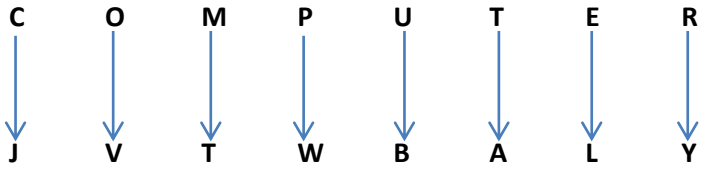
Key 3

(A shifts 3 position down the alphabets)

Ex:



Key 5



Key 7

```
//program for conversion of plain to cipher text
#include<iostream>
using namespace std;
//encrypt is a function to convert
//plain text into cipher text
void encrypt(string s, int n)
{
        cout<<"Plain_text : "<<s<<endl<<" "<<endl;
        string msg=s;
        int i=0, key=n;
        char ch;
        //loop runs till counter variable
        //reaches to null(end of string)
        while(msg[i]!='\0')
        {
                ch=msg[i];
                //converting each character in its cipher character using key value
                //shifting each character down equivalent to key value
```

```
                if(ch>='a' && ch<='z')
                {
                        ch=ch+key;
                        if(ch>'z')
                        {
                                ch=ch-'z'+'a'-1;
                        }
                        msg[i]=ch;
                }
                //similar codes for uppercase character
                else if(ch>='A' && ch<='Z')
                {
                        ch=ch+key;
                        if(ch>'Z')
                        {
                                ch=ch-'Z'+'A'-1;
                        }
                        msg[i]=ch;
                }
                i++;
        }
        cout<<"Cipher_text: "<<msg<<endl;
}
int main(void)
{
        //let the message to be encrypt be "ankur" and the key=5
        encrypt("Ankur", 5);
```

}

Input: Ankur Output: Fspzw

Vigenere cipher: This is slightly different from Cesar cipher as it uses multiple shift value instead of a number as a key value here, a “word” is used as a key.

Let the key be “bacon”

Key = bacon

M e e t m e a t t h e p a r k a t e l e v e n a m

| | | | | | | | | | | | | | | | | | | | | | | | |

b a c o n b a c o n b a c o n b a c o n b a c o n

Here, the message contains 25 letters and the key (bacon) contain 5 letters so it totally divide the message and 5 times bacon is used in the message. If the number of letters in plain text didn’t divided by the number of letter in key then we just end the final repetition of key early using only the letters needed to make everything match up.

We find the shift value of position of each letter of our key- “bacon” in- a to z alphabets

M e e t m e a t t h e p a r k a t e l e v e n a m

| | | | | | | | | | | | | | | | | | | | | | | | |

b a c o n b a c o n b a c o n b a c o n b a c o n

Positions:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ….and so on

a b c d e f g h I j k l m n o p q r s t u v w x y z

Index:

1 0 2 4 3

In our key “bacon” b is in position 1 in 0th index of a to z alphabets and position of a is 0 not 1 and the algorithm works like this.

From above position field the letter

M e e t m e a t t h e p a r k a t e l e v e n a m

| | | | | | | | | | | | | | | | | | | | | | | | |

b a c o n b a c o n b a c o n b a c o n b a c o n

N e g h z f a b h u f p c f x b t g z r w e p o z

M shifts by 1 place to become N

1st e does not shifts

2nd e shifts by 2 places to become g

t by 14th places to h

Cryptography categories are:

- Symmetric Key Cryptography:
  - Same algorithm with same key is used for encryption and decryption.
  - The key must be kept secret.
  - It may be impossible or at least impractical to decipher a message if no other information is available.

- Asymmetric Key Cryptography:
  - One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
  - One of the two keys must be kept secret.
  - It may be impossible or at least impractical to decipher a message if no other information is available.

References:

- Google.com
- CS50