## **Cryptography**

## 

## **Cryptography is the method of protecting information by transforming it into a secure format, a encrypted message in which letters are replaced with other characters.**

## 

## **Some terms :**

## **Plain text : Unencrypted message**

## **Cipher text : Encrypted message**

## **Encryption : Process of converting plain text into cipher text.**

## **Decryption : Process of converting cipher text into plain text.**

## **Algorithm : The method used to encrypt/decrypted the plain text.**

## **Key : The data used for encrypting/decrypting.**

## 

## **There are some cryptographic algorithms present, generally we categorise them as follows -**

## 

## **Symmetric Cryptography :**

## **In this one single key is used for encryption and the same key is used for decryption. DES is the example of symmetric key cryptography.**

## 

## **Asymmetric cryptography/Public key cryptography :**

## **In this two keys are used, Public key is used for encryption and private key is used for decryption like RSA.**

## 

## **Substitution cipher :**

## **Substitution cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext.**

## **Caesar Cipher works by adding or subtracting 3 or any characters. That means if in a Plain Text there is a Character E either it will be**

## **transferred it to B and if the character is A it will be transferred to X.**

## **This Cipher algorithm is having some mathematical equations which describe the functionality of a cryptography process.**

## **One more thing you can give alhphabets and substration, addition value according to your need. You can do addition to subtraction and subtraction to addition too**

## **to need.**

## 

## **Example Of Ceaser Cipher :**

## 

## **KEY : ABCDEFGHIJKLMNOPQRSTUVWXYZ**

## 

## **Encryption Algo : Subtraction and addition of 3 character of number**

## 

## **Substraction :**

## **Plain text : GOURAV**

## **Cipher text : DLROXS**

## 

## **Addition :**

## **Plain text : DLROXS**

## **Cipher text : GOURAV**

## 

## **Decryption Algo : Addition and substraction of 3 character of number**

## 

## **Addition :**

## **Plain text : GOURAV**

## **Cipher text : JRXUDY**

## 

## **Substraction :**

## **Plain text : JRXUDY**

## **Cipher text : GOURAV**

## 

## **Data Encryption Standard (DES)**

## **Introduced in 1975**

## **Standardized in 1977**

## **Problem with DES: short key length (56 bits)**

## **Now considered as insecure**

## **Improved version: Triple DES (involves DES three times)**

## **Problem with Triple DES: slow, compute heavy**

## 

## **Advanced Encryption Standard (AES)**

## **First published in 1998**

## **Became a federal government standard in 2002**

## **First approved (and only) publicly accessible cipher approved by the NSA for top secret information.**

## 

## 

## **Stegnography**

## 

## **Steganography is a process in which we basically hide a data inside a data. It is just a process of embedding a secret piece of text within a text, picture, or audio.**

## 

## **Commands for windows:**

## **CMD > copy /b sunset.jpg+secret.txt sunsetsecret.jpg**

## 

## **Here, /b is used for Binding the 2 files, Copy is used for copying the content of second file to first file.**

## 

## **#copy /b sunset.jpg+secret.txt sunsetsecret.jpg**

## 

## **Commmand for linux :**

## **#steghide embed -cf sunset.jpg -ef secret.txt - For hiding txt file data into this image.**

## **Now enter the password you want to give for this file.**

## **#steghide extract -sf sunset.jpg - For extracting data from image**

## **Enter the password and you will get the txt file.**

## **#steghide info kevinmitnick.jpg**

## 

## **Hashes :**

## **A hash is a function that converts one value to another. But there is a difference between a cipher encryption and a hash. The difference is encrypted text can be reverted**

## **and further decrypted, but hashes cannot be reverted. We need to crack the hashes.**

## **Hash function is that which takes an input and returns a fixed-size alphanumeric string. The string is called the hash value. Examples MD5 Hash.**

## 

## **EG. alphanumeric - scusege67dg367df7fd3fd37f3636d**

## 

## **Cracking methods for Hashes :**

## 

## **We have to create a dictionary and have to convert every word into the hash of a particular wordlists, and after that we will compare that particular hash.**

## **If matches it means that the specific word is found. Hashes are usually uniques.**

## 

## **Passwords & hash functions :**

## **https://www.youtube.com/watch?v=cczlpiiu42M**

## 

## **1. MD5 :**

## **It will convert the plain text into hexadecimal text of fixed length. It always creates a unique hash for the plain text.**

## 

## **Tool we can use for hash cracking :**

## **Hashcat is the world’s fastest and most advanced password recovery tool. It is the fastest hash recovery tool which converts the wordlist into the hashes and then**

## **matches those hashes with the specific hash we want to recover. It is pre-installed in kali linux OS.**

## **Instead of using standard CPU cores, it will use GPU or Graphic card cores.**

## 

## **Commands :**

## **#hashcat -m 0 -a 3 <hashfile in txt> <dictionary|wordlist>**

## **#hashcat -m 0 -a 3 /root/Desktop/hash.txt /usr/share/wordlists/rockyou.txt**

## **#hashcat -m 0 -a 3 /root/Desktop/hash.txt /usr/share/wordlists/rockyou.txt --force**

## 

## **Here,**

## **hashcat is the tool for password recovery**

## **-m : hash type**

## **0 : MD5**

## **-a : attack mode**

## **3 : Brute force attack**

## **hash.txt : file containing hashes to be recovered**

## **rockyou.txt : for brute forcing and comparing**

## **--force : to start forcefully**

## 