Basic Terms:

1. Cryptography:

The study of methods used to convert plain to cipher and cipher to plain text.

a. Symmetric Cryptography:

In symmetric cryptography, the key which is used for encryption is also used for decryption. But the key is going to be exchanged between the sender and the receiver through the internet which is an unsecure public channel. Mechanisms are applied to defend the keys from getting to attacker or exchanging the keys via a secure channel is also done but at the end it is the internet which is public. Examples of symmetric cryptography are DES, Triple DES, AES etc.

b. Asymmetric Cryptography:

In asymmetric cryptography, there are two keys with the sender and two keys are with the receiver, aender's public and private and receiver's public and private key. Here the public keys are general to public. The core concept of this cryptography is that if a person encrypts the message with his public key, it will be only decrypted by that person's private key and vice versa. For example, if a sender wants to send a message to the receiver, first the sender will get the receiver's public key because it will be public, then the sender will encrypt the message to be sent with receiver's public key, and will send over the internet. On receiving, the receiver will decrypt the message with his private key because private keys are private to sender as well as receiver. Example of asymmetric cryptography is the RSA encryption algorithm.

2. Plain text:

The message sender wants to send in its original form is called plain text.

3. Cipher text:

The convereted plain text after passing through an encryption algorithm by a applying a key is called cipher text.

4. Cipher:

The encryption algorithm is called the cipher.

5. Key:

The information applied to the encryption algorithm other than plain text to encrypt the plain text is called a key.

6. Cryptanalysis:

A malicious activity done by hackers in which attempts to know the plain text from the cipher text without using the key (Or decyphering without the key) is called cryptananlysis.

7. Cryptology:

The combination of cryptography and cryptanalysis.

BRUTE FORCE ATTACK:

• Trying all possible combinations .

• One of the ways to stop brute force attack is using captchas on login page.There are many ways to launch a brute force attack but on a login page we can use captchas This captcha will determine whether a human is accessing the computer system or a bot program. After trying a few password guesses, user is given a captcha. Captcha is given if multiple

times credentials are given, whether it is by human or a bot program. Bots cannot solve captchas.

• CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart"

• In cryptography Brute force attack means trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained .It is a guessing attempt.

SOME TOOLS USED FOR BRUTE FORCE:

- Aicrack-ng
- Hydra
- Hashcat
- Crack
- Ophcrack
- Rainbowcrack
- John the ripper
- DaveGrohl
- Cain and Abel