LECTURE-2
network security
DITS-512

Cryptography

→ There are two type of security techniques used ① cryptography
② Steganography

→ cryptography word coined from Greek word Kryptos and graphein mean's secret/ writing

× In other word we can say that cryptography is a conversion of meaningful data to meaningless data

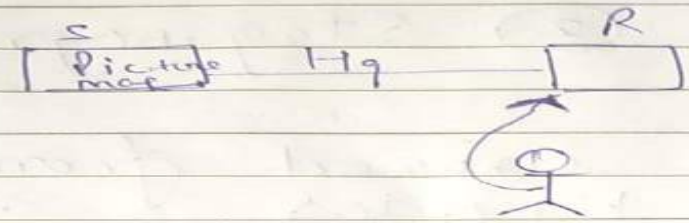
→ Algorithms are mathematical technique, applie cryptographic services to achieve security.

* In cryptography algo are two types of algo used
  ① Encryption
  ② Decryption.

→ Cryptography used mainly three type of mechanisms like symmetric key encipherment, Asymmetric key encipherment and Hash-ing.

Steganography

→ steganography with origins in Greek means "covered writing"



Means if we want to send a Message from Source (S) to Reciver (R), send it in hidden from, in above example Sender send a image with Message attacker think it a normal image but sender send covered message with this image, this type of technique is called steganography.

→ other hand in cryptography we converted normal message into encrypted from or secret form by alteration or security technique.

Diffrance Between

CRYPTOGRAPHY

- It is a kind of known communication.
- It is a technique to convert the secret message into an unreadable form.
- It alter the overall structure of the data
- Key is necessary
- The final result obtain is called ciphertext

STEGANOGRAPHY

It is a kind of hidden communication

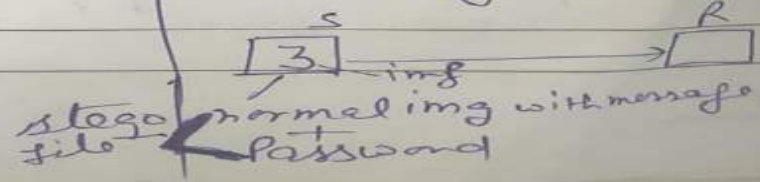
It is a technique to hide the existence of communication

It does not alter the overall structure of data.

Key is optional but if used provide more security

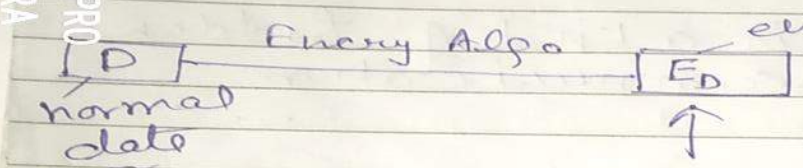
The final result obtained is called stego media

(img + secret info)



Attack — crypt analysis attack

Once it has been discovered, no one can easily get

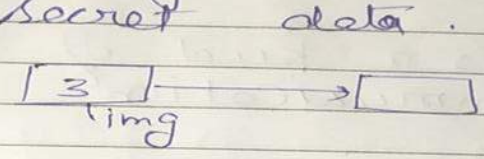


if any attacker get cipher text / data then he can not easily get original data because the Plain text is converted into the cipher text with the help of key. So that, person must have key for decryption that cipher that is not easy task mean Key searching. (cipher message + key) both are required for decryption.

* More popular approach

attack - steg analysis (art to detect the communication)

→ Once it has been discovered anyone can get the secret data.



if attacker search this is not a simple img, and this img has some message that he can easily

* Less popular approach

Text Steganography

Our secret message may be the 1st or nth character of the stego message.

Example-Susan eats truffles. Under pressure, that helps everything before Owning Major Bullwinkle.

real or secret message "Set Up the bOMB"

Tool:snow- used to conceal messages in ASCII text by appending white-space to the end of lines.