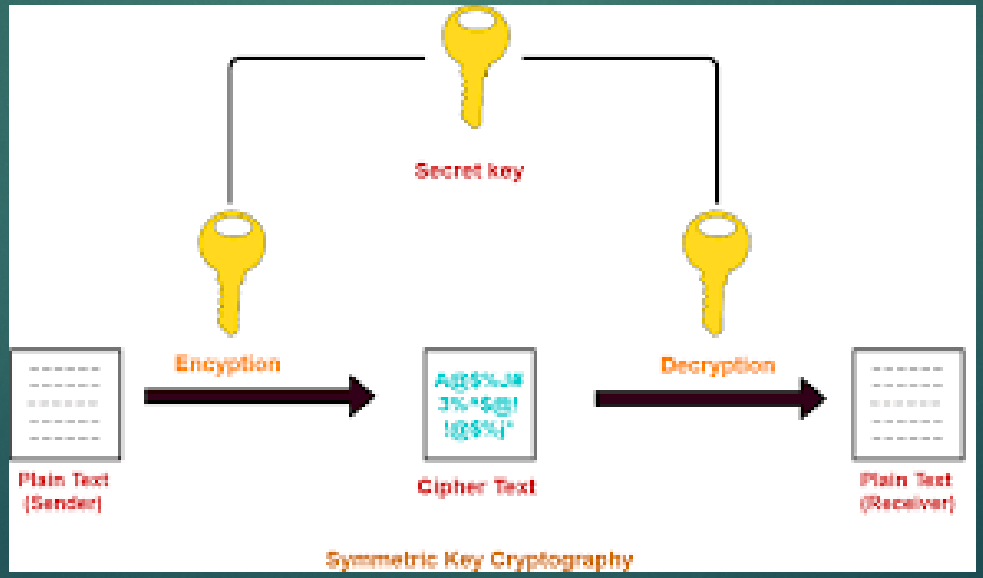
Network Security Laboratory – Lecture 2

SYMMETRIC CRYPTOGRAPHY & STEGANOGRAPHY

Symmetric Cryptography

- Most widely used encryption system
- Based on shared key between hosts
- Most common symmetric algorithms are: DES, AES, TwoFish, etc…



Netcat

- CLI Tool for plain text transmission
- Used for reading and writing data between two computer in the networks

- Useful commands:
  - Server:
    - netcat -l <port>
  - Client:
    - netcat <hostname> <port>

- It will be used to exchange encrypted messages between 2 hosts

OpenSSL Enc

- It allows to encrypt or decrypt data using various block and stream ciphers, keys based on passwords or explicitly provided
- Used to encrypt data from stdin or files

- Useful commands:
  - Encrypt:
    - openssl enc -<cipher> -e -k <key> -in <file>
  - Decrypt:
    - openssl enc -<cypher> -d -k <key> -out <file>

- It will be used to encrypt and decrypt data sent/received by hosts

Cryptocat

- Download exercise **cryptocat.pdf** on course website
- Create and execute a python3 script called **cryptocat.py**
- Execute Wireshark and sniff the traffic between the hosts
- What are the differences between plain text and cypher text on wireshark?
- Hint
  - To execute bash command through python you can use **os.system('your_command')** or the **subprocess** library

How to build an encrypted stream?

Cryptcat

- CLI Tool for encrypted text transmission in a stream
- It is a simple Unix utility which reads and writes data across network connections
- It makes use of TCP or UDP protocols
- It encrypts the data before transmission
- It is based on Netcat
- It uses a symmetric encryption algorithm (TwoFish) to send streams

- Useful commands:
  - Server:
    - cryptcat -l <port> -k <key>
  - Client:
    - cryptcat <hostname> <port> -k <key>

Cryptcat - attack

- Can we capture and decrypt an encrypted stream?
- YES, try to use
  - Decryptcat
  - Netcat
- Check **decrypt_cryptcat.pdf** on the website and follow the guide

Steganography

- Technique for hide data into images or video
- The output images contains secret data
- The hidden file cannot be seen immediately without a deeper analysis of the image itself
- Image must be decrypted in order to extract hidden data

Mutt

- It is a tool to send email through CLI
- It uses SMTP protocol

- Useful Commands:
  - Send email: mutt [-s subject] [-a attachment] receiver_address

Steghide

- Download exercise **Steghide.pdf** on course website
- Build and execute **steghide.py**
- Capture the traffic using wireshark
- Useful commands:
  - Encryption:
    - steghide embed -cf <source> -ef <data_to_encrypt> -sf <output_file> [-k key]
  - Decryption:
    - steghide extract -sf <image_with_encrypted_data>