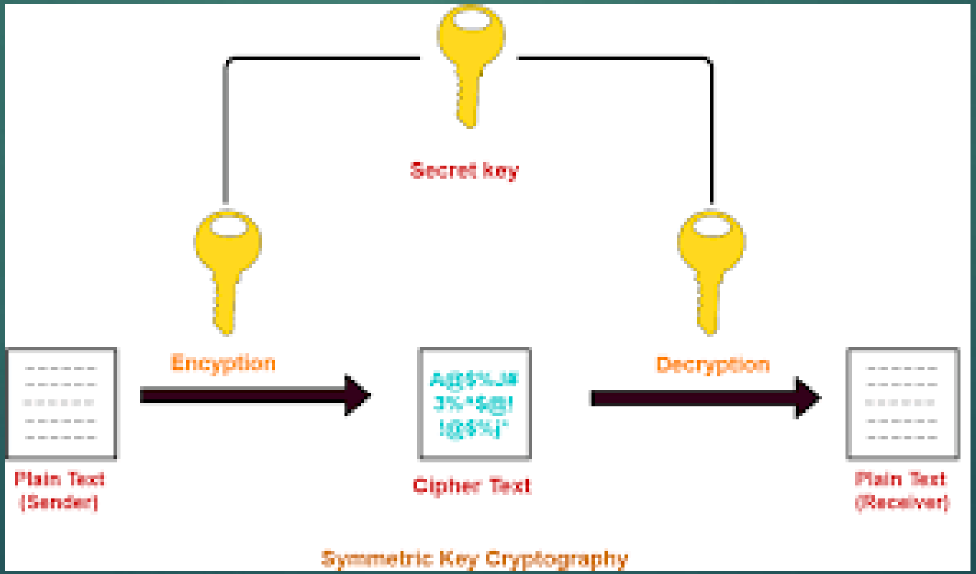
Network Security Laboratory – Lecture 2

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...



Symmetric Key Cryptography

Netcat

- CLI Tool for plain text transmission
- Used for reading and writing to network connections
- We will use to establish a simple stream

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

OpenSSL Enc

- Tool for encryption
- Used to encrypt data from stdin or files
- We will use it for data encryption and send it on network stream

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

Cryptocat

- Download exercise Cryptocat.pdf on course website
- Build and Run cryptocat.py and see what's going on on wireshark
- What are the differences between plain text and cypher text on wireshark?
- Useful commands:
    - To execute bash command through python use os.system('your_command')

But.. how to build an encrypted stream?

Cryptcat

- CLI Tool for encrypted text transmission in a stream
- Based on Netcat
- For encryption it uses TwoFish
  - A symmetric encryption algorithm

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

Cryptcat - attack

- Can we capture and decrypt an encrypted stream?

- We can do this with some technique and some useful tools like:
  - Decryptcat
  - Netcat

- On course website there is the guide **decrypt_cryptcat.pdf** that will help us to do this

Cryptcat

- Cryptcat is a CLI tool
- Ensure a stream using symmetric cryptography
- Based on NetCat

Useful commands:

Server:

```
netcat -l <port>
```

Client:

```
netcat <hostname> <port>
```

Steganography

- Technique for hide data into images or video
- The output images contains secret data
- the hidden file cannot be seen with the naked eye
- To show it we should decrypt the images

Mutt

- Is a tool to send email through CLI
- Using SMTP protocol
- For configuration go on https://github.com/DeMaCS-UNICAL/NetworkSecurity/tree/master/esercitazioni/Lectures_20-21/Symmetric_Cryptography/steghide
- Download installAndConfigure_msmtp.txt and msmtp_config.txt
- Configure msmtp to send email with mutt

- Useful Commands:
  - Send email: mutt [-s subject] [-a attachment, use -- at end of attachments] receiver_address

Steghide

- Download exercise Steghide.pdf on course website
- Build Run steghide.py and see what’s going on on 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>

Questions?

The lesson is over.

Thank you!