PROGRAMMAZIONE DI

SISTEMI E RETI

(SER)

A.S. 2020-2021

– CLASSE 5R–

Prof. Enrico Contini

Prof. Piermario Carboni

Tecniche di filtraggio del traffico di rete

Questa parte è stata affrontata prevalentemente in laboratorio con l'uso del software di simulazione Cisco Packet Tracer.

Introduzione. Richiami ai protocolli TCP/IP e al modello ISO/OSI. Relazione tra apparati di rete, filtraggio e sicurezza. Il problema del protocollo ARP/RARP e il funzionamento di hub e switch. Il router e indirizzamento. Il protocollo Spanning T. Le reti VPN

Tecniche crittografiche applicate alla protezione dei sistemi e delle reti.

PARTE I: Introduzione.

Concetti introduttivi sulla crittografia e sulla steganografia. Cenni storici agli albori della critto-steganorafia. Relazione della crittografia e della steganografia con i concetti più generali di sicurezza informatica.

LEZ_intro_critto_stegano.pdf

PARTE II: Steganografia.

Steganografia "forte" testuale: la maschera (griglia) di Cardano. Digitalizzazione della griglia. Steganografia "debole" testuale: ricostruzione del messaggio da testo in chiaro. Steganografia da immagini. Relazione con la crittografia.

LEZ_stegano.pdf

PARTE III: Crittografia classica.

Cifrario di Cesare. Applicazione della forza bruta per decifrare un messaggio del cifrario di Cesare. I cifrari di Alberti (Dischi di Alberti): le "case" e la chiave. Primi esempi storici di crittoanalisi e statistica al servizio della decifratura. Il cifrario di De Vigenere e il concetto di "verme" e cifrario polialfabetico. Relazione del cifrario con quello di Vernom.

crittografiche applicate alla protezione dei sistemi e delle reti.

PARTE IV: Crittografia moderna.

Il teorema di Kirkhof e il cifrario perfetto. Cenni al teorema di Shannon. Crittografia simmetrica, asimmetrica e hashing. Chiavi pubbliche e private. Il crivello di Eratostene e i numeri primi. Algoritmo di Diffie-Hellman (DH). Crittografia ibrida. Firma digitale. Il cifrario matematicamente inattaccabile (Cifrario russo) e contesto storico .

LEZ_critto_classica.pdf

Modello client/server

PARTE I: I serventi web.

La storia di Apache2 e le versioni per windows e per GNU/Linux. L'integrazione con il PHP e i linguaggi lato server.

LEZ_server_web.pdf

Studenti prof. Enrico Contini prof. Piermario Carboni

_____ _____

_____

_____