

**PROGRAMMA SVOLTO A.S. 2022/23  
SISTEMI E RETI**

**Modelli di riferimento per le reti:**

- TCP/IP e pila ISO-OSI
- Architettura di rete: strati, protocolli e interfacce; PDU, servizi e primitive
- Comunicazione tra protocolli
- Indirizzi IP - IPv4 e IPv6
- Metodologia Classful - Subnetting
- Il protocollo IP: IP-header (Analisi dell'intestazione del pacchetto IP: nomi dei campi e loro funzionalità)
- Protocolli di servizio dello strato Internet: ARP e ICMP
- Protocolli di Trasporto: TCP, UDP e le relative intestazioni, le porte, i socket, e le connessioni

**Apparati di rete locali e per connessione a reti geografiche**

- hub - switch - router

**Sicurezza della Rete**

- Tecniche crittografiche per la sicurezza di rete
- Cifrario a sostituzione e a Trasposizioni
- Crittografia simmetrica: DES - Triple-DES
- Crittografia a chiave pubblica: RSA
- Attacchi alla rete: phishing, Dos, Ip spoofing, port scanning
- Firewall e DMZ.

**Sessione e Presentazione**

- Funzionalità del livello sessione e presentazione.
- Algoritmi di compressione

**Protocolli e servizi di rete a livello applicativo**

- Il sistema dei nomi di dominio: Architettura del DNS, Funzionamento del DNS, Organizzazione del DNS
- Posta elettronica: Architettura e funzionamento del servizio e-mail (SMTP, POP3/IMAP)
- Il protocollo FTP
- Il protocollo HTTP: la comunicazione nel

web e i messaggi HTTP

**Protocolli e servizi di rete a livello applicativo**

- DNS
- HTTP /HTTPS
- SMTP, POP3, IMAP
- FTP

**Applicazioni, protocolli, componenti**

**hardware per garantire la sicurezza nelle reti**

- Firma digitale
- HTTPS
- FIREWALL
- DMZ

**Firma digitale**

- la firma digitale: autenticazione del mittente e non ripudio di un documento
- Digest cifrato: impronta digitale per garantire l'integrità del messaggio
- Certificati digitale e enti certificatori
- Sicurezza: VPN e i protocolli dell'Ipsec

**Progettazione di reti**

- Progettazione di una rete, LAN, MAN, WAN
  - SICUREZZA FISICA, principi di sicurezza dei sistemi, superfici e tipologie di attacco, protezione dei sistemi e delle reti
  - sicurezza al livello APPLICATIVO: crittografia
  - sicurezza al livello DI RETE
- Relazione e implementazione degli esercizi svolti tramite l'applicativo CISCO PACKET TRACER
- I comandi in linea per la risoluzione di problemi di rete, per accedere alla configurazione e per ottenere utili informazioni sulle connessioni: ipconfig, netstat, tracert, nslookup
- Analisi delle prove d'esame degli anni passati