1 - Informatica

1.1. Basi di Dati - Sicurezza

Noi vogliamo garantire alcuni principi fondamentali, tipici della crittografia = CIA.

- **Confidenzialità** (C = Confidenzialità)
- **Integrità** (I = Integrità)
- **Disponibilità** (A = Availability)

Una base di dati ha alcune proprietà:

- **Persistenza**: i dati sopravvivono ai programmi che li utilizzano
- **Condivisione**: accesso simultaneo da più utenti/applicazioni
- **Affidabilità**: protezione da malfunzionamenti e perdite
- **Efficienza**: prestazioni ottimali nelle operazioni
- **Efficacia**: soddisfa i requisiti dell'utente

1.2 Modello E-R

Il modello E-R (Entità - Relazione) rappresenta delle **realtà / domini** (es. vuoi modellare una biblioteca / cinema) che permetta di salvarne le informazioni in un *modo semplice ma preciso* (sicuro e permanente)!

È strutturato in:

1. Entità

- Oggetti del mondo reale di interesse per l'applicazione
- Rappresentate con rettangoli
- Esempi: STUDENTE, CORSO, DOCENTE

2 Attributi

- Proprietà delle entità
- Rappresentati con ellissi
- Tipi:
    - **Semplici**: non scomponibili (Nome)
    - **Composti**: scomponibili (Indirizzo = Via + Città + CAP)
    - **Chiave**: identificano univocamente l'entità (sottolineati)

3. Relazioni

- Associazioni tra entità
- Rappresentate con rombi
- **Cardinalità**: 1:1, 1:N, N:N

Regole di Traduzione E/R → Relazionale

1. **Ogni entità** diventa una **tabella**
2. **Ogni attributo** diventa una **colonna**
3. **Relazioni 1:1**: chiave esterna in una delle due tabelle
4. **Relazioni 1:N**: chiave esterna nella tabella "molti"
5. **Relazioni N:N**: nuova tabella con le chiavi delle entità coinvolte

> Possibili collegamenti:
>
> - Storia (800/900 rispetto alle guerre - tecnologia e sviluppo dei mezzi di comunicazione (relazioni = salvataggio permanente delle informazioni)
> - Inglese (Figure chiave dell'informatica - Alan Turing)

1.3. Modello relazione

Relazione (Tabella)

- Insieme di *tuple* (righe) con stessa struttura
- Ogni tupla rappresenta un'*istanza* dell'entità

Schema di Relazione

- $R(A_1, A_2, ..., A_n)$ dove R è il nome e $A_1...A_n$ sono gli attributi
    - Es. Studenti("CF", Nome, Cognome, Data)

Dominio

- Insieme dei valori ammissibili per un attributo

Chiave Primaria

- Attributo/i che identificano univocamente ogni tupla

- Non può contenere valori NULL

Chiave Esterna (Foreign Key)

- Attributo che referenzia la chiave primaria di un'altra tabella
- Garantisce l'integrità referenziale

> Possibili collegamenti:
>
> - TPS (Salvare i permessi di ogni utente all'interno di XML e fare in modo che siano separati)

1.4 Normalizzazione

Prima Forma Normale (1NF)

Una relazione è in 1NF se:

- Ogni attributo contiene **valori atomici** (non scomponibili) .- singoli logicamente
- Non ci sono **attributi multivalore**

Esempio NON in 1NF:

```
STUDENTE(Matricola, Nome, Telefoni)
123, Mario Rossi, "123456, 789012"
```

Esempio in 1NF:

```
STUDENTE(Matricola, Nome)
TELEFONO(Matricola, Numero)
```

Seconda Forma Normale (2NF)

Una relazione è in 2NF se:

- È in **1NF**
- Ogni attributo non-chiave dipende **completamente** dalla chiave primaria

Dipendenza Funzionale: A → B (A determina B)

Terza Forma Normale (3NF)

Una relazione è in 3NF se:

- È in **2NF**
- Non ci sono **dipendenze transitive** (A → B → C, quindi A → C)

> Possibili collegamenti:
>
> - Inglese / Storia

1.5. SQL

Classificazione SQL

1. Creazione

- CREATE, ALTER, DROP
- Definisce la struttura del database

2. Modifica / cancellazione

- SELECT, INSERT, UPDATE, DELETE
- Manipola i dati

3. Controllo

- GRANT, REVOKE
- Gestisce i permessi

> Possibili collegamenti:
>
> - Sistemi (Crittografia / Permessi solo utili ai singoli utenti + la parte Reti)
> - TPS (GPDR - Framework sicurezza + AI)

Creazione Database

```
CREATE DATABASE nome_database;
```

Creazione Tabella

```
CREATE TABLE STUDENTE (
    Matricola INT PRIMARY KEY,
    Nome VARCHAR(50) NOT NULL,
    Cognome VARCHAR(50) NOT NULL,
    DataNascita DATE,
    Email VARCHAR(100) UNIQUE
);
```

Vincoli di Integrità

- **PRIMARY KEY**: chiave primaria
- **FOREIGN KEY**: chiave esterna
- **NOT NULL**: campo obbligatorio
- **UNIQUE**: valore univoco
- **CHECK**: controllo su valori ammissibili

Inserimento

```
INSERT INTO STUDENTE (Matricola, Nome, Cognome)
VALUES (123, 'Mario', 'Rossi');
```

Modifica

```
UPDATE STUDENTE
SET Email = 'mario.rossi@email.com'
WHERE Matricola = 123;
```

Cancellazione

```
DELETE FROM STUDENTE
WHERE Matricola = 123;
```

Sintassi Base

```
SELECT attributi
FROM tabelle
WHERE condizioni
GROUP BY attributi
HAVING condizioni_gruppo
ORDER BY attributi;
```

Operatori di Confronto

- `=, <>, <, >, <=, >=`
- `LIKE` (pattern matching con % e _)
- `IN` (appartenenza a un insieme)
- `BETWEEN` (intervallo)
- `IS NULL / IS NOT NULL`

Operatori Logici

- `AND, OR, NOT`

Funzioni di Aggregazione

- `COUNT()` : conta le righe
- `SUM()` : somma valori
- `AVG()` : media
- `MAX(), MIN()` : valore massimo/minimo

INNER JOIN (equi-join)

```
SELECT s.Nome, c.Titolo
FROM STUDENTE s
INNER JOIN ISCRIZIONE i ON s.Matricola = i.Matricola
INNER JOIN CORSO c ON i.CodCorso = c.CodCorso;
```

LEFT/RIGHT JOIN

- Include anche le righe senza corrispondenza

Tipi di JOIN

- **Theta JOIN**: condizione generica
- **Equi JOIN**: condizione di uguaglianza
- **Natural JOIN**: su attributi con stesso nome

1.6 - Collegamenti Informatica

STORIA

1.1 Basi di Dati - Sicurezza (CIA)

- **Controllo dell'informazione nei regimi totalitari**: schedatura fascista e nazista per controllare la popolazione
- **Guerra Fredda**: intelligence e protezione delle informazioni strategiche
- **Archivi storici**: necessità di preservare documenti storici (disponibilità) e garantirne l'autenticità (integrità)

1.2 Modello E-R

- **Genealogie reali**: modellazione delle dinastie europee (entità SOVRANO, relazioni SUCCESSIONE)
- **Reti commerciali medievali**: entità MERCANTE, CITTÀ, PRODOTTO con relazioni commerciali
- **Organizzazione militare**: strutture gerarchiche dell'esercito come modelli E-R

1.4 Normalizzazione

- **Riorganizzazione amministrativa**: eliminazione di duplicazioni burocratiche nell'Unità d'Italia
- **Standardizzazione industriale**: principi tayloristi e fordisti per eliminare sprechi

ITALIANO

1.1 Basi di Dati - Sicurezza

- **Verismo**: documentazione "scientifica" della realtà sociale (persistenza delle informazioni)
- **Archivi letterari**: conservazione e catalogazione del patrimonio culturale

1.2 Modello E-R

- **Personaggi dei Malavoglia**: modellazione delle relazioni familiari e sociali
- **Strutture narrative**: entità AUTORE, OPERA, PERSONAGGIO, TEMA
- **Intertestualità**: relazioni tra opere letterarie

1.4 Normalizzazione

- **Stile essenziale di Ungaretti**: eliminazione del superfluo poetico
- **Editing letterario**: processo di revisione per eliminare ridondanze

1.5 SQL

- **Interrogative indirette**: struttura logica simile alle query SQL
- **Concordanze bibliche**: primi esempi di "query" su testi

INGLESE

1.1 Basi di Dati - Sicurezza

- **Cybersecurity**: terminologia tecnica CIA (Confidentiality, Integrity, Availability)
- **Digital privacy**: protezione dei dati personali nell'era digitale

1.2 Modello E-R

- **Alan Turing**: pioniere dell'informatica e dei modelli computazionali
- **Database design**: metodologie di progettazione in ambito internazionale

1.5 SQL

- **Structured Query Language**: linguaggio standardizzato internazionale
- **Technical documentation**: manuali e specifiche tecniche in inglese

MATEMATICA

1.2 Modello E-R

- **Teoria degli insiemi**: entità come insiemi, relazioni come prodotti cartesiani
- **Grafi**: rappresentazione matematica delle relazioni
- **Funzioni**: chiavi primarie come funzioni iniettive

1.3 Modello Relazionale

- **Relazioni matematiche**: R ⊆ A × B
- **Algebra relazionale**: operazioni di unione, intersezione, differenza

1.4 Normalizzazione

- **Dipendenze funzionali**: f: A → B
- **Ottimizzazione**: minimizzazione della ridondanza

1.5 SQL

- **Logica proposizionale**: operatori AND, OR, NOT
- **Funzioni di aggregazione**: operazioni matematiche su insiemi
- **Serie numeriche**: per ottimizzazione delle query

SISTEMI E RETI

1.1 Basi di Dati - Sicurezza

- **Crittografia simmetrica e asimmetrica**: protezione dei dati in transito
- **Firewall e DMZ**: protezione perimetrale dei database server
- **VPN**: accesso sicuro ai database remoti

1.3 Modello Relazionale

- **Database distribuiti**: frammentazione e replicazione
- **Load balancing**: distribuzione del carico sui server database

1.5 SQL

- **Protocolli TCP/IP**: comunicazione client-server con database
- **Backup e recovery**: strategie di disaster recovery

TPSIT

1.1 Basi di Dati - Sicurezza

- **GDPR**: regolamentazione europea sulla protezione dati
- **AI Act**: normative su intelligenza artificiale e dati
- **Audit trail**: tracciabilità delle operazioni sui dati

1.3 Modello Relazionale

- **ORM**: mapping oggetto-relazionale in sviluppo software
- **API RESTful**: operazioni CRUD via HTTP

1.5 SQL

- **Prepared statements**: prevenzione SQL injection
- **Connection pooling**: gestione efficiente delle connessioni database

GPOI

1.1 Basi di Dati - Sicurezza

- **Business continuity**: piani di continuità operativa
- **Risk management**: gestione rischi informatici
- **Compliance**: conformità normativa (SOX, GDPR)

1.2 Modello E-R

- **Organigramma aziendale**: modellazione strutture organizzative
- **Process mapping**: rappresentazione dei processi business

1.4 Normalizzazione

- **Lean management**: eliminazione sprechi (waste)
- **Business Process Reengineering**: ottimizzazione processi

1.5 SQL

- **Business Intelligence**: analisi dati per decisioni strategiche
- **KPI dashboard**: indicatori di performance aziendale

---

2. Sistemi e Reti

2.1 Fondamenti Reti

Classifichiamo le reti per **estensione (grandezza)**:

- **LAN** (Local Area Network): reti locali (edificio, campus)
- **MAN** (Metropolitan Area Network): reti metropolitane
- **WAN** (Wide Area Network): reti geografiche
- **PAN** (Personal Area Network): reti personali (Bluetooth, NFC)

Per topologia (forma)

- **Bus**: tutti i nodi collegati a un cavo comune
- **Stella**: nodi collegati a un hub/switch centrale
- **Anello**: nodi collegati in circolo
- **Mesh**: collegamenti multipli tra nodi

Per prestazioni (Quality of Service - QoS) - Qualità

- **Larghezza di banda**: capacità di trasmissione (bps)
- **Latenza**: tempo di propagazione del segnale
- **Throughput**: velocità effettiva di trasferimento
- **Jitter**: variazione della latenza

Le prestazioni dipendono anche dal materiale!

Cavi in Rame (Economico ma più lento)

- **Twisted Pair** (UTP/STP): Cat5e, Cat6, Cat6a
- **Coassiale**: per reti cablaye e satellitari

Fibra Ottica (Luce) - Velocissima

- **Monomodale**: lunghe distanze, laser
- **Multimodale**: medie distanze, LED

Wireless (Senza fili - Access Point)

- **Wi-Fi**: IEEE 802.11 (a/b/g/n/ac/ax)
- **Bluetooth**: comunicazioni a corto raggio
- **Satellitare**: copertura globale

2.2 Modelli ISO-OSI e TCP-IP

Ci sono due macro-modelli:

- ISO/OSI = Teorico = Riferimento per applicazioni e programmi
- TCP/IP = Applicativo = Realmente usato nelle applicazioni

2.2.1 Modello OSI (7 livelli)

Livello 7 - Applicazione (Programma dell'utente)

- Interfaccia con l'utente e scopo dell'applicazione
- Protocolli: HTTP, SMTP, FTP, DNS

Livello 6 - Presentazione (Forma standard del dato)

- Crittografia, compressione, codifica (come salvare i dati)
- Formati: JPEG, MPEG, SSL/TLS

Livello 5 - Sessione (Mantieni attiva l'applicazione)

- Gestione delle sessioni di comunicazione
- Sincronizzazione, checkpoint

Livello 4 - Trasporto (Modi affidabili / non-affidabili)

- Comunicazione end-to-end
- Protocolli: TCP, UDP

Livello 3 - Rete (Instradamento - Arrivare a destinazione)

- Routing e indirizzamento logico
- Protocolli: IP, ICMP, OSPF, BGP

Livello 2 - Collegamento (Accesso al canale condiviso e poi correzione errori)

- Controllo accesso al mezzo, rilevamento errori
- Protocolli: Ethernet, Wi-Fi, PPP

Livello 1 - Fisico (Segnali e uso mezzi trasmissivi)

- Trasmissione bit su mezzo fisico
- Specifiche elettriche, ottiche, radio

2.2.2 Architettura TCP/IP (4 livelli)

Livello Applicazione (corrisponde a OSI 5-6-7)

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

Livello Trasporto (corrisponde a OSI 4)

- TCP: affidabile, orientato alla connessione
- UDP: veloce, senza connessione

Livello Internet (corrisponde a OSI 3)

- IP: indirizzamento e routing
- ICMP: messaggi di controllo

Livello Accesso alla Rete (corrisponde a OSI 1-2)

- Ethernet, Wi-Fi, PPP

2.2.3. Focus: Indirizzamento IP

2.2.3.1 Indirizzamento Classful

Classe A: 1.0.0.0 - 126.255.255.255

- Subnet mask: 255.0.0.0 (/8)
- 16.777.214 host per rete

Classe B: 128.0.0.0 - 191.255.255.255

- Subnet mask: 255.255.0.0 (/16)
- 65.534 host per rete

Classe C: 192.0.0.0 - 223.255.255.255

- Subnet mask: 255.255.255.0 (/24)
- 254 host per rete

Indirizzi Speciali

- **Loopback**: 127.0.0.0/8
- **Private**: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- **APIPA**: 169.254.0.0/16

2.2.3.2 Indirizzamento Classless (CIDR)

Subnet Mask Variabile

- Notazione CIDR: 192.168.1.0/24
- Supernetting: aggregazione di reti
- VLSM: Variable Length Subnet Mask

Subnetting

- Divisione di una rete in sottoreti più piccole
- Formula host: 2^(32-prefix) - 2
- Indirizzo rete: tutti bit host a 0
- Indirizzo broadcast: tutti bit host a 1

2.2.4. Focus Livello di Trasporto

2.2.4.1 Protocollo TCP (Affidabile)

Caratteristiche

- **Affidabile**: controllo errori e ritrasmissioni
- **Orientato alla connessione**: three-way handshake
- **Controllo di flusso**: window sliding

- **Controllo di congestione**: slow start, congestion avoidance

Three-Way Handshake

1. Client → Server: SYN
2. Server → Client: SYN-ACK
3. Client → Server: ACK

Disconnessione (Four-Way Handshake)

1. Client → Server: FIN
2. Server → Client: ACK
3. Server → Client: FIN
4. Client → Server: ACK

Formato Pacchetto TCP

- **Source/Destination Port**: 16 bit ciascuno
- **Sequence Number**: 32 bit
- **Acknowledgment Number**: 32 bit
- **Flags**: SYN, ACK, FIN, RST, PSH, URG

2.2.4.2 Protocollo UDP

Caratteristiche

- **Veloce**: overhead minimo
- **Senza connessione**: no handshake
- **Non affidabile**: no controllo errori
- **Applicazioni**: DNS, DHCP, streaming video

Formato Pacchetto UDP

- **Source/Destination Port**: 16 bit ciascuno
- **Length**: 16 bit
- **Checksum**: 16 bit

2.2.4.3 Porte e Socket

Porte Well-Known (0-1023)

- HTTP: 80, HTTPS: 443
- SMTP: 25, POP3: 110, IMAP: 143
- FTP: 20/21, SSH: 22, Telnet: 23
- DNS: 53, DHCP: 67/68

Socket

- Combinazione di IP + Porta
- Endpoint di comunicazione
- Esempio: 192.168.1.100:80

2.2.5. Focus Livello Applicativo

2.2.5.1 Protocollo HTTP/HTTPS

HTTP (HyperText Transfer Protocol)

- Protocollo request-response
- Metodi: GET, POST, PUT, DELETE, HEAD
- Status code: 2xx (successo), 4xx (errore client), 5xx (errore server)

HTTPS (HTTP Secure)

- HTTP + SSL/TLS
- Crittografia end-to-end
- Certificati digitali per autenticazione

2.2.5.2 Protocolli Email

SMTP (Simple Mail Transfer Protocol)

- Invio email (port 25, 587)
- Relay tra server email

POP3 (Post Office Protocol v3)

- Download email dal server (port 110)
- Email cancellate dal server

IMAP (Internet Message Access Protocol)

- Accesso email remote (port 143)
- Email rimangono sul server
- Sincronizzazione multi-device

2.2.5.3 Altri Protocolli

DNS (Domain Name System)

- Risoluzione nomi → indirizzi IP
- Gerarchia: root, TLD, domini
- Tipi record: A, AAAA, CNAME, MX, NS

FTP (File Transfer Protocol)

- Trasferimento file (port 20/21)
- Modalità attiva/passiva

DHCP (Dynamic Host Configuration Protocol)

- Assegnazione automatica IP
- Lease time, reservation, scope

2.3 Sicurezza nelle reti

2.3.4.1 Crittografia

La crittografia è la pratica di codificare informazioni per renderle illeggibili a persone non autorizzate, garantendo la riservatezza e l'integrità dei dati. Ne esistono due tipi:

Crittografia Simmetrica (1 Chiave sola condivisa tra Mittente - A e Destinatario - B)

- Stessa chiave per cifrare/decifrare
- Algoritmi: AES (Più sicuro), DES, 3DES
- Veloce ma problema distribuzione chiavi

Crittografia Asimmetrica (1 Chiave condivisa + Coppia chiavi private per A e B)

- Coppia chiavi: pubblica/privata
- Algoritmi: RSA (Numeri primi), DH, ECC
- Lenta ma risolve distribuzione chiavi

1. Algoritmo RSA (Rivest-Adleman-Shamir)

- Basato su fattorizzazione numeri primi
    1. Prodotto tra numeri primi "p", "q",
    2. Funzione di Eulero $\phi(n) = (p-1)*(q-1)$
    3. Prendiamo e, numero coprimo (primi tra di loro) con l'input
    4. Calcolo chiavi
- Chiave pubblica: (n, e)
- Chiave privata: (n, d)

2. Algoritmo Diffie-Hellman

- Scambio sicuro di chiavi su canale insicuro
- Basato su logaritmo discreto (scambio di chiavi con funzioni logaritmo / modulo)

2.3.4.2 Certificati Digitali e PKI

Un caso d'uso pratico dell'utilizzo di crittografia, abbastanza quotidiano è rappresentato dai seguenti.

Certificato Digitale (XML - PEC - SPID)

- Documento elettronico che lega identità a chiave pubblica
- Standard X.509
- Contiene: nome soggetto, chiave pubblica, CA, scadenza

> Collegamenti: TPS (PEC / XML come formato dati)

Certification Authority (CA)

- Ente che emette certificati (Es. Ministero dell'Interno)
- Catena di fiducia
- Root CA (Radice)→ Intermediate CA → End Entity (Finale)

> Esempio: Carta di identità (Ministero dell'Interno --> Comune di Padova --> Te) - Catena di fiducia

Firma Digitale - Usata dentro i certificati

- Autenticazione e non ripudio
- Hash del documento cifrato con chiave privata

2.3.4.3 SSL/TLS

Usato a livello sicurezza per crittografare una comunicazione (normalmente in ambito HTTP -> HTTPS oppure a livello trasporto)

SSL/TLS Handshake (Apertura connessione + Comunicazione sicura tra parti)

1. Client Hello (Messaggio di apertura)
2. Server Hello + Certificate (Destinatario risponde)

3. Key Exchange (Scambio chiavi e certificati)
4. Change Cipher Spec (Si certificano le parti delle comunicazioni)
5. Finished (Conclusione trasmissione)

2.3.4.4 Sicurezza Perimetrale

All'interno devi salvaguardare il *perimetro* (la porzione controllabile della rete) - ci sono vari modi per farlo.

Firewall - Può essere sia Hardware (Fisico = Router) oppure Software (Programma - Windows Firewall)

- **Packet Filtering**: controllo su header pacchetti
- **Stateful**: memoria delle connessioni
- **Application Gateway**: controllo applicativo

Varie tipologie di firewall

- **Router Filtrante**: liste di accesso di controllo su router
- **Single-Homed**: un'interfaccia di rete
- **Dual-Homed**: due interfacce separate
- **Host Bastione**: server sicuro in DMZ (Demilitarized Zone)

DMZ (Demilitarized Zone)

- Zona intermedia tra rete interna ed esterna
- Ospita server pubblici (web, mail, DNS)

Proxy Server (Server di controllo intermedio - Meccanismo di controllo esatto)

- **Forward Proxy**: nasconde client
- **Reverse Proxy**: nasconde server

2.3.4.5 VPN (Virtual Private Network)

VPN = Meccanismo di tunneling (nascondimento delle parti all'interno di una rete) - le parti dentro ad una rete sono schermate.

Protocolli VPN

- **IPSec**: cifratura a livello IP
- **L2TP**: tunneling livello 2
- **OpenVPN**: basato su SSL/TLS

2.4 Modello client-server e distribuito

Modello = Impronta logica di una rete Architettura = Impronta fisica di una rete = Impostazione esatta dei ruoli in una rete

2.4.1 Modello Client/Server

Caratteristiche

- Server: fornisce servizi
- Client: richiede servizi
- Comunicazione request-response

Vantaggi

- Centralizzazione risorse (client chiedono a server accessi vari)
- Sicurezza e controllo accessi
- Scalabilità verticale (espandiamo facilmente il numero di server a seconda di quanti client)

Svantaggi

- Single point of failure (Se ti va giù il server = Tutto va giù = Collo di bottiglia / Bottleneck)
- Collo di bottiglia server
- Costi hardware server

2.4.2 Sistemi Distribuiti

Distribuiti = Tutti hanno stessi ruoli.

Caratteristiche

- Elaborazione distribuita su più nodi (punti) della rete
- Trasparenza: location, failure, scaling
- Tolleranza ai guasti (in caso di errori, regge)

Modelli

- **Peer-to-Peer**: nodi equivalenti
- **Grid Computing**: risorse condivise
- **Cloud Computing**: servizi on-demand

2.5 Collegamenti Sistemi e Reti

STORIA

Fondamenti delle Reti

- **Evoluzione delle comunicazioni**: dal telegrafo ottico (Napoleone) alle reti digitali
- **Prima Guerra Mondiale**: importanza delle comunicazioni militari, sistemi di crittografia
- **Guerra Fredda**: sviluppo di ARPANET per resistere ad attacchi nucleari
- **Globalizzazione**: Internet come fattore di integrazione economica mondiale

Sicurezza delle Reti

- **Crittografia in guerra**: Enigma tedesca vs. Colossus britannico
- **Intelligence**: nascita dei servizi segreti moderni e intercettazioni
- **Controllo dell'informazione**: censura nei regimi totalitari vs. libertà digitale

Architetture Distribuite

- **Decentramento**: federalismo vs. centralismo negli stati moderni
- **Resistenza partigiana**: reti clandestine come modello di sistemi distribuiti

ITALIANO

Modello OSI/TCP-IP

- **Struttura letteraria**: i 7 livelli OSI come la struttura della Divina Commedia (Inferno-Purgatorio-Paradiso con suddivisioni)
- **Comunicazione letteraria**: mittente-messaggio-destinatario vs. client-server

Protocolli di Comunicazione

- **Linguaggio formale**: protocolli di rete come "grammatica" delle comunicazioni digitali
- **Standardizzazione linguistica**: nascita dell'italiano standard vs. protocolli standardizzati

Sicurezza

- **Cifrari letterari**: messaggi segreti nella letteratura (Foscolo, Pellico)
- **Censura**: controllo delle comunicazioni nei regimi vs. firewall

INGLESE

Terminologia Tecnica

- **Protocol**: HTTP, SMTP, FTP - linguaggio tecnico internazionale
- **Cybersecurity**: terminologia specifica (firewall, proxy, encryption)
- **Network administration**: documentazione e manuali tecnici

Evoluzione Digitale

- **Internet governance**: organismi internazionali (ICANN, IEEE, RFC)
- **Global connectivity**: inglese come lingua franca delle reti
- **Digital divide**: disparità nell'accesso alle tecnologie

MATEMATICA

Indirizzamento IP

- **Sistemi di numerazione**: binario, decimale, esadecimale
- **Calcoli VLSM**: 2^n per determinare numero host/subnet
- **Algebra booleana**: operazioni logiche AND, OR, NOT per subnet mask

Crittografia

- **Aritmetica modulare**: base dell'algoritmo RSA
- **Numeri primi**: fattorizzazione in RSA
- **Logaritmo discreto**: algoritmo Diffie-Hellman
- **Funzioni matematiche**: hash crittografici

Prestazioni di Rete

- **Statistica**: analisi del traffico, throughput medio
- **Teoria delle code**: modelli di congestione di rete
- **Serie numeriche**: convergenza dei protocolli di routing

INFORMATICA

Database e Reti

- **Database distribuiti**: replicazione, frammentazione, consistency
- **Client-server**: applicazioni web con database MySQL
- **Sicurezza dati**: crittografia per protezione database

Integrazione Applicativa

- **SQL via rete**: connessioni remote ai database
- **API RESTful**: comunicazione tra sistemi distribuiti
- **Web services**: SOAP, REST per integrazione applicazioni

TPSIT

Sviluppo Web

- **Stack LAMP**: integrazione Linux-Apache-MySQL-PHP
- **Protocolli applicativi**: HTTP/HTTPS per web applications
- **Sicurezza applicativa**: SQL injection, XSS, CSRF

Internet of Things

- **ESP32**: microcontrollori per IoT
- **Protocolli IoT**: MQTT, CoAP per comunicazioni M2M
- **Edge computing**: elaborazione distribuita su dispositivi

Normative

- **GDPR**: protezione dati in transito e a riposo
- **AI Act**: regolamentazione IA e sistemi autonomi
- **Cybersecurity**: framework di sicurezza europei

GPOI

Gestione di Progetto

- **Infrastruttura IT**: progettazione e implementazione reti aziendali
- **Risk management**: analisi rischi per la continuità operativa
- **SLA**: Service Level Agreement per servizi di rete

Economia Aziendale

- **TCO**: Total Cost of Ownership per infrastrutture di rete
- **ROI**: Return on Investment per aggiornamenti tecnologici
- **Outsourcing**: cloud vs. infrastruttura in-house

Organizzazione

- **Strutture distribuite**: organizzazioni virtuali e smart working
- **Business continuity**: piani di disaster recovery
- **Change management**: gestione cambiamenti tecnologici

---

3. TPS

3.1 Reti e protocolli

Le reti sono evolute da semplice comunicazione locale a interconnessione sempre più frequente e continua. La strutturazione ha preso sempre più conformità in *architetture di rete*:

Client/Server - Cliente/Servente

- **Client**: richiede servizi
- **Server**: fornisce servizi

- **Vantaggi**: centralizzazione, sicurezza, controllo
- **Svantaggi**: single point of failure, scalabilità limitata

Peer-to-Peer (P2P) - Pari a pari - Ognuno nella rete conta uguale = Consenso - Maggioranza

- Tutti i nodi sono equivalenti
- Condivisione diretta di risorse
- **Vantaggi**: scalabilità, resistenza ai guasti
- **Svantaggi**: sicurezza, controllo difficile

Architetture Ibride - Unisce le due possibilità

- Combinazione client/server e P2P
- Esempi: Skype, BitTorrent con tracker

Comunicazione di rete si basa su dei pilastri logici:

Internet - Modello generalissimo di collegamento tra tutto

- Rete globale di reti interconnesse
- Basata su protocollo TCP/IP
- Infrastruttura di comunicazione

World Wide Web (WWW) - Connessione continua tramite ipertesti / collegamenti

- Servizio che gira su Internet
- Basato su HTTP/HTTPS
- Documenti ipertestuali (HTML)

Differenze Fondamentali

- Internet = infrastruttura fisica e logica
- Web = servizio applicativo su Internet

3.2 Servizi di rete

I servizi cambiano a seconda del tipo di applicazione.

3.2.1 Applicazioni Aziendali e GDPR

Enterprise Resource Planning (ERP) - Gestionali

- Integrazione processi aziendali
- Database centralizzato

Customer Relationship Management (CRM)

- Gestione relazioni con clienti
- Analisi comportamenti e preferenze
- Marketing automation

Supply Chain Management (SCM)

- Gestione catena di fornitura
- Ottimizzazione logistica
- Tracciabilità prodotti

GDPR (General Data Protection Regulation) - Framework di sicurezza obbligatorio dal 2016 - Linea guida generale

- Regolamento UE 2016/679
- **Principi**: liceità, correttezza, trasparenza
- **Diritti**: accesso, portabilità, cancellazione
- **Obblighi**: privacy by design, data protection officer
- **Sanzioni**: fino al 4% del fatturato annuo

Esistono varie tipologie di servizi finanziari tramite web.

Home Banking

- Accesso online ai servizi bancari
- Autenticazione forte (2FA)
- Crittografia end-to-end

Pagamenti Digitali

- **POS**: Point of Sale
- **Mobile payment**: NFC, QR code

3.2.2 Crittografia (Uguale a Sistemi)

Crittografia Simmetrica

- Stessa chiave per cifratura/decifratura
- **Algoritmi**: AES-128/192/256, DES, 3DES
- **Vantaggi**: velocità
- **Svantaggi**: distribuzione chiavi

Crittografia Asimmetrica

- Coppia chiavi: pubblica/privata
- **Algoritmi**: RSA, ECC, Diffie-Hellman
- **Vantaggi**: no problema distribuzione chiavi
- **Svantaggi**: lentezza

Calcolo Chiavi RSA

1. Scegliere due primi p, q
2. Calcolare n = p × q
3. Calcolare φ(n) = (p-1)(q-1)
4. Scegliere e coprimo con φ(n)
5. Calcolare d: e × d ≡ 1 (mod φ(n))
6. Chiave pubblica: (n, e)
7. Chiave privata: (n, d)

3.2.3 Firma Digitale e PEC (Uguale a Sistemi)

Firma Digitale

- **Autenticazione**: identifica il firmatario
- **Integrità**: garantisce non alterazione
- **Non ripudio**: impedisce di negare la firma
- **Processo**: hash del documento + crittografia con chiave privata

Certificati Digitali

- Standard X.509
- Certificate Authority (CA)
- Catena di fiducia

PEC (Posta Elettronica Certificata)

- Valore legale equivalente a raccomandata A/R
- Ricevute di consegna e accettazione
- Timestamp e firma digitale
- Conservazione sostitutiva

3.3 Server per reti e web

La rete comunica in modo standard seguendo vari protocolli:

3.3.1 Servizi di Rete Fondamentali

DNS (Domain Name System) - Risoluzione degli indirizzi IP in parti raggiungibili a gerarchia

- Risoluzione nomi → indirizzi IP
- **Gerarchia**: root servers, TLD, domini (.it / .com)
- **Funzionamento**: richiesta ricorsiva alla gerarchia dei server per arrivare a una destinazione

DHCP (Dynamic Host Configuration Protocol) - Routing/instradamento dinamico (se un dispositivo entra, si connette da solo)

- Assegnazione automatica configurazione IP
- **Parametri**: IP, subnet mask (maschera di sottorete) - subnetting, gateway, DNS

3.2 Server Web

Apache HTTP Server - Open source - Gratuito

- Web server open source più diffuso
- **Moduli**: Funziona a parti frammentate

3.3 Server Email

**Componenti Sistema Email - Posta elettronica - Mittente / corriere / destinatario **

- **MTA** (Mail Transfer Agent): invio/routing email
- **MDA** (Mail Delivery Agent): consegna email
- **MUA** (Mail User Agent): client email

Protocolli Email - Standard in trasmissione

- **SMTP**: invio email (port 25, 587, 465)
- **POP3**: download email (port 110, 995)
- **IMAP**: accesso email remote (port 143, 993)

3.4 Sicurezza Perimetrale

NAT (Network Address Translation) - Nascondere indirizzi IP all'esterno

- Traduzione indirizzi privati ↔ pubblici
- **SNAT**: Source NAT (uscita)
- **DNAT**: Destination NAT (port forwarding)
- **PAT**: Port Address Translation

Proxy Server - Server intermedi di controllo della trasmissione

- **Forward proxy**: nasconde client ai server
- **Reverse proxy**: nasconde server ai client
- **Funzioni**: caching (salvataggio dati a seconda del fine), filtering (filtraggio comunicazioni), load balancing (smarcare traffico pacchetti)

Firewall - Controllo hardware (HW) e software (SW)

- **Packet filtering**: controllo header pacchetti
- **Stateful inspection**: memoria delle connessioni
- **Application gateway**: controllo applicativo
- **Next-gen firewall**: DPI, IPS, antivirus

3.5 Controllo degli Accessi

In una rete c'è il principio del privilegio minimo - chi entra nella rete deve avere meno permessi possibile solitamente. Esistono varie modalità di gestione dati.

Modelli di Controllo

- **DAC** (Discretionary Access Control): ciascun utente decide le proprie possibilità
- **MAC** (Mandatory Access Control): policy centralizzate - amministratore di rete decide per tutti

Autenticazione

- **Fattori**: something you know/have/are
- **Single Sign-On (SSO)**: accesso unificato
- **Multi-Factor Authentication (MFA)**: più fattori
- **Protocolli**: Kerberos, LDAP, SAML, OAuth