www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Scheda 1

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 1 → INFORMATICA

COS'È L'INFORMATICA?

Insieme di processi e tecnologie che permettono di creare, raccogliere, elaborare, salvare e diffondere le informazioni
- Sistemi di Elaborazione dell'Informazione (computer)

ETIMOLOGIA
La parola "informatica" deriva dal francese information électronique automatique e indica l'insieme delle attività legate all'elaborazione automatica delle informazioni
- a seconda della lingua, anche il nome del computer cambia: "elaboratore" (ragionamento e calcolo); "ordinateur" (organizza i dati) e "computer" (eseguire calcoli, come una calcolatrice)

HARDWARE e SOFTWARE

Ogni computer è formato da due componenti fondamentali: l'hardware e il software
- hardware → la parte fisica, visibile e tangibile del computer: lo schermo, la tastiera, la stampante, il mouse
- software → la parte logica: tutti quei programmi e istruzioni che fanno funzionare l'hardware, come i sistemi operativi

Per capirlo meglio, si può pensare al corpo umano: l'hardware è il corpo, mentre il software è la mente che lo fa muovere

RUOLO DEI DATI

I dati sono la materia prima dell'informatica
- semplici (numeri, caratteri, date)
- complessi (immagini, grafici, filmati)

I computer moderni sono capaci di gestire dati complessi con grande efficienza: raccolgono informazioni, le elaborano, le salvano nella memoria, le trasmettono ad altri dispositivi e le utilizzano per svolgere funzioni utili
- in pratica, ogni giorno ci affidiamo all'informatica senza neanche rendercene conto

APPLICAZIONI INFORMATICA

L'informatica è presente in ogni ambito: medicina, istruzione, ingegneria, arte, intrattenimento e lavoro
Tra i settori dove è più utilizzata ci sono:
- la gestione aziendale
- la formazione
- i database
- il mondo dello svago (come videogiochi e piattaforme di streaming)

SISTEMA INFORMATIVO

Nel contesto aziendale, è importante distinguere tra sistema informativo aziendale e sistema informatico
- sistema informativo aziendale → insieme di tutti i dati e tutti i processi che riguardano l'archiviazione
- sistema informatico → insieme delle risorse tecnologiche

Nelle imprese, l'informatica è uno strumento essenziale per svolgere molte attività quotidiane; per gestire transazioni con clienti e fornitori, per fare analisi finanziarie, per la produzione di documenti (office automation), ma anche per supportare il processo decisionale con sistemi chiamati DSS (Decision Support Systems)
- impiegata anche per fare data mining, ovvero l'analisi approfondita dei dati per trarre informazioni utili

In ambito industriale, l'informatica è usata in due modi principali:
- CAD (Computer-Aided Design) → progettare oggetti, disegni e modelli, spesso in 3D
- CAM (Computer-Aided Manufacturing) → controllare robot o macchine che producono oggetti (catena di montaggio)

ELENCO APPLICAZIONI

- home banking → gestire conti bancari, fare bonifici e controllare investimenti da casa
- e-government → servizi pubblici sono diventati digital (riduce l'uso della carta, l'efficienza e trasparenza ai cittadini)
- medicina e salute → gestire i dati clinici, di supportare i medici nella diagnosi, e di fornire terapie personalizzate
- telelavoro → e-job (domiciliare, mobile)
- istruzione e formazione → digitalizzazione attività scolastiche, CBT (Computer-Based Training) e l'e-learning
- commercio elettronico → nascita dell'e-commerce (vendere e comprare online con negozi virtuali)
- sistema di navigazione globale → GPS (tecnologia del sistema di navigazione globale)

Digital Divide (impossibilità d'avvicinarsi alla tecnologia)
- riutilizzo dell'hardware (trashware), software libero

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

STORIA DELL'INFORMATICA

La storia dell'informatica è affascinante e ricca di innovazioni:

- Nel 2400 a.C. si usava l'abaco per contare.
- Nel 1642, Pascal costruì la prima calcolatrice meccanica.
- Nel 1833, Charles Babbage progettò un computer meccanico.
- Ada Lovelace, nel 1843, scrisse il primo algoritmo: è considerata la prima programmatrice della storia.
- Verso il 1890, vennero usate le schede perforate per registrare i dati.
- Nel 1945, l'architettura di von Neumann pose le basi per i computer moderni.
- Il primo computer elettronico nacque nel 1946: enorme, pesava 30 tonnellate, consumava tantissimo ed era fragile
- Nel 1952, l'UNIVAC riuscì addirittura a prevedere il risultato delle elezioni negli Stati Uniti
- Tra gli anni '60 e '90 arrivarono tante novità: le calcolatrici tascabili, la nascita di Internet (con ARPANET), i personal computer (PC), i CD, le stampanti laser, i cellulari, il wireless, i DVD

IL FUTURO DELL'INFORMATICA

L'evoluzione dell'informatica continua, seguendo alcune tendenze molto chiare:

- miniaturizzazione: i computer diventano sempre più piccoli (si pensi agli smartwatch)
- aumento di velocità: tutto diventa più rapido ed efficiente.
- riduzione dei costi: i dispositivi tecnologici sono più accessibili.

L'informatica pervasiva: ormai presente ovunque, dai forni alle automobili, dai televisori agli elettrodomestici.
Convergenza: dispositivi non servono per vedere contenuti o telefonare, ma anche per navigare su Internet

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 2 → INFORMAZIONE

INFORMAZIONI e BIT

Un bit rappresenta la più piccola unità di informazione, ed è in grado di assumere solamente due valori: 0 oppure 1
- con un solo bit è possibile rappresentare due stati distinti, come ad esempio acceso/spento o vero/falso

I segnali analogici sono continui e possono assumere infiniti valori, ma risultano molto più sensibili ai disturbi e alle interferenze
I segnali digitali lavorano solo con due stati (0 e 1) e per questo motivo sono più affidabili, perché più resistenti alle interferenze

Tutte le informazioni che usiamo con i computer devono essere convertite in bit per poter essere memorizzate ed elaborate
- un processo chiamato codifica, che trasforma i dati reali in formato binario, e un processo opposto chiamato decodifica, che restituisce i dati nella loro forma comprensibile

Le informazioni si possono dividere in due grandi categorie:
- informazioni tradizionali, come numeri e testi, sono quelle più classiche.
- informazioni multimediali, come immagini (che possono essere vettoriali o bitmap), audio e video

Tutti questi dati, indipendentemente dalla loro forma, vengono rappresentati in bit.

Un gruppo di 8 bit prende il nome di byte → esistono poi dei multipli del byte usati per esprimere quantità più grandi di dati
- kilobyte (KB) equivale a 1024 byte
- megabyte (MB) a 1024 kilobyte

con unità più grandi come gigabyte (GB), terabyte (TB) e petabyte (PB).

SISTEMI NUMERICI

I sistemi numerici utilizzati per rappresentare i dati si dividono in due tipi: il primo è quello non posizionale, come ad esempio i numeri romani, in cui il valore delle cifre non dipende dalla loro posizione mentre il secondo è il sistema posizionale, come quello decimale, in cui ogni cifra ha un peso che dipende dalla sua posizione all'interno del numero

DA SISTEMA DECIMALE A SISTEMA BINARIO

Per calcolare il valore di un numero in un sistema posizionale si usa una formula: $V(N) = d_3 \times r^3 + d_2 \times r^2 + d_1 \times r^1 + d_0 \times r^0$
- dove r rappresenta la base del sistema (es: nel sistema decimale, r è pari a 10, e le cifre variano da 0 a 9)
- prendendo il numero 8427, possiamo esprimerlo come $8\times10^3 + 4\times10^2 + 2\times10^1 + 7\times10^0$

DA SISTEMA BINARIO A SISTEMA DECIMALE

Nel caso del sistema binario, la base r è uguale a 2, e le cifre ammesse sono solo 0 e 1
- esempio classico è il numero binario 1011_2, che corrisponde al valore decimale $1\times2^3 + 0\times2^2 + 1\times2^1 + 1\times2^0$, cioè 11_{10}

ALTRE BASI NUMERICHE

Oltre ai sistemi decimale e binario, esistono anche altre basi numeriche
- sistema ottale, base 8 e usa le cifre da 0 a 7.
- sistema esadecimale, base 16 e le cifre da 0 a 9 accompagnate dalle lettere A a F per i valori da 10 a 15

BIT NECESSARI

Per rappresentare un valore massimo X, è necessario usare un certo numero di bit n, calcolabile come $n = \log_2(X)$
- più grande è il valore X, maggiore sarà il numero di bit richiesto per rappresentarlo

Quando si cerca di rappresentare un numero troppo grande con pochi bit, si rischia di generare un errore di overflow.
- ad esempio, con soli 4 bit, è possibile rappresentare al massimo il numero 15 (cioè $2^4 - 1$)

BIT, BYTE E WORD

Il bit è l'unità base di informazione. Un insieme di 8 bit forma un byte. Un gruppo di più bit, chiamato word, viene usato dal processore per elaborare dati. Le word possono avere dimensioni di 16, 32 o 64 bit
- più grande è la word, maggiore sarà la quantità di dati e indirizzi che il computer può gestire in una sola operazione

CODIFICA DEI CARATTERI

Per rappresentare testi, il computer utilizza una tabella di codifica. Una delle più diffuse è la codifica ASCII, che usa 7 bit per rappresentare 128 simboli diversi. Esiste anche una versione estesa chiamata ASCII esteso, che usa 8 bit per codificare fino a 256 simboli, includendo anche caratteri speciali e lettere accentate
- uniforme, che serve per includere caratteri speciali (come lettere accentate, simboli di lingue non latine)
- usa 16 bit: può rappresentare 65.536 simboli diversi

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 3 → SOFTWARE

SOFTWARE → Il software consente al sistema di elaborazione di funzionare e svolgere le sue attività
Si può dividere in due grandi categorie:

- software di sistema, che comprende i sistemi operativi e i linguaggi di programmazione
- software applicativo, i programmi che utilizzi per lavorare, studiare o divertirti (un elaboratore di testi o un videogioco)

SISTEMI OPERATIVI (SO)

I sistemi operativi sono programmi fondamentali che permettono al computer di funzionare e fanno sì che ogni parte dell'hardware (memoria, processore, file, stampanti) venga gestita correttamente, spesso senza che l'utente se ne accorga

- grazie al sistema operativo puoi aprire un programma, salvare un documento o inviare un file alla stampante: tutte queste operazioni sono possibili proprio perché il SO coordina ogni risorsa del computer

PROGRAMMI APPLICATIVI

Possiamo pensare al computer come a un attore che appena riceve un "copione" (un programma) può iniziare a recitare

- i programmi applicativi sono proprio questi copioni: permettono al computer di eseguire compiti specifici, come scrivere un testo o calcolare tabelle → gli strumenti concreti che l'utente utilizza per portare a termine un'attività

PROGRESSO DELL'INFORMATICA

L'evoluzione dell'informatica è un processo graduale: le nuove tecnologie non si diffondono immediatamente, ma richiedono tempo per essere comprese e adottate su larga scala; le innovazioni si manifestano su tre diversi livelli:

- nell'hardware, ossia i componenti fisici del computer
- sistemi operativi, che diventano sempre più completi
- programmi applicativi, che offrono funzionalità sempre più sofisticate

ALTRI TIPI DI PROGRAMMI

Oltre ai programmi, esistono molte altre tipologie di software: intrattenimento, istruzione, consultazione e utilità

EVOLUZIONE DEI SISTEMI OPERATIVI

Negli anni '50 non esistevano i sistemi operativi, al loro posto c'erano operatori umani che gestivano manualmente le attività del computer. Oggi i SO si occupano di controllare l'intero funzionamento del sistema, gestendo ogni risorsa

INTERFACCE UTENTE

L'interfaccia utente è ciò che vedi sullo schermo e usi per interagire con il computer. Può essere a caratteri, dove i comandi vengono scritti tramite tastiera, oppure grafica → chiamata GUI (Graphical User Interface).

INTERFACCE GRAFICHE UTENTE (GUI)

Le prime GUI sono nate nei laboratori Xerox, ma oggi sono ampiamente diffuse. Sistemi come Windows, macOS e Linux, offrono interfacce intuitive e facili da usare, proprio perché trasformano azioni complesse in semplici clic

GUI: CARATTERISTICHE COMUNI

Le interfacce grafiche condividono alcune caratteristiche fondamentali, permettono l'interazione tramite finestre e l'uso del mouse per cliccare e navigare. Seguono il principio del WYSIWYG ("What You See Is What You Get") e inoltre, offrono comandi standard comuni a molte applicazioni, come copia, incolla, salva, stampa

SISTEMI OPERATIVI (SO)

Con il tempo, i sistemi operativi si sono arricchiti di nuove funzioni

- oggi gestiscono anche la connessione a Internet, oltre a funzioni audio e video
- quando una funzionalità diventa di uso comune, viene spesso integrata nel sistema operativo

FUNZIONI DEL SO

Il sistema operativo ha diversi compiti importanti: gestire le risorse del computer, controllare le operazioni, determinare dove memorizzare dati e programmi, coordinare la comunicazione e gestisce l'interazione tra utente e applicazioni

RUOLO DEL BIOS

BIOS → BASIC INPUT OUTPUT SYSTEM, ossia il primo software che viene eseguito quando accendi il computer

- un chip della scheda madre e ha il compito di interpretare tastiera e schermo, oltre a controllare le porte e i collegamenti hardware; in altre parole rappresenta il ponte tra l'hardware e il software

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

INTERPRETE DEI COMANDI

All'interno del sistema operativo c'è un interprete dei comandi, ovvero quella parte del software che capisce cosa vuoi fare
- per esempio, quando fai doppio clic su un'icona, è l'interprete che comprende l'azione e avvia il programma

SISTEMI MULTITASKING

I computer una volta erano in grado di eseguire un solo programma alla volta. Oggi è normale usare più applicazioni contemporaneamente; questo è possibile perché il sistema operativo gestisce il tempo del processore tra le varie attività

SISTEMI MULTITHREADING

All'interno di un singolo programma, il computer può svolgere più operazioni allo stesso tempo
- ad esempio, di un programma di scrittura che controlla l'ortografia, salva automaticamente e stampa un documento allo stesso tempo → multithreading ed è ciò che rende i programmi moderni più veloci e reattivi

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 4 → CALCOLATORI

ARCHITETTURA CALCOLATORI

Calcolatore è un sistema → oggetto costituito da parti che interagiscono, cooperando, al fine di ottenere un comportamento
Studiare l'architettura di un sistema vuol dire:

- individuare ciascun componente del sistema
- comprendere i principi generali di funzionamento di ciascun componente
- comprendere come i vari componenti interagiscono tra di loro

HARDWARE → la struttura fisica del calcolatore, costituita da componenti elettronici ed elettromeccanici

- l'unità centrale di elaborazione (CPU) e la memoria

SOFTWARE → l'insieme dei programmi che consentono all'hardware di svolgere dei compiti utili

- il software comprende il software di base (tra cui il sistema operativo) e il software applicativo

BUS e MASTER-SLAVE

Il bus è una linea a cui sono contemporaneamente connesse le unità del calcolatore e che consente il trasferimento di dati

- Problema: contesa su un mezzo condiviso
- Soluzione: CPU = master, periferiche = slave

PREGI: Semplicità (1 sola linea di connessione), estendibilità (nuovi dispositivi), standardizzabilità (definizione di normative)
DIFETTI: lentezza (inibisce la parallelizzazione), limitata capacità, sovraccarico della CPU

TIPI di BUS

- Bus dati: utilizzato per trasferire dati (es. fra memoria e CPU, fra CPU e interfacce di I/O)
- Bus indirizzi: che identifica la posizione delle celle di memoria un cui la CPU va a scrivere o leggere
- Bus di controllo: in cui transitano i segnali di controllo

INSTRUCTION SET ARCHITECTURE (ISA)

L'Instruction Set Architecture, o ISA, rappresenta l'interfaccia tra l'hardware e il software. In altre parole, è il "linguaggio" che il processore capisce per poter eseguire le istruzioni di un programma

L'ISA stabilisce diversi aspetti fondamentali: definisce quali istruzioni sono disponibili e determina come sono strutturati i dati e i registri interni al processore; e specifica come si accede alla memoria

- questo insieme di regole e definizioni include le operazioni che la CPU può eseguire, i tipi di dati che può gestire, le diverse modalità di indirizzamento (cioè i modi per individuare i dati in memoria) e l'elenco dei registri accessibili

Grazie a queste caratteristiche, l'ISA è utile sia per progettare i processori, sia per costruire i compilatori, ovvero i programmi che traducono il codice scritto dai programmatori in istruzioni eseguibili

ELEMENTI di una CPU

UNITÀ CONTROLLO	UNITÀ ARITMETICO-LOGICA	REGISTRI
Legge le istruzioni dalla memoria e ne determina il tipo	Esegue le operazioni necessarie per eseguire le istruzioni	Memoria ad alta velocità Determina il parallelismo della CPU (registri generici e registri specifici)

REGISTRI di CPU

IR	PC	MAR	MDR	PSW	R0, R1, Rn
contiene istruzione	tiene traccia	locazione memoria	memoria → CPU	info programma	registri generali

ESECUZIONE ISTRUZIONI

CICLO FETCH-DECODE-EXECUTE → ogni istruzione che il processore esegue passa attraverso un ciclo di esecuzione

- fetch: consiste nel prelevare l'istruzione dal registro istruzioni (IR) e incrementa il program counter (PC)
- decode: determina il tipo dell'istruzione corrente
- execute: viene eseguita l'operazione

Questo processo si ripete in continuazione ed è il "ciclo vitale" di ogni comando all'interno del processore

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

FORMATO DELLE ISTRUZIONI → Ogni istruzione ha almeno due elementi fondamentali: l'opcode, che specifica quale operazione deve essere eseguita, e gli operandi, cioè i dati o i registri su cui lavorare

TIPI DI ISTRUZIONI → Le istruzioni si possono classificare in base alla loro funzione

- istruzioni aritmetiche: come add, sub, mul e div, che si occupano dei calcoli matematici
- istruzioni logiche: come and, or, not, servono per operazioni sui bit
- istruzioni di controllo: permettono di gestire i salti condizionati nel programma, come beq (branch if equal) o j (jump)
- istruzioni di memoria: come lw (load word) e sw (store word), servono a leggere o scrivere dati nella memoria

Ogni gruppo di istruzioni ha un ruolo specifico all'interno dell'esecuzione del programma

TIPI DI INDIRIZZAMENTO

Un altro aspetto chiave dell'ISA è il modo in cui il processore trova i dati: questo si chiama indirizzamento

- nel modo immediato, il valore da usare è già contenuto nell'istruzione stessa
- nel modo diretto, l'istruzione indica esattamente l'indirizzo di memoria da cui leggere o scrivere
- nel modo indiretto, invece, usa un registro che contiene l'indirizzo della memoria da accedere
- nel modo indicizzato, prevede che si sommi un certo valore a un registro per ottenere l'indirizzo finale

CISC e RISC

CISC → architettura CISC (Complex Instruction Set Computing) offre un insieme di istruzioni, anche complesse

- istruzioni potenti semplificano la programmazione
- riduce il gap tra linguaggio di macchina e linguaggio di alto livello
- uso efficiente della memoria

RISC → architettura RISC (Reduced Instruction Set Computing) è basata su un numero limitato di istruzioni semplici

- memorie più veloci ed economiche
- comportamento dei programmi
- conviene costruire processori molto veloci

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 5 → CPU

REGISTRI SPECIALI DEL PROCESSORE

All'interno della CPU ci sono delle piccole memorie chiamate registri speciali, ognuna con un ruolo ben preciso

- Program Counter (PC) → bit del registro PC indicano in RAM l'istruzione da eseguire
- Registro Istruzione (IR) → bit del registro IR indicano l'istruzione appena letta dalla RAM e da decodificare
- Registro Indirizzi Memoria (MAR) → bit del registro MAR in RAM il cui contenuto deve essere letto dal processore

Esistono altri registri fondamentali:

- Registro Dati Memoria (MDR) → i bit MDR indicano una copia del contenuto di una parola in RAM letto dal processore o il valore di bit che devono essere scritti in RAM dal processore
- Registro di Stato (SR) → i bit SR indicano che una condizione si è verificata a seguito dell'esecuzione di un'istruzione

REGISTRI DI USO GENERALE

Il processore dispone anche di registri di uso generale, che possiamo immaginare come una memoria a breve termine

- utilizzati per salvare dati temporanei, contenere numeri su cui eseguire operazioni e memorizzare i risultati finali
- sono strumenti versatili e fondamentali per il funzionamento efficiente del processore

I registri generali sono usati per l'esecuzione di istruzioni memorizzando, ad esempio:

- contenuto di una parola di memoria letto dal processore
- risultato di un'elaborazione sul contenuto di uno o più registri
- operandi di un'istruzione aritmetica

ALU: UNITÀ ARITMETICO-LOGICA

All'interno della CPU troviamo anche la ALU, l'Unità Aritmetico-Logica → costituita da un insieme di circuiti in grado di svolgere le operazioni di tipo aritmetico e logico, leggere i dati contenuti nei registri e esegue operazioni e memorizza il risultato

- eseguire i calcoli, come somme o sottrazioni, ma anche di effettuare confronti logici

Per svolgere queste operazioni, la ALU utilizza i registri generali, da cui prende i dati su cui lavorare e dove poi salva i risultati

ISTRUZIONI

Il processore può eseguire molte azioni diverse, seguendo un insieme di istruzioni base. Ad esempio, può leggere o scrivere dati nella RAM, eseguire operazioni matematiche come somme, invertire o spostare i bit all'interno di un valore binario

- il processore funziona seguendo una lista di comandi molto semplici, scritti in un linguaggio binario

Le istruzioni che un processore può eseguire sono anch'esse rappresentate in formato digitale

- si sceglie di usare un certo numero di bit e si fa corrispondere ad un'operazione o un registro di una configurazione

A seconda dello spazio di indirizzamento, si sceglie di usare un certo numero di bit e si fa corrispondere ad un indirizzo una configurazione, le istruzioni sono rappresentate in formato digitale e mantenute all'interno della RAM

COME SONO CODIFICATE LE ISTRUZIONI

Ogni istruzione che il processore esegue è rappresentata da una sequenza di bit (assegnato un codice binario specifico)

- l'operazione ADD potrebbe essere rappresentata da 1011
- il registro R3 potrebbe corrispondere al codice 0011

L'intero programma che il computer esegue è costituito da una lunga sequenza di bit codificati, interpretati dal processore

ESEMPIO DI CODIFICA

Per chiarire meglio, consideriamo l'istruzione ADD R3, R8, R13. Se codifichiamo l'operazione ADD con 1011, R3 con 0011, R8 con 1000 e R13 con 1101, allora l'intera istruzione verrà scritta nella memoria come una sequenza di 16 bit:

- 1011 0011 1000 1101

Questa rappresentazione binaria permette al processore di capire cosa fare, con quali registri e in quale ordine

IL BUS

Una domanda importante è come comunicano tra loro le varie componenti del computer: la CPU, la RAM e le periferiche? Attraverso il bus, un insieme di fili, o linee di comunicazione, che collegano tutte le parti del sistema

- trasportare indirizzi (dove leggere o scrivere), dati (contenuto vero e proprio) e comandi (istruzione da eseguire)

Un buon esempio per capire cos'è il bus è quello dell'autostrada: è come una rete stradale con corsie condivise, dove viaggiano contemporaneamente i dati e i comandi, collegando tutte le componenti tra loro

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 6 → ALGEBRA BOOLEANA

L'algebra booleana è un sistema logico ideato da George Boole nel XIX secolo, le sue variabili possono assumere due valori:

- VERO: rappresentato come 1, true o acceso
- FALSO: che corrisponde a 0, false o spento

FUNZIONI BOOLEANE

Le funzioni booleane sono funzioni logiche che utilizzano variabili booleane come input

- es: F(x, y, z), restituisce un risultato booleano solo 1 (vero) oppure 0 (falso), a seconda dei valori delle variabili

Nell'algebra booleana esistono due costanti fondamentali: 0, che rappresenta il valore falso, e 1, che rappresenta il valore vero

TABELLA DELLA VERITÀ: rappresentare visivamente tutte le combinazioni possibili di input e i corrispondenti risultati di una funzione logica si utilizza la tabella della verità (es: se una funzione ha 3 variabili di input, esisteranno 8 combinazioni diverse)
FUNZIONI COMPLETAMENTE SPECIFICATE → se per ogni combinazione di input è indicato un valore determinato di output
FUNZIONI NON COMPLETAMENTE SPECIFICATE → se alcune combinazioni non hanno un valore della funzione definito

TIPI DI OPERATORI

Gli operatori logici sono strumenti che permettono di manipolare variabili o costanti booleane, possono essere di due tipi:

- monadici: se agiscono su un solo valore di input (come l'operatore NOT)
- diadici: se agiscono su due valori (come AND o OR)

Gli operatori booleani vengono spesso rappresentati con simboli specifici: NOT si scrive con una barra sopra la variabile ($\bar{}$), AND si rappresenta con un punto (·), OR con il simbolo più (+), e XOR con il simbolo ($\oplus$)

OPERATORE NOT

operatore NOT ha il compito di invertire il valore della variabile → se l'input è 0, l'output sarà 1; se l'input è 1, l'output sarà 0

OPERATORE AND

operatore AND → restituisce vero 1 solo se entrambi gli input sono veri, in ogni altro caso, il risultato sarà 0

OPERATORE OR

operatore OR → il risultato è vero se almeno uno dei due input è vero (es: 0 OR 1 e 1 OR 1 danno come risultato 1)

OPERATORE XOR

operatore XOR → restituisce 1 solo se uno dei due valori è vero, ma non entrambi (es: 0 XOR 1 è 1, mentre 1 XOR 1 è 0)

OPERATORI UNIVERSALI

Utilizzando solo gli operatori AND, OR e NOT è possibile costruire qualsiasi funzione logica. Tuttavia, anche NAND e NOR, sono detti operatori universali, perché permettono comunque di ottenere ogni funzione logica combinandoli nel modo giusto

OPERATORE NAND

operatore NAND → restituisce 0 solo nel caso in cui entrambi gli input siano 1, mentre per le altre combinazioni restituisce 1

OPERATORE NOR

operatore NOR → restituisce 1 solo se entrambi gli input sono 0. In tutti gli altri casi, il risultato sarà 0

ESPRESSIONI LOGICHE

Le espressioni logiche sono formule composte da variabili booleane, costanti e operatori

- esempio di espressione → T = $\bar{a}\cdot b + a\cdot\bar{b}$, dove si combinano AND, OR e NOT

PRECEDENZA DEGLI OPERATORI: priorità d'esecuzione
operatore AND (·) ha una priorità più alta rispetto all'operatore OR (+), viene eseguito per primo

PROPRIETÀ DELL'ALGEBRA BOOLEANA

L'algebra booleana possiede diverse proprietà fondamentali

- idempotenza dice che una variabile AND (X·X = X) e OR (X + X = X)
- complementazione prevede che una variabile OR (X + $\overline{X}$ = 1) e AND il suo complemento dà 0 (X·$\overline{X}$ = 0)
- proprietà commutativa, di assorbimento e distributiva, che regolano la riorganizzazione delle espressioni
- proprietà associativa, che consente di cambiare la posizione delle parentesi senza modificare il risultato
- le leggi di De Morgan, che permettono di trasformare negazioni di espressioni complesse

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 7 → ALGORITMI

ALGORITMO → una sequenza ordinata di passaggi che consente di risolvere un problema a partire da determinati dati iniziali

- ogni singolo passo è semplice e ben definito, così da non lasciare ambiguità su cosa fare

PROPRIETÀ DI UN ALGORITMO

Per essere considerato efficace, un algoritmo deve avere tre caratteristiche fondamentali:

- finitezza: composto da un numero finito di passi elementari; le operazioni sono eseguite un numero finito di volte
- non ambiguità: i risultati non variano in funzione della macchina/persona che esegue l'algoritmo (deterministico)
- realizzabilità: deve essere eseguibile con le risorse a disposizione

RAPPRESENTAZIONE ALGORITMI

Necessario far riferimento a dei formalismi che:

- non introducano ambiguità e siano riconosciuti ed interpretati allo stesso modo da un generico esecutore
- permettano di rappresentare in modo efficace un algoritmo

Costituiscano un utile strumento per poi poter passare alla fase di codifica in un linguaggio di programmazione

- rappresentazione grafica e testuale

OPERAZIONI BASE DI UN ALGORITMO

Ogni algoritmo è costruito attorno ad alcune operazioni fondamentali

- istruzioni di input/output
- istruzione di assegnamento
- valutazione espressioni (esecuzione di calcoli)
- strutture di controllo (prendere decisioni sul passo da eseguire)

FLOW CHART: SIMBOLI

Nei diagrammi di flusso, ogni tipo di operazione è rappresentata da un simbolo specifico:

INPUT/OUTPUT

Nel pseudocodice, le istruzioni di input/output sono scritte con comandi come leggi A o B

- istruzioni inserite all'interno di un parallelogramma

ASSEGNAMENTO

L'istruzione di assegnamento permette di assegnare un valore ad una variabile

- usato il simbolo = per indicare l'istruzione di assegnamento (sarà lo stesso usato nel linguaggio C)

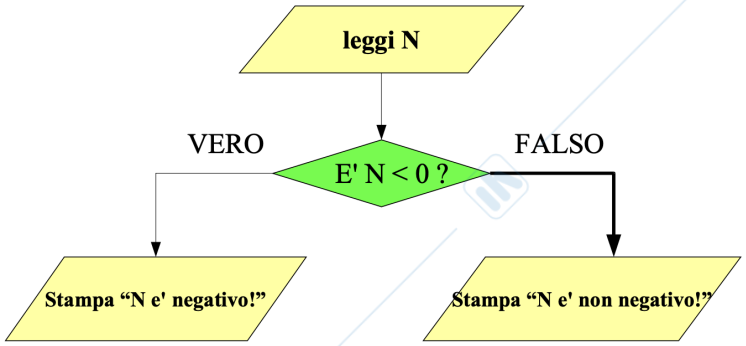
Un'assegnazione consiste nel salvare un valore in una variabile, che può essere vista come un "contenitore"

- fondamentale che ogni variabile venga inizializzata, cioè riceva un valore iniziale

A prima vista, un'istruzione come A = A + 1 potrebbe sembrare un errore. In realtà, significa che si calcola il nuovo valore di A sommando 1 al valore attuale, e poi si sovrascrive il vecchio valore con il nuovo.

- l'esecutore è in grado di valutare espressioni aritmetiche ed assegnarle alla variabile specificata nella parte sinistra

STRUTTURA DI SELEZIONE



www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 8 → RETI COMPUTER

RETE → Le reti sono un componente fondamentale per la realizzazione di un sistema informativo
- senza la rete i computer non possono comunicare fra loro e le modalità di decentralizzazione dell'elaborazione dell'informazione sono costituite da: collegamento di terminali ad un computer centrale, trasferimento di file

Le reti rendono le attività quotidiane più comode ed efficienti

Si parla di rete di computer quando effettivamente più sistemi di elaborazione autonomi (computer) possono dialogare fra loro scambiandosi informazioni attraverso un mezzo fisico di connessione e quando tale meccanismo di comunicazione e di scambio è replicabile su più computer, senza dipendere dalla specificità delle due macchine che comunicano fra loro
- interconnettere fra loro reti diverse, anche mediante mezzi trasmissivi eterogenei

COME SI REALIZZA una RETE

Una rete si compone di:
- componenti fisiche → computer, router, switch, cavi, onde radio.
- componenti software → programmi (integrati nel sistema operativo) che gestiscono la comunicazione tra i dispositivi.

Ogni computer ha un'interfaccia di rete che consente lo scambio di dati attraverso un canale fisico
- il software client si collega a un server, e la comunicazione è gestita dai rispettivi sistemi operativi

PACKET SWITCHING

I dati in rete sono suddivisi in pacchetti, che viaggiano separatamente, questa tecnica permette a più dispositivi di condividere lo stesso canale di comunicazione, un po' come la CPU con il multitasking
- i pacchetti corrotti possono essere trasmessi singolarmente e il destinatario riassembla i pacchetti nell'ordine

TIPI di RETE

- **Reti broadcast**: tutti i dispositivi condividono un unico canale, ma solo quello destinato viene elaborato (LAN)
- **Reti punto-punto**: i dati viaggiano da nodo a nodo, instradati tramite algoritmi di routing (WAN)

DIMENSIONI RETI

- LAN (Local Area Network): fino a 1 km, come in un ufficio
- MAN (Metropolitan): pochi km, come reti aziendali in città
- WAN (Wide Area Network): coprono vaste aree, anche mondiali

La distanza influenza la scelta delle tecnologie trasmissive

Reti LAN → proprietà di un'organizzazione e limitate geograficamente e velocità molto elevate (fino a 1 Gbps)
- Bus: un unico canale condiviso (es: Ethernet)
- Ring: tutti i nodi sono disposti ad anello (es: Token Ring IBM)

Reti WAN → coprono grandi distanze, anche globali (es. Internet) e sono composte da:
- End-point (computer utenti)
- Canali trasmissivi (fibra, radio, satelliti)
- Router e gateway che gestiscono l'instradamento

Le tecnologie WAN sono molto varie, dai cavi alle onde radio

SOFTWARE per RETI

Due programmi (client e server) comunicano tra loro e ogni nodo può agire da client o server (modello peer-to-peer)
- la comunicazione avviene attraverso strati software sovrapposti, ciascuno con funzioni specifiche

Il software di rete è diviso in livelli (stack), dove ogni livello comunica con il superiore e l'inferiore
L'idea è semplificare la comunicazione nascondendo i dettagli implementativi
- una catena di montaggio: ogni livello aggiunge/rimuove informazioni (header) ai pacchetti

La comunicazione è segmentata in pacchetti in modo che il canale trasmissivo non sia impegnato continuativamente per tempi molto lunghi e in caso di errore di trasmissione debba essere rispedito solo un pacchetto e non l'intero flusso di dati
- in fase di trasmissione, ogni livello aggiunge al pacchetto ricevuto dallo strato sovrastante un header, formando così un pacchetto più grande (il pacchetto viene "imbustato")
  - l'header contiene informazioni di servizio utili per lo scambio del pacchetto di dati
- in fase di ricezione ogni livello riceve un pacchetto "imbustato" dal livello inferiore
  - controlli di integrità del pacchetto
  - il ricevitore ricostruisce il flusso di comunicazione originario concatenando i pacchetti ricevuti

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

ARCHITETTURE delle RETI

Esistono modelli teorici per la definizione di un'architettura di una rete e architetture effettive nel mondo delle reti

- Modello OSI (Open Systems Interconnection)
  - consiste in 7 livelli, forse un po' troppo astratti e di difficile implementazione (ricalca IBM SNA)
- Architettura TCP/IP (Trasmission Control Protocol / Internet Protocol)
  - consiste in 4 livelli (semplificando il modello OSI)
  - Network Access, Internet (IP), Transport (TCP/UDP), Application (HTTP, FTP)

Stack TCP/IP

- livello Network Access gestisce i dettagli fisici della trasmissione
- livello Internet usa IP per instradare i pacchetti
- livello Transport (TCP/UDP) gestisce la suddivisione e il riassemblaggio dei dati
- livello Application è dove operano i programmi (browser, email)

LIVELLO FISICO → tratta la trasmissione analogica del segnale (elettrico, ottico, radio); la capacità di trasmissione dipende dalla banda passante e dal rapporto segnale/rumore, secondo i teoremi di Nyquist e Shannon

LIVELLO DATA LINK → fornisce una comunicazione affidabile tra due nodi su un canale fisico. Suddivide i dati in frame, gestisce errori e flusso tramite checksum e ritrasmissioni. Implementato spesso nei driver o firmware delle schede di rete

LIVELLO NETWORK → trasporta i dati tra nodi non direttamente collegati, grazie a router e algoritmi di routing; è il cuore delle reti complesse. Il protocollo IP gestisce frammentazione, riassemblaggio, indirizzamento e time-to-live

INDIRIZZI IP

Un pacchetto IP è una sequenza di byte costituita da un header e da un segmento di dati

- un indirizzo IP è composto da 32 bit, suddivisi in 4 gruppi da 8 bit (4 byte)

L'indirizzo viene assegnato ad ogni interfaccia di un nodo della rete per identificarlo univocamente; contiene due informazioni:

- l'identificativo della rete in cui si trova l'host
- l'identificativo dell'host all'interno della rete

Sono disponibili identificativi per reti IP private, non connesse direttamente ad Internet

L'insieme dei 32 bit che costituiscono l'indirizzo IP viene ripartito tra bit all'identificazione della rete e bit riservati all'identificazione dell'host in base al numero di host che devono essere indirizzati in una stessa rete

CLASSI INDIRIZZI

Gli indirizzi di rete sono distinti in tre diverse classi, a seconda del numero di bit riservati all'identificazione della rete o host:

- 126 reti di classe A, che possono contenere 16 milioni di host ciascuna
- 16.382 reti di classe B, con circa 64.000 host ciascuna
- 2 milioni di reti di classe C, con 254 host ciascuna

Per le reti private (non connesse direttamente alla rete Internet!) sono riservate le seguenti classi IP (RFC 1918):

- 1 classe A: 10.0.0.0 – 10.255.255.255
- 16 classi B: 172.16.0.0 – 172.31.255.255
- 256 classi C: 192.168.0.0 – 192.168.255.255

Le classi IP private possono essere utilizzate da chiunque su una rete privata, senza doverne richiedere l'autorizzazione ad un organismo di governo della rete; due reti che usano la stessa classe di indirizzi privati non possono essere collegate tra loro

- viene riservato anche un indirizzo riservato a rappresentare l'host stesso (indirizzo di loopback): 127.0.0.1

Per collegare alla rete pubblica Internet una rete con indirizzi IP privati, è necessario utilizzare un apparato (gateway) che esegua il NAT (network address translation)

RETE INTERNET

La rete Internet è formata dall'interconnessione di reti IP: gli indirizzi degli host (a meno delle reti private connesse attraverso meccanismi di NAT) sono identificati univocamente da indirizzi IP

- grafo ha una topologia che localmente è quella di una stella

È cresciuta fino a includere l'Internet delle Cose (IoT). Si passa gradualmente a IPv6 per aumentare lo spazio degli indirizzi

LIVELLO TRANSPORT → gestisce la comunicazione tra programmi su nodi diversi:

- TCP: garantisce consegna, ordine e integrità dei dati → servizio affidabile nella consegna del dato
- UDP: più leggero, ma non garantisce nulla (usato per streaming o giochi) → protocollo semplice e non affidabile

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

SOCKET

Un socket è un punto di accesso alla rete: unione tra indirizzo IP e numero di porta. Le API di sistema permettono ai programmi di aprire, gestire e chiudere connessioni TCP mentre i server possono creare un processo per ogni client connesso

LIVELLO APPLICATION → effettivamente due applicazioni (un client ed un server) che operano su due nodi della rete
- protocolli di servizio, standard, proprietari

Un protocollo applicativo è costituito da un insieme di comandi e da una sintassi

DNS

Domain Name System associa nomi a indirizzi IP → funziona come una rubrica distribuita e gerarchica
- ogni nome completo (FQDN) è unico e strumenti come nslookup e whois aiutano a esplorare il DNS

Il sistema DNS è costituito da
- uno schema gerarchico di definizione dei nomi, basato sul concetto di dominio
- un database distribuito che memorizza e rende disponibile l'insieme dei nomi
- un protocollo di comunicazione

I nomi host associati ad un indirizzo IP hanno la seguente struttura: hostname.subdomain.domain.top-level-domain
- un nome di host che comprenda tutte le componenti è un FQDN: fully qualified domain name

DATABASE

Il database del DNS è un database "gerarchico": ICANN e IANA gestiscono dell'albero e demandano ad altre organizzazioni la gestione dei top-level-domain:
- Country Code TLD (ccTLD): ".it", ".fr", ".uk", ".es", ".de", ".tv" e sono TLD assegnati alle autorità nazionali della rete
- Generic TLD (gTLD): ".com", ".net", ".org", ".edu", ".gov", ".mil" e sono TLD generici non corrispondenti ad un paese

Due sono i tool software più comuni per l'interrogazione dei database DNS del registro dei nomi di dominio:
- nslookup: è un software client per interrogare un DNS server e richiedere la risoluzione di un hostname dell'IP
- whois: è un client per interrogare i database "whois" delle autorità di registrazione dei domini

FTP

File Transfer Protocol, un protocollo della suite TCP/IP che permette di trasferire file tra un client e un server, usato per scaricare (download) o caricare (upload) file, sia in formato testuale (ASCII) che binario (immagini, programmi, file compressi)
- il protocollo FTP gestisce il concetto di sessione nell'ambito di uno stesso collegamento da un client verso un server

È un protocollo nato per scopi piuttosto generali e viene utilizzato per stabilire connessioni via rete in emulazione di terminale da un host remoto verso un server

SMTP

Simple Mail Transfer Protocol, protocollo per trasmettere messaggi di posta elettronica da un (mail transfer agent) ad un altro
- per dominio Internet deve essere definito (mediante record di tipo MX sul server DNS) almeno un mail exchanger

Il protocollo SMTP gestisce una sessione di lavoro tramite la quale possono messaggi di posta elettronica

POP3

Post Office Protocol, uno dei protocolli che consente ad un software client di posta elettronica di connettersi ad un mail server su cui risiedono le mailbox degli utenti, autenticare l'utente, e scaricare i messaggi di posta elettronica giacenti sul server

APPARATI di RETE

HUB	BRIDGE	SWITCH	ROUTER	FIREWALL
invio di dati a tutte le porte (livello 1)	collega due reti diverse (livello 2)	versione avanzata del bridge (LAN Ethernet)	collega reti diverse, indirizzi IP (livello 3)	controlla traffico in entrata/uscita

DOMINI COLLISIONE e BROADCAST

- Dominio di collisione → perimetro della rete entro cui i pacchetti possono andare in collisione fra di loro
- Dominio di broadcast → perimetro della rete entro cui i pacchetti vengono inviati in modalità broadcast a tutti i nodi

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 9 → SICUREZZA INFORMATICA (A)

Affinché un sistema informatico sia considerato sicuro, deve assicurare tre elementi fondamentali

- confidenzialità: solo i soggetti autorizzati possono accedere ai dati
- integrità: solo i soggetti autorizzati possono modificarli
- disponibilità: i dati devono essere accessibili quando necessario

SICUREZZA → la sicurezza è un campo ampio e attuale, che riguarda sia contesti militari che civili

- privati cittadini sono coinvolti, e la lezione si concentrerà su aspetti utili per l'uso quotidiano del computer

AVVERSARIO

In ambito informatico, i nemici della sicurezza possono essere di due tipi

- agenti software → ovvero programmi dannosi come virus, malware e trojan
- agenti umani → come hacker che cercano di violare i sistemi sfruttando software malevoli

LA SICUREZZA NON ESISTE

È importante sapere che nessun sistema può essere sicuro al 100%, la protezione dipende dal valore dell'informazione e da quanto siamo disposti a investire per proteggerla rispetto agli sforzi dell'attaccante

- la sicurezza perfetta non è realistica, ma è possibile trovare un equilibrio tra protezione e costi

CRITTOGRAFIA

La crittografia è una tecnica che permette di proteggere i dati trasformandoli in modo che diventino illeggibili

- Cifratura: il processo di conversione dei dati in una forma non comprensibile a persone non autorizzate (dati cifrati)
- Decifratura: il processo di riconversione dei dati cifrati nella loro forma originale, accessibili a chiunque (dati in chiaro)

CRITTOGRAFIA A CHIAVE SIMMETRICA (simmetrica)

La crittografia simmetrica è un metodo in cui la stessa chiave viene usata sia per cifrare sia per decifrare il messaggio

- tecnica finalizzata ad alterare l'informazione per renderla inutilizzabile a chiunque tranne che alle persone autorizzate

Se un attaccante intercetta un messaggio cifrato, ma non ha la chiave, non può sapere quale fosse il contenuto

VANTAGGI	SVANTAGGI
• molto rapido cifrare e decifrare • molto difficile da violare	• concordare la chiave • una chiave per ogni possibile coppia di entità

XOR (base della cifratura)

Alla base di molte tecniche di cifratura c'è un'operazione logica chiamata XOR → A XOR B = C C XOR B = A

- se 1 XOR 0 il risultato è 1 e se 1 XOR 1, il risultato è 0

Questa operazione viene applicata bit per bit e puoi sempre tornare ad A facendo C XOR B

- cifratura → "testo in chiaro" XOR "chiave" = testo cifrato
- decifratura → "testo cifrato" XOR "chiave" = testo in chiaro

COMPLESSITÀ E SICUREZZA

Complessità computazionale lineare nella lunghezza (in bit) di K

- quando si conosce la chiave, cifrare e decifrare è facile e veloce

Ma se la chiave è segreta, l'unico modo per scoprirla è provare tutte le combinazioni possibili

- se la chiave è lunga n bit, le combinazioni sono 2^n

Aumentare anche solo di 1 bit raddoppia il numero di combinazioni da provare, rendendo il compito molto più difficile

CRITTOGRAFIA A CHIAVE PUBBLICA (asimmetrica)

La chiave usata per cifrare è diversa dalla chiave per decifrare → le chiavi vengono create a coppie <PR, PU>

- PR: la chiave privata è nota solo all'utente
- PU: la chiave pubblica è nota a tutti

In questo sistema, ogni persona possiede due chiavi: una pubblica, visibile a tutti, e una privata, che deve restare segreta

- cifrare un messaggio utilizzando la chiave pubblica, ma solo il destinatario può decifrarlo usando la chiave privata

VANTAGGI	SVANTAGGI
• non richiede lo scambio preventivo di chiavi	• cifratura e decifratura più lente

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

SICUREZZA su INTERNET

Quando si parla di sicurezza su Internet, ci si riferisce alla protezione delle informazioni durante la comunicazione online
- per garantire questa sicurezza, vengono usati algoritmi crittografici molto noti e affidabili

Tra i più famosi ci sono l'RSA, che si basa sulla crittografia a chiave pubblica, e l'algoritmo di Diffie-Hellman, che permette a due persone di scambiarsi una chiave segreta attraverso un canale insicuro

FIRMA DIGITALE

La firma digitale è uno strumento che permette di autenticare digitalmente un documento, garantendo tre aspetti fondamentali
- assicura l'autenticità, l'integrità, irriproducibilità, permette il non-ripudio e non-riuso

FUNZIONE DI HASH

Alla base della firma digitale c'è la funzione di hash, che ha il compito di creare un riassunto del messaggio
- si tratta di una stringa breve e unica che rappresenta tutto il contenuto

MEMORIZZARE LE CHIAVI

Le chiavi crittografiche, che servono per firmare e verificare i documenti, vengono salvate in modi sicuri
- possono essere conservate su dispositivi hardware (come token USB o smart card) oppure all'interno di software

TIPI DI FIRMA DIGITALE

Esistono diversi formati di firma digitale, ognuno adatto a determinati tipi di file
- CADES è usato per file firmati con estensione .p7m
- PADES è il formato specifico per i documenti PDF firmati digitalmente, compatibile con programmi Adobe Acrobat
- firma cloud-based, che consente di firmare documenti direttamente a distanza, senza dover inserire una chiave fisica

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 10 → SICUREZZA INFORMATICA (B)

Per navigare in modo sicuro su Internet si usano diverse tecnologie, tra cui la crittografia a chiave pubblica, che protegge i dati durante la trasmissione, e i protocolli sicuri come HTTPS, che garantiscono connessioni protette tra il browser e il sito web

MALWARE

Indica un qualunque programma finalizzato a compiere azioni illecite in un computer

VIRUS

Un virus è un tipo di malware capace di autoreplicarsi e di diffondersi nel computer ed in altri computer
- un virus informatico può restare nascosto nel computer

Ad esempio: ILOVEYOU (uno dei virus più devastanti: si diffondeva via email mascherato da dichiarazione d'amore)

WORM

A differenza dei virus i worms operano attraverso reti di computers, utilizzano infatti le reti per trasmettere repliche di se stessi a tutti i computer che sono connessi a quella rete.
- la loro propagazione rallenta le prestazioni dei PC e delle reti

Ad esempio: CONFICKER (sfruttato vulnerabilità di Windows per infettare 9 milioni di PC, creando una botnet)

TROJAN

Un trojan infatti è malware mascherato da software utile, in genere programmi gratuiti o add-ons di browsers, si attivano infatti su azione dell'utente: ad esempio quando l'utente apre allegati infetti alle email, oppure scarica ed esegue file .exe da Internet
- in particolare, i trojan possono creare backdoors che permettono all'hacker di accedere illegittimamente

Ad esempio: ZBOT (trojan progettato per rubare credenziali bancarie)

SPYWARE

Gli spyware spiano quello che fai sul computer e su Internet, possono monitorare la tua attività accedendo a file di logs
- tutte le informazioni raccolte vengono inviate ad aziende oppure ad hackers

ADWARE

Adware deriva da advertisement (pubblicità) e malware → gli adware mostrano pubblicità all'utente
- diventa più pericoloso quando l'adware viene accompagnato da spyware, cosa sempre più frequente

KEYLOGGER

I keyloggers registrano quello che digiti con la tastiera, per poi inviare queste informazioni ad hackers
- grazie ai keyloggers, gli hackers possono rubare username e passwords, informazioni finanziarie

Ad esempio: SPYEYE (keylogger specializzato in frodi bancarie)

EXPLOIT

Un exploit è un codice che sfrutta una particolare vulnerabilità di un programma per computer (del sistema operativo stesso)
- permettere a chi attacca il PC di ottenerne il controllo

Ad esempio: MS12-020 Microsoft Remote Desktop Use-After-Free DoS

ROOTKIT

Un malware progettato accedere nel sistema operativo e nei registri eludendo il controllo di antivirus o programmi di sicurezza
- il rootkit serve agli hackers per ottenere accesso remote al tuo computer con privilegi di amministratore

RANSOMWARE

Il ransomware è una forma di malware che impedisce all'utente di accedere ai files del proprio computer attraverso la cifratura
- visualizza invece un messaggio per forzare l'utente a pagare per riavere accesso in chiaro ai files

Ad esempio: CRYPTOLOCKER (worm ransomware a criptazione)

DIFESA dai MALWARE

Tre strategie principali:
- Software di sicurezza (antivirus, antimalware, firewall)
- Aggiornamenti costanti
- Comportamento consapevole dell'utente

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

ANTIVIRUS

Gli antivirus servono a rilevare ed eliminare i malware, sono programmi che scansionano (=passano in rassegna) tutti i file sull'hard disk alla ricerca di virus: prevengono le infezioni scansionando o permettono di limitare i danni

- un antivirus protegge solo contro i virus che conosce

Per essere efficaci devono essere aggiornati regolarmente e funzionare in tempo reale

FIREWALL

Un firewall è una barriera di protezione tra il tuo dispositivo e Internet, controllano il traffico di rete e quando notano attività sospette, avvisano l'utente → serve saper interpretare i messaggi per decidere se bloccare o meno

- blocca gli accessi non autorizzati e filtra le comunicazioni in entrata e uscita

MULTIUTENZE

I sistemi operativi recenti supportano l'accesso alla macchina da parte di diversi utenti con diversi diritti di accesso.

- alcuni utenti sono amministratori cioè possono modificare tutte le impostazioni di una macchina
- altri utenti hanno accesso limitato

NAVIGAZIONE SICURA

Navigare in sicurezza significa anche fare attenzione ai siti visitati. È bene preferire siti con protocollo HTTPS, evitare di cliccare su link o popup sospetti e non scaricare file da fonti poco affidabili

- in Internet circolano molti messaggi il cui scopo è imbrogliare gli utenti ingenui

PHISHING

Il phishing è una tecnica per rubare dati personali fingendosi un'entità affidabile, come la banca o un servizio noto

- per difendersi, è importante controllare sempre il mittente e i link nell'email
- non inserire password se il sito sembra sospetto e diffidare da messaggi che creano urgenza o offrono premi

BACKUP

Un backup è una copia di sicurezza dei tuoi dati, fondamentale per non perdere tutto in caso di virus, furti o guasti

- possono essere salvati su un disco esterno o su un servizio cloud, e ti permettono di recuperare i tuoi file

PASSWORD

Strumento di identificazione molto diffuso poiché non richiede hardware apposito (come un lettore di impronte digitali) e permette un discreto livello di sicurezza se usate correttamente

- quando l'utente sceglie la password, una funzione (di cifratura) viene applicata

ATTACCO FORZA BRUTA → l'attaccante prova tutte le combinazioni possibili, tuttavia la difficoltà cresce esponenzialmente con la lunghezza: 8 caratteri = 100 miliardi di miliardi di combinazioni (morale: password lunghe ≥ 8 caratteri)

ATTACCHI DIZIONARIO → usano parole comuni o nomi come password e gli attaccanti usano elenchi per provarle

- esistono degli elenchi di nomi, parole e semplici concatenazioni di queste con numeri

PRIVACY

La privacy è un diritto riconosciuto da leggi italiane ed europee → è il diritto di controllare quali informazioni si rivelano agli altri

Le tecnologie moderne permettono di raccogliere e analizzare grandi quantità di dati, spesso deducendo informazioni che non erano state fornite direttamente (bisogna trovare un equilibrio tra vantaggi e tutela della privacy)

- non solo le informazioni che rilasciamo esplicitamente possono essere usate per violare la nostra privacy

L'utente deve poter avere il controllo sulle informazioni che vengono rilasciate

GDPR (Regolamento Generale sulla Protezione dei Dati), adottato dall'Unione Europea, tutela i dati personali degli utenti.

- le aziende devono informarti su quali dati raccolgono, chiederti il consenso per usarli, e rispettare il tuo diritto all'oblio, ovvero la possibilità di far cancellare i tuoi dati su richiesta.

CONCLUSIONI

Anche se la sicurezza totale non esiste, è possibile migliorare la protezione dei propri dati adottando comportamenti consapevoli e usando strumenti come antivirus, backup, e crittografia.
Inoltre, è fondamentale conoscere i propri diritti, specialmente quando si tratta di dati personali e privacy online

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 11 → FIRMA DIGITALE

FIRMA DIGITALE → La firma digitale è il risultato di una procedura informatica basata su tecniche crittografiche che consente di associare in modo indissolubile un numero binario (la firma) a un documento informatico

- insieme di bit che rappresenta fatti, atti o dati giuridicamente rilevanti
- indispensabile per conferire validità legale ai documenti informatici in una serie di contesti

UTILIZZO FIRMA DIGITALE

Non è una "semplice" firma elettronica, ma una particolare tipologia che si basa, appunto, sul sopra descritto meccanismo di chiavi crittografiche, la firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata

- la firma digitale è una tipologia di firma elettronica che soddisfando requisiti particolarmente stringenti relativi garantisce autenticità, integrativa, affidabilità e validità legale ai documenti

La firma digitale è uno strumento che permette ai cittadini, ai professionisti ed alle imprese di firmare dei documenti facendoli diventare documenti con valore legale, ed è il risultato di un procedimento informatico che si basa sui concetti di:

- autenticità: assicurare e garantire chi è che ha firmato il documento si è assunto la responsabilità del suo contenuto
- integrità: condizione che serve a dimostrare che non è mai stato modificato
- non ripudio: in quanto chi ha firmato il documento mediante la firma elettronica non può poi disconoscerlo

L'assegnazione è a carico di un soggetto istituzionalmente qualificato (il certificatore) – in Italia dall'Agenzia per l'Italia Digitale

FUNZIONAMENTO FIRMA DIGITALE

La firma digitale è uno strumento sia informatico che legale che permette di identificare con certezza chi ha firmato un documento e di verificare che il contenuto non sia stato modificato

La firma digitale si basa su un sistema di coppie di chiavi crittografiche: una chiave pubblica e una chiave privata

- la chiave è installata in un ambiente sicuro (nella smart card il microchip) e può essere utilizzata solamente tramite una password di sblocco che è nota come PIN

Per firmare, il titolare utilizza un software che iniziata la procedura di firma calcola l'impronta digitale del documento tramite la cosiddetta funzione di hash (meccanismo che trasforma il documento in una stringa di caratteri molto breve, ma unica)

- predisposta l'impronta, il software di sottoscrizione la invia all'ambiente sicuro dove è custodita la chiave privata (dispositivo di firma) → questa per essere attivata deve validare il PIN inserito dal titolare

Il dispositivo di firma procede alla cifratura dell'impronta del documento con la chiave privata, il risultato dell'operazione è la firma digitale del documento

- indispensabile associare la firma al documento e questo avviene attraverso specifici formati
- (PDF → PAdES); (CAD → CAdES); (XML → XAdES)

Il procedimento ha anche altre variabili in gioco, come la validità del certificato rispetto al tempo e al titolare

FIRMA ELETTRONICA

Nel regolamento sono anche definite le Firme Elettroniche, più precisamente la Firma Elettronica Avanzata (FEA), firma elettronica che è connessa unicamente al firmatario e lo identifica, per la sua creazione il firmatario può esercitare il proprio esclusivo controllo, ed è collegata ai dati firmati con una connessione che permette di rilevare ogni modifica dei dati

- Firma Elettronica Qualificata (FEQ) e anche il Sigillo Elettronico
- firma digitale si ottiene dai prestatori di servizi fiduciari presenti in una serie di elenchi di fiducia gestiti dai singoli stati

Esistono diversi prodotti di firma digitale ed essi sono generalmente costituiti da un device, solitamente una smart card, che contiene un certificato di firma digitale rinnovabile ed un dispositivo che serve per leggere la smart card.

- sul mercato è possibile trovare da un po' di anni anche un kit che è costituito da una chiavetta USB

In pratica, bisogna quindi rivolgersi a uno dei provider qualificati, che in Italia sono in tutto 18

- ogni provider ha una sua procedura e un suo kit di installazione
- ci sono poi dei software che servono invece a verificare la firma digitale

COSTI FIRMA DIGITALE

In generale l'ordine di grandezza è di qualche decina di euro (25/30 + IVA) anche per modalità di sottoscrizione remota

- costo sale se si sceglie il chip installato in un token USB
- la normativa di riferimento nazionale sulla firma digitale è nel Codice dell'amministrazione digitale (CAD)

La firma digitale è obbligatoria in molti scenari amministrativi, professionali e aziendali

La tendenza normativa rappresentata dall'ultimo CAD è che per i cittadini si debba utilizzare lo SPID (Sistema Pubblico di Identità Digitale)

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 12 → RETI IP

RETI IP → Per instradare correttamente i pacchetti trasmessi attraverso una rete, i router necessitano di informazioni riguardanti la topologia della rete stessa. Deve dunque essere identificato univocamente ogni nodo della rete

- ogni host all'interno della rete è identificato da un indirizzo, chiamato indirizzo IP (IP address)

INDIRIZZO IP

Un indirizzo IP è costituito da una sequenza di quattro numeri decimali, aventi ciascuno un massimo di tre cifre
Ad es.: 193.183.44.30

- indirizzo di rete=network number= network prefix : identifica la rete a cui un computer appartiene
- indirizzo di host=host number : identifica il computer della rete

SOTTORETI

È possibile modificare, parzialmente, la struttura dell'indirizzamento utilizzando le sottoreti (subnet)
Il campo definito come indirizzo locale host, può essere suddiviso arbitrariamente in due campi:

- sottorete
- host

L'operazione di suddivisione di una rete in sottoreti si chiama segmentazione (migliorare la strutturazione della rete stessa)
La creazione delle sottoreti (subnetting) è ottenuta suddividendo la parte host dell'indirizzo IP in due parti:

- parte di subnetting
- parte di host

Viene eseguita un'operazione di AND tra il numero IP e la sua maschera di sottorete. Quando un pacchetto viene inviato in rete, il suo destinatario IP viene sottoposto, anch'esso, a un AND logico con la subnet mask

- I bit 1 corrispondenti alle cifre del numero di rete esteso formano la subnet mask

Se il risultato del processo coincide con l'indirizzo di rete, l'host in questione appartiene a quella rete; diversamente il pacchetto viene inviato a un router che provvede a smistarlo

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 13 → INFORMAZIONI MULTIMEDIALI

DIGITALIZZAZIONE → Il primo passaggio nell'operazione di digitalizzazione consiste nell'individuare come rendere discreta una fonte che in realtà è continua; qualunque informazione può essere rappresentata attraverso una sequenza di bit:

- a patto che sia discreta (e finita)
- il modo in cui viene rappresentata l'informazione influenza: lo spazio che occupa e l'efficienza degli algoritmi

IMMAGINI → L'immagine digitale è una rappresentazione di un'immagine bidimensionale tramite un'opportuna serie di valori:

- immagine bitmap: i valori formano una matrice di punti, ogni punto (=pixel) indica le caratteristiche dell'immagine
- immagine vettoriale: insieme di punti uniti in linee e curve, a loro volta unite in forme più complesse

IMMAGINI → PIXEL

Lo schermo di un computer è suddiviso in una griglia di punti chiamati pixel (=picture element)

- il computer visualizza ogni pixel nel colore dell'immagine da rappresentare: maggiore è il numero di pixel in ogni riga e colonna, maggiore risulta la risoluzione dell'immagine

Le immagini possono essere di due tipi:

- vettoriali → create tramite formule geometriche che definiscono linee, curve e forme
- bitmap (raster) → composte da una griglia di pixel, ovvero piccoli quadratini colorati

COLORI IMMAGINI

PROFONDITÀ di COLORI: profondità di colore indica quanti bit sono necessari per rappresentare il colore di un singolo pixel

- con 1 bit si possono distinguere solo due colori (bianco e nero), con 8 bit si possono rappresentare 256 colori, mentre con 24 bit si raggiungono circa 16 milioni di colori, che è lo standard per fotografie e immagini realistiche

CODIFICA COLORI: metodi di codifica del colore sono basati soprattutto sulla percezione umana (lunghezza onda)

- digitalizzazione dei colori → RGB (Red Green Blue)

DIMENSIONE DELL'IMMAGINE

La dimensione di un'immagine (in bit) dipende da due fattori: il numero di pixel e la profondità di colore

- la formula per calcolarla è: larghezza × altezza × bit per pixel
- maggiore è la qualità, maggiore sarà anche lo spazio occupato

COMPRESSIONE DELLE IMMAGINI: le immagini possono occupare molto spazio, si utilizzano tecniche di compressione

- lossless (senza perdita), dove la qualità originale viene mantenuta (es. formato PNG)
- lossy (con perdita), che sacrifica una parte della qualità per risparmiare spazio (es. formato JPEG)

SUONO → AUDIO

Il suono, per essere gestito dal computer, viene prima campionato: cioè si prelevano dei valori dell'onda sonora a intervalli regolari (per esempio ogni millisecondo) e questi valori vengono poi digitalizzati, cioè trasformati in numeri binari

- oscillazione = variazione di pressione (vibrazione di un oggetto trasmessa nell'aria)
- frequenza = numero di oscillazioni al secondo (maggiore è la frequenza, più acuto risulta il suono)
- intensità/forza della pressione = ampiezza dell'oscillazione

DIGITALIZZAZIONE SUONO

- Convertitore analogico-digitale (ADC) → campiona l'onda a intervalli regolari e la passa alla memoria (numeri binari)
- Convertitore digitale-analogico (DAC) → ricrea l'onda elettrica più semplice che "passa" per tutti i punti rappresentati

PARAMETRI AUDIO: per rappresentare correttamente l'audio digitale, servono tre parametri:

- frequenza di campionamento (quanti campioni al secondo vengono presi)
- risoluzione o bit depth (quanti bit sono usati per ciascun campione)
- numero di canali, come mono o stereo.

DIMENSIONE DEL FILE AUDIO

La dimensione di un file audio si calcola con la formula: frequenza × profondità in bit × durata × numero di canali

- anche l'audio può essere compresso per occupare meno spazio: lossless o lossy (come MP3 o OGG)

VIDEO

Un video è composto da una sequenza di immagini (chiamate fotogrammi o frame) a cui si aggiunge l'audio
Senza compressione, i file video sarebbero troppo grandi per essere archiviati o trasmessi facilmente.

- per questo si usano formati compressi come MP4, AVI o MKV

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

CAP 14 → DISCRETIZZAZIONE

DIGITALIZZAZIONE → Nel processo di digitalizzazione che permette di convertire un segnale analogico in modo da poterlo elaborare con dispositivi numerici di calcolo, si operano due distinte discretizzazioni:

- una discretizzazione nel dominio del tempo o campionamento che riduce gli infiniti valori di un segnale analogico
- una discretizzazione nel dominio delle ampiezze o quantizzazione permette di rappresentare con bit

La discretizzazione è utilizzata per convertire segnali analogici (come suoni o immagini) in formato digitale

- uniforme: dominio continuo è suddiviso in intervalli di uguale ampiezza
- non Uniforme: intervalli hanno ampiezze diverse, determinate in base alla distribuzione dei dati

QUANTIZZAZIONE

Sostituisce ai valori continui del segnale analogico dei valori discreti (quantificati) cioè non-continui, "a salti"

- l'approssimazione introdotta dalla quantizzazione si manifesta in forma di rumore (rumore di quantizzazione)

La quantizzazione riduce il rapporto segnale/rumore del sistema → si ricorre a tecniche di compressione (es: PCM)

PROBLEMA FREQUENZA CAMPIONAMENTO

Punti di campionamento troppo distanti possono dare luogo a significative perdite di informazione (spreco di risorse)

TEOREMA di SHANNON → dato un segnale a banda limitata x(t), il segnale è completamente determinato a partire dalla sequenza x(nT) dei suoi campioni acquisiti ad intervalli uniformi di durata

- errori nel campionamento: aliasing
- errori nel campionamento: frequency folding
- evitare errori nel campionamento: filtro anti aliasing

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari