



PRINCIPLES OF IT

Computer and IT fundamentals

1st Edition

معرفی کوتاه کتاب

کتابی که پیش روی شماست، یکی از پایه‌ای‌ترین و مقدماتی‌ترین منابع برای آشنایی با مفاهیم اولیه کامپیوتر و فناوری اطلاعات (IT) است. این اثر به‌گونه‌ای تدوین شده که نقطه‌ی آغازین ورود به دنیای فناوری محسوب شود؛ به عبارت دیگر، می‌توان آن را قدم اول هر مسیر آموزشی در حوزه رایانه و IT دانست. مطالب این کتاب با زبانی ساده و قابل درک برای علاقه‌مندان، دانشجویان و هنرجویان تنظیم شده است و به‌عنوان پیش‌نیاز بسیاری از دوره‌ها و آموزش‌های تخصصی‌تر عمل می‌کند. بنابراین، مطالعه آن به شما کمک می‌کند تا بنیانی محکم برای یادگیری‌های بعدی خود بسازید و با مفاهیم کلیدی این حوزه به شکلی روان و کاربردی آشنا شوید.

کتاب
مرجع
مبانی
IT

کتاب مرجع کامل مبانی فناوری اطلاعات
Principles of Information technology

Computer and IT Fundamentals

حسین سیلانی
ویرایش اول

۱۴۰۴



سرشناسه	سیلانی، حسین، ۱۳۶۰.
عنوان و نام پدیدآور	مبانی فناوری اطلاعات
مشخصات نشر	حسین سیلانی؛ ویراستاری حسین سیلانی.
مشخصات ظاهری	تهران: کیان دانش، ۱۴۰۴.
شابک	600 ص.
وضعیت فهرست نویسی	۹۷۸.۶۲۲.۴۰۱.۰۳۵.۶
موضوع	فیپا
	مبانی فناوری اطلاعات
	IT
شناسه افزوده	سیلانی، حسین، ۱۳۶۰.
رده بندی کنگره	۷۶/۷۶QA
رده بندی دیویی	۴۳۲/۰۰۵
شماره کتابشناسی ملی	۹۶۷۳۵۹۳
اطلاعات رکورد کتابشناسی	فیپا

نشر کیان دانش: ناشر کتاب‌های دانشگاهی



عنوان: مبانی فناوری اطلاعات
تألیف: حسین سیلانی
صفحه آرای و ویراستاری: حسین سیلانی
چاپ و صحافی: موسسه مهراد
طراحی جلد: حسین سیلانی
چاپ اول: ۱۴۰۴
شمارگان: ۱۰۰ جلد
شابک: ۹۷۸.۶۲۲.۴۰۱.۰۳۵.۶
حق چاپ محفوظ است.

خیابان ۱۲ فروردین، خیابان شهدای ژاندارمری، شماره ۱۲۶، طبقه چهارم

سخنی از نویسنده
با سلام و احترام به دوست گرامی

از اینکه این کتاب را انتخاب کرده‌اید و در این مسیر همراه من هستید صمیمانه سپاسگزارم. امیدوارم این اثر برای علاقه‌مندان به حوزه لینوکس مفید و اثربخش باشد. همچنین از شما درخواست دارم که اگر نواقص یا کاستی‌هایی در کتاب مشاهده کردید آن‌ها را نادیده نگیرید و با ارائه نظرات و پیشنهادات سازنده‌ی خود، به بهبود کیفیت این اثر کمک کنید.

شایان ذکر است که این کتاب یکی از صدها کتاب لینوکسی من است که بسیاری از آن‌ها در حال ترجمه یا نگارش هستند. این مجموعه در راستای پروژه‌های متن‌باز شخصی‌ام و با هدف طراحی و توسعه توزیع‌های لینوکس نوشته شده است. امیدوارم این تلاش‌ها گامی هرچند کوچک در جهت گسترش دانش و استفاده از سیستم‌عامل‌های متن‌باز باشد.

🔗 <https://predator-os.ir/>

🔗 <https://little-Psycho.ir>

🔗 <https://emperor-os.ir/>

🔗 <https://artystone.ir>

تصمیم دارم محتوای آموزشی فارسی در حوزه‌های لینوکس و نرم‌افزارهای متن‌باز را در قالب‌های متنوعی مانند کتابچه، کتاب، فلش کارت، فایل‌های صوتی و ویدئوهای آموزشی تولید کرده و از طریق یک سایت در دسترس عموم قرار دهم. هدف من از این کار، ایجاد یکی از بزرگترین و جامع‌ترین مراجع آموزشی فارسی در این زمینه است. برای دسترسی به سایت و اطلاع از آخرین اخبار و محتواهای آموزشی، می‌توانید از طریق راه‌های ارتباطی زیر با من در تماس باشید:

🔗 learninghive.ir: آدرس سایت

🔗 [@LinuxTnt](https://t.me/LinuxTnt): کانال تلگرام

🔗 [@seilany](https://t.me/seilany): آیدی تلگرام

🔗 h.seilany@gmail.com: ایمیل

🔗 [hosseinseilani](https://github.com/hosseinseilani): گیت‌هاب

منتظر حضور و همراهی شما هستم!

تقديم به تو

يگانه فرزانه دلم

- ۳۰ - مخاطبین هدف این دوره چه کسانی هستند؟

- ۳۲ - بیت (Bit)

- ۳۴ - ذخیره‌سازی داده‌ها (Storing Data)

- ۳۴ - داده‌های دودویی (Binary Data)

- ۳۶ - بیت (Bit)

- ۳۷ - داده‌های هگزادسیمال (Hexadecimal Data)

- ۳۷ - نمونه تبدیل اعداد

- ۳۸ - تشخیص انواع داده‌ها

- ۳۸ - نکته آزمون (Exam Tip):

- ۳۸ - رمزگذاری کاراکترها (Character Encoding)

- ۳۹ - بایت و بیت در پردازش متن

- ۳۹ - استاندارد ASCII

- ۳۹ - مقایسه سیستم‌های داده‌ای

- ۴۰ - تاریخچه ASCII و Unicode

- ۴۰ - نحوه نمایش کاراکترهای غیرانگلیسی

- ۴۰ - ترکیب داده‌های هگزادسیمال و باینری برای رمزگذاری

- ۴۱ - انواع داده‌ها (Data Types)

- ۴۱ - سیستم‌های ذخیره‌سازی و نوع داده‌ها

- ۴۱ - نکته آزمون (Exam Tip):

- ۴۲ - داده‌های بولی (Boolean Data)

- ۴۲ - کاربردهای داده‌های بولی

- ۴۳ - اصطلاحات تخصصی

- ۴۳ - ترکیب داده‌های بولی با سایر انواع داده‌ها

- ۴۳ - کاربردهای پیشرفته داده‌های بولی

- ۴۳ - مزایای استفاده از داده‌های بولی

- ۴۳ - داده‌های عددی (Numeric Data)

- ۴۴ - اعداد صحیح (Integers)

- ۴۴ - اعداد اعشاری (Floating-Point / Floats)

- ۴۵ - نحوه ذخیره و پردازش داده‌های عددی

داده‌های متنی (Text Data) ----- ۴۵ -

کاراکتر تک Char ----- ۴۶ -

رشته‌های متنی Strings ----- ۴۶ -

مزایای انتخاب نوع داده مناسب ----- ۴۷ -

فصل ۲ ----- ۴۹ -

ورودی (Input) ----- ۴۹ -

تعریف ورودی (Input) ----- ۴۹ -

اهمیت ورودی در محاسبات ----- ۴۹ -

انواع ورودی (Types of Input) در محاسبات و فناوری اطلاعات ----- ۵۰ -

ورودی انسانی (Human Input) ----- ۵۰ -

الف) کیبورد (Keyboard) ----- ۵۰ -

ب) ماوس (Mouse) ----- ۵۰ -

ج) صفحه لمسی (Touchscreen) ----- ۵۰ -

د) ورودی صوتی (Voice Input) ----- ۵۰ -

ورودی ماشینی یا غیر انسانی (Non-Human Input) ----- ۵۱ -

الف) حسگرها (Sensors) ----- ۵۱ -

ب) ورودی از فایل‌ها (File Input) ----- ۵۱ -

ج) ورودی شبکه‌ای (Network Input) ----- ۵۱ -

مزایا و معایب ورودی انسانی ----- ۵۱ -

ورودی در دنیای واقعی ----- ۵۲ -

۱. سیستم‌های بانکی ----- ۵۲ -

۲. بازی‌های ویدیویی ----- ۵۲ -

۳. ترموستات‌های هوشمند و خانه‌های هوشمند ----- ۵۲ -

۴. سیستم‌های فروشگاهی و انبارداری ----- ۵۲ -

پردازش (Processing) ----- ۵۳ -

اهمیت پردازش در سیستم‌های IT ----- ۵۳ -

واحدهای پردازش اصلی (Main Processing Units) ----- ۵۳ -

اجزای اصلی CPU ----- ۵۴ -

حافظه دسترسی تصادفی / RAM (Random Access Memory) ----- ۵۴ -

انواع پردازش داده‌ها ----- ۵۶ -

پردازش اعداد صحیح (Integer Processing) ----- ۵۶ -

پردازش اعداد اعشاری (Floating-point Processing) ----- ۵۷ -

مزایا و چالش‌های پردازش عددی ----- ۵۷ -

پردازش منطقی (Logical Processing) ----- ۵۷ -

پردازش داده متنی (Text Processing) ----- ۵۸ -

پردازش تصویر و صوت (Multimedia Processing)	۵۹ -
خروجی (Output)	۶۱ -
انواع خروجی (Types of Output)	۶۲ -
۱. خروجی بصری (Visual Output)	۶۲ -
۲. خروجی صوتی (Audio Output)	۶۲ -
۳. خروجی داده‌ای (Data Output)	۶۳ -
۱. خروجی بصری (Visual Output)	۶۳ -
۲. خروجی صوتی (Audio Output)	۶۳ -
۳. خروجی داده‌ای (Data Output)	۶۴ -
دستگاه‌ها و فناوری‌های خروجی	۶۴ -
۱. مانیتور و نمایشگرها	۶۴ -
۲. چاپگرها	۶۴ -
۳. بلندگوها و هدست‌ها	۶۴ -
۴. سیستم‌های شبکه‌ای و API ها	۶۵ -
خروجی در صنایع مختلف IT	۶۵ -
ذخیره‌سازی (Storage)	۶۶ -
اهمیت ذخیره‌سازی در سیستم‌های IT	۶۶ -
انواع ذخیره‌سازی	۶۶ -
۱. ذخیره‌سازی موقت (Volatile Storage)	۶۶ -
۲. ذخیره‌سازی دائم (Non-Volatile Storage)	۶۷ -
۱. هارد دیسک (HDD – Hard Disk Drive)	۶۷ -
۲. حافظه حالت جامد (SSD – Solid State Drive)	۶۷ -
۳. ذخیره‌سازی نوری (Optical Storage)	۶۷ -
ساختار داده‌ها در ذخیره‌سازی	۶۷ -
۱. بیت (Bit)	۶۷ -
۲. بایت (Byte)	۶۸ -
۳. بلاک (Block)	۶۸ -
۴. فایل (File)	۶۸ -
تکنیک‌های ذخیره‌سازی داده‌ها	۶۸ -
اصول ذخیره‌سازی ترتیبی	۶۸ -
ترتیب داده‌ها	۶۸ -
مزایا و معایب ذخیره‌سازی ترتیبی	۶۹ -
تکنیک‌ها و الگوریتم‌های ذخیره‌سازی ترتیبی	۶۹ -
۲. ذخیره‌سازی تصادفی (Random Access Storage)	۷۰ -
دسترسی مستقیم به داده‌ها	۷۰ -
تکنیک‌ها و الگوریتم‌های ذخیره‌سازی تصادفی	۷۱ -

ذخیره‌سازی در سیستم‌های ابری (Cloud Storage) - ۷۲ -

فصل ۳ - ۷۶ -

ارزش داده‌ها (Value of Data) - ۷۶ -

داده و اطلاعات به عنوان دارایی - ۷۶ -

داده (Data): - ۷۶ -

اطلاعات (Information): - ۷۶ -

اهمیت سرمایه‌گذاری در امنیت داده‌ها - ۷۷ -

رابطه داده با تولید اطلاعات - ۷۷ -

مالکیت فکری و محصولات دیجیتال - ۷۸ -

انواع مالکیت فکری در فضای دیجیتال - ۷۸ -

۱. حق نشر (Copyright) - ۷۸ -

۲. علامت تجاری (Trademark) - ۷۸ -

۳. اختراع (Patent) - ۷۸ -

۴. اسرار تجاری (Trade Secrets) - ۷۸ -

تصمیم‌گیری‌های کسب‌وکاری مبتنی بر داده (Data-Driven Decisions) - ۷۹ -

اطلاعات (Information) - ۸۰ -

تصمیم‌گیری‌های کسب‌وکاری مبتنی بر داده (Data-Driven Business Decisions) - ۸۰ -

حق نسخه‌برداری (Copyrights) - ۸۱ -

علائم تجاری (Trademarks) - ۸۲ -

اصول و قوانین پایه علائم تجاری - ۸۲ -

انواع علائم تجاری و کاربردهای صنعتی - ۸۳ -

نمادها - ۸۴ -

اختراعات (Patents) - ۸۴ -

انواع اختراعات - ۸۵ -

مراحل ثبت اختراع - ۸۵ -

امنیت داده‌ها (Securing Data) - ۸۶ -

اهمیت امنیت داده‌ها در کسب‌وکار - ۸۶ -

ریسک‌های ناشی از عدم امنیت داده‌ها: - ۸۷ -

ریسک‌های ناشی از عدم امنیت داده‌ها - ۸۷ -

۱. نفوذ به سیستم‌ها و سرقت داده‌ها (Data Breach) - ۸۷ -

۲. از دست رفتن اعتماد مشتریان (Loss of Trust) - ۸۷ -

۳. خسارات مالی (Financial Losses) - ۸۸ -

پیامدهای قانونی و مقرراتی (Legal and Regulatory Consequences) - ۸۸ -

اقدامات امنیتی ضروری در کسب‌وکارها - ۸۸ -

۱. اقدامات فنی (Technical Controls) - ۸۸ -

- ۲. آموزش کارکنان (Employee Training) ----- - ۸۸ -
- ۳. سیاست‌ها و فرآیندهای امنیتی (Security Policies and Procedures) ----- - ۸۹ -
- ۴. نظارت و ارزیابی مستمر (Continuous Monitoring and Assessment) ----- - ۸۹ -
- استانداردها و چارچوب‌های ITF+ در امنیت داده‌ها ----- - ۸۹ -
- مثال‌های صنعتی و کاربردی ----- - ۸۹ -
- مراحل اصلی امنیت داده‌ها ----- - ۹۰ -
- محافظت از دارایی‌های فکری ----- - ۹۲ -
- امنیت داده‌های شخصی ----- - ۹۲ -
- انواع داده‌های شخصی ----- - ۹۲ -
- تهدیدات امنیتی داده‌های شخصی ----- - ۹۳ -
- اقدامات امنیتی برای حفاظت از داده‌های شخصی ----- - ۹۳ -
- رمزگذاری داده‌ها (Data Encryption) ----- - ۹۳ -
- احراز هویت چند مرحله‌ای (Multi-Factor Authentication – MFA) ----- - ۹۳ -
- محدود کردن دسترسی بر اساس نقش (Role-Based Access Control – RBAC) ----- - ۹۳ -
- آموزش کارکنان در مورد تهدیدات امنیتی ----- - ۹۳ -
- تهیه نسخه پشتیبان (Backup) ----- - ۹۳ -
- پایش و نظارت بر شبکه و سیستم‌ها ----- - ۹۴ -
- به‌روزرسانی نرم‌افزارها و سیستم‌ها ----- - ۹۴ -

چالش‌ها در امنیت داده‌های شخصی ----- - ۹۴ -

فصل ۴ ----- - ۹۷ -

واحدهای اندازه‌گیری – (Units of Measure) ----- - ۹۷ -

- اهمیت واحدهای اندازه‌گیری در فناوری اطلاعات ----- - ۹۷ -
- ۱. واحدهای ذخیره‌سازی داده‌ها (Storage Units) ----- - ۹۷ -
- بایت‌ها (Bytes) ----- - ۹۷ -
- ۲. واحدهای توان عملیاتی (Throughput Units) ----- - ۹۸ -
- توان عملیاتی شبکه (Network Throughput) ----- - ۹۸ -
- واحدهای اندازه‌گیری توان عملیاتی ----- - ۹۸ -
- تفاوت توان عملیاتی (Throughput) و پهنای باند (Bandwidth) ----- - ۹۹ -
- عوامل مؤثر بر توان عملیاتی شبکه ----- - ۹۹ -
- بهینه‌سازی توان عملیاتی شبکه ----- - ۹۹ -
- توان عملیاتی دیسک‌ها (Disk Throughput) ----- - ۹۹ -
- واحدهای اندازه‌گیری توان عملیاتی دیسک ----- - ۹۹ -
- عوامل مؤثر بر توان عملیاتی دیسک ----- - ۱۰۰ -
- بهینه‌سازی توان عملیاتی دیسک ----- - ۱۰۱ -
- ۳. واحدهای سرعت پردازش (Processing Speed Units) ----- - ۱۰۱ -
- واحدهای انتقال داده (Throughput) ----- - ۱۰۲ -
- واحدهای استاندارد ذخیره‌سازی داده ----- - ۱۰۲ -

- ۱۰۳ - روش های انتقال داده در شبکه ها
- ۱۰۳ - (۱. شبکه های سیمی (Wired Networks))
- ۱۰۴ - (۲. شبکه های بی سیم (Wireless Networks))
- ۱۰۴ - (۳. شبکه های فیبر نوری (Fiber–Optic Networks))
- ۱۰۵ - توان عملیاتی شبکه و چندگانه های (Multiples of bps) bps
- ۱۰۶ - اهمیت توان عملیاتی در شبکه
- ۱۰۶ - (اندازه گیری سرعت پردازنده (Measuring Processor Speed))
- ۱۰۶ - مرکز پردازش و نقش CPU
- ۱۰۶ - (چرخه (Cycle))
- ۱۰۷ - (واحد اندازه گیری سرعت پردازنده: هرتز (Hertz))
- ۱۰۷ - چگونگی عملکرد ساعت داخلی CPU
- ۱۰۷ - مقایسه با حافظه و شبکه
- ۱۰۸ - (چرخه های پردازنده و دستورالعمل ها (CPU Cycles and Instructions))
- ۱۰۸ - توسعه در فناوری CPU
- ۱۰۸ - نسل های اولیه
- ۱۰۸ - نسل های میانی
- ۱۰۹ - پردازنده های مدرن
- ۱۰۹ - واحدهای مرتبط با سرعت پردازنده
- ۱۰۹ - فناوری های افزایش توان پردازنده
- ۱۱۰ - کش CPU
- ۱۱۰ - فناوری های توربو و بهینه سازی فرکانس
- ۱۱۰ - تاثیر فرکانس و هسته ها بر عملکرد واقعی
- ۱۱۰ - تاریخچه تکامل CPU

فصل ۵ - - ۱۱۲

روش شناسی رفع اشکال - - ۱۱۲

- ۱۱۲ - (شناسایی مشکل (Identify the Problem))
- ۱۱۴ - (انجام تحقیق (Conduct Research))
- ۱۱۴ - (ایجاد نظریه (Establish a Theory))
- ۱۱۴ - (آزمایش نظریه (Test the Theory))
- ۱۱۵ - (برنامه ریزی اقدامات (Establish a Plan of Action))
- ۱۱۵ - (پیاده سازی یا ارجاع مشکل (Implement or Escalate))
- ۱۱۵ - (تایید عملکرد (Verify Functionality))

مستندسازی (Document Your Work)	- ۱۱۵ -
واسط‌های دستگاه‌های ورودی/خروجی (Input/Output Device Interfaces)	- ۱۱۶ -
تعریف رابط دستگاه (Device Interface)	- ۱۱۶ -
انواع رابط‌ها و کانکتورها (Interfaces and Connectors)	- ۱۱۶ -
رابط‌های سیمی (Wired Interfaces)	- ۱۱۶ -
رابط‌های بی‌سیم (Wireless Interfaces)	- ۱۱۷ -
تطبیق کابل و کانکتور با دستگاه	- ۱۱۷ -
رابط‌های شبکه (Network Interfaces)	- ۱۱۷ -
شبکه‌های سیمی (Wired Networks)	- ۱۱۷ -
شبکه‌های بی‌سیم (Wireless Networks)	- ۱۱۸ -
شبکه‌های سیمی (Wired Networks)	- ۱۱۹ -
شبکه‌های بی‌سیم (Wireless Networks)	- ۱۲۰ -
مقایسه شبکه‌های سیمی و بی‌سیم	- ۱۲۱ -
رابط‌های دستگاه‌های جانبی (Peripheral Interfaces)	- ۱۲۲ -
USB (Universal Serial Bus)	- ۱۲۲ -
انواع کانکتور USB	- ۱۲۲ -
FireWire	- ۱۲۳ -
انواع FireWire	- ۱۲۳ -
کاربردهای FireWire	- ۱۲۴ -
(Serial ATA (SATA	- ۱۲۵ -
رابط‌های گرافیکی (Graphic Interfaces)	- ۱۲۷ -
(VGA (Video Graphics Array	- ۱۲۷ -
(DVI (Digital Visual Interface	- ۱۲۷ -
(HDMI (High-Definition Multimedia Interface	- ۱۲۸ -
نسخه‌های HDMI	- ۱۲۸ -
Mini DisplayPort, DisplayPort	- ۱۲۸ -
نصب دستگاه‌های جانبی (Installing Peripherals)	- ۱۳۰ -
سناریوهای نصب دستگاه‌های جانبی (Peripheral Installation Scenarios)	- ۱۳۱ -
سناریو ۱: اتصال پرینتر به لپ‌تاپ شخصی در خانه	- ۱۳۱ -
سناریو ۲: راه‌اندازی اسکنر در محیط اداری	- ۱۳۲ -
سناریو ۳: اتصال هارد اکسترنال به سرور	- ۱۳۲ -
انواع دستگاه‌های جانبی (Peripheral Types)	- ۱۳۳ -
۱. کیبورد و ماوس (Keyboards and Mice)	- ۱۳۳ -
۲. نمایشگرها (Displays)	- ۱۳۴ -

- ۳. دستگاه‌های همه‌کاره (All-in-One, AIO) ----- ۱۳۴ -
- ۴. بلندگوها و هدفون‌ها (Speakers and Headphones) ----- ۱۳۴ -
- ۵. پرینترها و اسکنرها (Printers and Scanners) ----- ۱۳۴ -
- ۶. دوربین‌ها (Cameras) ----- ۱۳۴ -
- ۷. هارد دیسک‌های خارجی (External Hard Drives) ----- ۱۳۵ -

دستگاه‌های ساده با فناوری Plug-and-Play (PnP) ----- ۱۳۵ -

۲. نصب دستی دستگاه‌های تخصصی یا قدیمی ----- ۱۳۸ -

۳. دستگاه‌های شبکه‌ای برای کل دفتر ----- ۱۳۸ -

فصل ۶ ----- ۱۴۲ -

اجزای داخلی رایانه (Internal Computing Components) ----- ۱۴۲ -

- ۱. مادربرد (Motherboard) ----- ۱۴۲ -
- ۲. واحد پردازش مرکزی (CPU – Central Processing Unit) ----- ۱۴۳ -
- ۳. حافظه دسترسی تصادفی (RAM – Random Access Memory) ----- ۱۴۳ -
- ۴. واحد پردازش گرافیکی (GPU – Graphics Processing Unit) ----- ۱۴۴ -
- ۵. دستگاه‌های ذخیره‌سازی (Storage Devices) ----- ۱۴۴ -
- ۶. منبع تغذیه (PSU – Power Supply Unit) ----- ۱۴۵ -
- ۷. سیستم خنک‌کننده (Cooling System) ----- ۱۴۵ -

اجزای جانبی و تکمیلی در رایانه‌های مدرن ----- ۱۴۶ -

رابطه بین اجزای داخلی ----- ۱۴۶ -

اهمیت اجزای داخلی در کارایی سیستم ----- ۱۴۶ -

واحد پردازش مرکزی (CPU – Central Processing Unit) ----- ۱۴۶ -

سازندگان CPU و تنوع آن‌ها ----- ۱۴۶ -

- شرکت Intel اینتل ----- ۱۴۷ -
- شرکت AMD ای‌ام‌دی Advanced Micro Devices ----- ۱۴۷ -
- شرکت ARM (ARM Holdings) ----- ۱۴۸ -
- Apple Silicon ----- ۱۴۸ -

پردازنده‌ها در دستگاه‌های مک (Mac Processors) ----- ۱۴۹ -

- مک‌های مبتنی بر پردازنده‌های Intel (تا ۲۰۲۰) ----- ۱۴۹ -
- مهاجرت به Apple Silicon از ۲۰۲۰ به بعد ----- ۱۵۰ -
- نسل‌های Apple Silicon ----- ۱۵۰ -

CPU در دستگاه‌های موبایل (Smartphones & Tablets) ----- ۱۵۱ -

- عملکرد و ویژگی‌های CPU ----- ۱۵۱ -

مادربرد (Motherboard) یا System Board ----- ۱۵۱ -

فرم‌ویر Firmware ----- ۱۵۲ -

حافظه (MEMORY) ----- ۱۵۳ -

- ویژگی مهم – RAM ناپایداری (Volatility) ----- ۱۵۳ -

درایوهای دیسک (DISK DRIVES) ----- ۱۵۳ -

کارت‌های شبکه (NETWORK INTERFACE CARDS – NIC) ----- ۱۵۴ -

واحد پردازش گرافیکی (GPU – Graphics Processing Unit) ----- - ۱۵۴ -

برق و خنک سازی (POWER AND COOLING) ----- - ۱۵۵ -

نیاز به خنک سازی (Cooling) : ----- - ۱۵۵ -

فصل ۷ ----- - ۱۵۸ -

انواع خدمات اینترنت (Internet Service Types) ----- - ۱۵۸ -

انواع متداول خدمات اینترنتی ----- - ۱۵۸ -

Dial-up دیال آپ ----- - ۱۵۸ -

DSL (Digital Subscriber Line) خط دیجیتال مشترک ----- - ۱۵۸ -

Cable Internet اینترنت کابلی ----- - ۱۵۹ -

Fiber-Optic Internet اینترنت فیبر نوری ----- - ۱۵۹ -

Satellite Internet اینترنت ماهواره ای ----- - ۱۵۹ -

Cellular Internet اینترنت سلولار - اینترنت موبایل ----- - ۱۵۹ -

Leased Line خط اختصاصی اجاره ای ----- - ۱۵۹ -

Broadband (باند پهن) چیست؟ ----- - ۱۶۰ -

تفاوت Broadband با Dial-up ----- - ۱۶۰ -

ویژگی های کلیدی Broadband ----- - ۱۶۰ -

انواع فناوری های Broadband ----- - ۱۶۱ -

Dial-up Modems مودم های دیال آپ ----- - ۱۶۲ -

مودم (Modem) چیست؟ ----- - ۱۶۲ -

صدای مودم های دیال آپ ----- - ۱۶۳ -

DSL (Digital Subscriber Line) خط دیجیتال مشترک ----- - ۱۶۳ -

تعریف DSL ----- - ۱۶۴ -

تفاوت اصلی DSL با Dial-up ----- - ۱۶۴ -

انواع DSL ----- - ۱۶۴ -

نحوه کار DSL ----- - ۱۶۴ -

Cable Internet اینترنت کابلی ----- - ۱۶۵ -

Coaxial Cable (کابل کوآکسیال) چیست؟ ----- - ۱۶۶ -

DOCSIS ----- - ۱۶۶ -

Fiber-Optic Internet اینترنت فیبر نوری ----- - ۱۶۷ -

ساختار کابل فیبر نوری ----- - ۱۶۸ -

ویژگی های اصلی اینترنت فیبر نوری ----- - ۱۶۸ -

نحوه عملکرد اینترنت فیبر نوری ----- - ۱۶۹ -

استانداردهای اینترنت فیبر نوری ----- - ۱۶۹ -

اتصالات بی سیم Wireless Connections ----- - ۱۷۰ -

انواع اتصالات بی سیم ----- - ۱۷۱ -

Wi-Fi وای فای ----- - ۱۷۱ -

Bluetooth بلوتوث ----- - ۱۷۱ -

شبکه های سلولی: G/4G/5G Cellular Networks ----- - ۱۷۱ -

Satellite Internet (اینترنت ماهواره ای) ----- - ۱۷۲ -

- ۱۷۲ - Infrared مادون قرمز
- ۱۷۲ - امنیت در ارتباطات بی سیم
- ۱۷۲ - کاربردهای ارتباطات بی سیم
- ۱۷۳ - اینترنت ماهواره‌ای و پوشش جهانی
- ۱۷۳ - اینترنت اشیاء (IoT) و نیاز به اتصال سریع و ایمن
- ۱۷۳ - نقش Edge Computing در شبکه‌های آینده
- ۱۷۳ - اساس ارتباطات بی سیم (Radio Frequency (RF)
- ۱۷۴ - امنیت و چالش‌های فناوری‌های بی سیم
- ۱۷۴ - کاربردهای عملی و تحول در زندگی روزمره
- ۱۷۴ - کاربردهای RF در IT و شبکه
- ۱۷۴ - مزایای RF (Radio Frequency)
- ۱۷۵ - معایب RF (Radio Frequency)
- ۱۷۵ - امنیت در RF
- ۱۷۵ - اینترنت ماهواره‌ای (Satellite Internet)
- ۱۷۵ - ترکیب RF و اینترنت ماهواره‌ای
- ۱۷۵ - نحوه کار اینترنت ماهواره‌ای
- ۱۷۶ - انواع ماهواره‌ها برای اینترنت
- ۱۷۶ - امنیت اینترنت ماهواره‌ای

فصل ۸ - ذخیره‌سازی (Storage)

- ۱۷۹ - ذخیره‌سازی فرّار یا Volatile Storage
- ۱۷۹ - ویژگی‌های RAM
- ۱۸۰ - نسل‌های مختلف RAM
- ۱۸۰ - Nonvolatile Storage ذخیره‌سازی غیرفرّار
- ۱۸۰ - ویژگی‌های ذخیره‌سازی غیرفرّار
- ۱۸۰ - انواع حافظه غیرفرّار
- ۱۸۰ - رابطه RAM و حافظه غیرفرّار
- ۱۸۱ - روش‌های اندازه‌گیری Nonvolatile Storage
- ۱۸۱ - هارد دیسک‌های مغناطیسی
- ۱۸۱ - نحوه کار HDD
- ۱۸۲ - Solid-State Drives (SSD) درایوهای حالت جامد
- ۱۸۲ - Flash Drives
- ۱۸۳ - ویژگی‌های Flash Drives
- ۱۸۳ - Secure Digital (SD) Cards
- ۱۸۴ - نسل‌ها و استانداردها SD Card ها
- ۱۸۴ - معماری SD Card
- ۱۸۵ - Optical Drives درایوهای نوری
- ۱۸۸ - انواع دیسک‌های نوری

خدمات ذخیره‌سازی سازمانی (Enterprise Storage Services)	۱۹۰ -
ذخیره‌سازی ابری Cloud Storage	۱۹۱ -
نسل‌ها و انواع Cloud Storage	۱۹۱ -
ویژگی‌های Cloud Storage :	۱۹۳ -
سرورهای فایل File Servers	۱۹۳ -
ذخیره‌سازی متصل به شبکه (Network Attached Storage (NAS)	۱۹۳ -
آرایه‌های افزونه دیسک RAID	۱۹۴ -
نسل‌ها و انواع RAID	۱۹۴ -
فصل ۹	۱۹۸ -
دستگاه‌های محاسباتی (Computing Devices)	۱۹۸ -
کامپیوترهای دسکتاپ – Desktop Computers	۱۹۸ -
Workstations ایستگاه‌های کاری	۱۹۸ -
سرورها – Servers	۱۹۹ -
کاربردهای سرورهای کامپیوتری	۱۹۹ -
دستگاه‌های موبایل Mobile Devices	۲۰۰ -
ویژگی‌های Mobile Devices :	۲۰۰ -
لپ‌تاپ‌ها Laptop Computers	۲۰۱ -
کاربردهای لپ‌تاپ‌ها	۲۰۱ -
مزایای لپ‌تاپ‌ها	۲۰۲ -
معماری لپ‌تاپ‌ها	۲۰۲ -
روش کارکرد لپ‌تاپ‌ها	۲۰۲ -
ویژگی‌های لپ‌تاپ‌ها:	۲۰۲ -
گوشی‌های هوشمند Smartphones	۲۰۳ -
تبلت‌ها Tablets	۲۰۳ -
لپ‌تاپ‌های تبدیل‌شونده Convertible Laptops	۲۰۳ -
کنسول‌های بازی Gaming Consoles	۲۰۴ -
اینترنت اشیا (IoT – Internet of Things)	۲۰۴ -
دستگاه‌های IoT خانگی	۲۰۵ -
سیستم‌های خانه هوشمند:	۲۰۵ -
دستگاه‌های IoT در محیط کاری	۲۰۵ -
IoT در مراقبت‌های بهداشتی	۲۰۵ -
مزایا و چالش‌های IoT	۲۰۶ -
شبکه‌بندی (TCP/IP Networking) (TCP/IP)	۲۰۶ -
انواع شبکه‌ها (Network Types)	۲۰۶ -
کاربردهای شبکه‌های محلی	۲۰۷ -

- ۲۰۷ - معماری شبکه‌های محلی
- ۲۰۷ - شبکه‌های بی‌سیم (Wireless Networks)
- ۲۰۷ - کاربردهای شبکه‌های بی‌سیم
- ۲۰۸ - مزایای شبکه‌های بی‌سیم
- ۲۰۸ - معماری شبکه‌های بی‌سیم
- ۲۰۸ - روش کارکرد شبکه‌های بی‌سیم
- ۲۰۹ - شبکه‌های شخصی (PANs – Personal Area Networks)
- ۲۰۹ - مزایا و اهمیت شبکه‌ها
- ۲۰۹ - شبکه‌بندی (TCP/IP Networking)
- ۲۱۰ - TCP/IP چیست؟
- ۲۱۰ - تاریخچه TCP/IP
- ۲۱۰ - کاربردهای TCP/IP
- ۲۱۰ - مزایای TCP/IP
- ۲۱۱ - ۵. معماری TCP/IP لایه‌ها
- ۲۱۱ - (Transmission Control Protocol (TCP
- ۲۱۲ - (Internet Control Message Protocol (ICMP
- ۲۱۲ - آدرس‌دهی شبکه (Network Addressing)
- ۲۱۲ - آدرس‌های IP (IP Addresses)
- ۲۱۲ - تعریف آدرس IP
- ۲۱۳ - تاریخچه و تکامل آدرس‌های IP
- ۲۱۳ - ساختار آدرس‌های IP
- ۲۱۳ - IPv4, ۱
- ۲۱۳ - کلاس‌های آدرس IPv4
- ۲۱۳ - IPv6, ۲
- ۲۱۳ - مزایای IPv6 نسبت به IPv4
- ۲۱۴ - انواع آدرس‌های IP
- ۲۱۴ - کاربردهای آدرس‌های IP
- ۲۱۴ - مزایای سیستم آدرس‌دهی IP
- ۲۱۴ - روش کارکرد آدرس‌های IP
- ۲۱۵ - MAC Address آدرس کنترل دسترسی رسانه
- ۲۱۵ - تعریف MAC Address
- ۲۱۵ - تاریخچه MAC Address
- ۲۱۵ - ساختار MAC Address
- ۲۱۷ - نحوه استفاده از آدرس‌های IP در شبکه
- ۲۱۷ - آدرس‌های IP در ارتباطات شبکه
- ۲۱۷ - روش‌های تخصیص IP Address

شناسایی آدرس‌های معتبر IPv4	- ۲۱۸ -
قوانین شناسایی آدرس‌های معتبر IPv4	- ۲۱۸ -
آدرس‌های (MAC (Media Access Control Addresses	- ۲۱۸ -
(Domain Name System (DNS	- ۲۱۹ -
۳٫۲ رکوردهای DNS	- ۲۱۹ -
پروتکل تفکیک آدرس (Address Resolution Protocol – ARP)	- ۲۲۰ -
کاربردهای ARP	- ۲۲۰ -
معماری ARP	- ۲۲۰ -
وب‌سایت‌ها و پروتکل‌های وب	- ۲۲۱ -
پروتکل HTTP	- ۲۲۱ -
امن‌HTTP HTTPS	- ۲۲۲ -
زبان‌های طراحی و نمایش صفحات وب	- ۲۲۲ -
ایمیل و پروتکل‌های مرتبط	- ۲۲۲ -
چگونگی کارکرد ایمیل	- ۲۲۳ -
دریافت ایمیل و پروتکل‌ها	- ۲۲۳ -
نسخه‌های امن پروتکل‌های ایمیل	- ۲۲۳ -
پروتکل‌های برنامه کاربردی (Application Protocols)	- ۲۲۴ -
FTP و SFTP انتقال فایل	- ۲۲۴ -
DNS سیستم نام دامنه	- ۲۲۴ -
DHCP پروتکل پیکربندی خودکار شبکه	- ۲۲۴ -
MQTT پروتکل پیام‌رسانی سبک برای IoT	- ۲۲۵ -
Telnet و SSH دسترسی از راه دور	- ۲۲۵ -
سوئیچ‌ها (Switches)	- ۲۲۵ -
نحوه عملکرد سوئیچ‌ها	- ۲۲۶ -
سوئیچ‌ها و اتصال دستگاه‌ها	- ۲۲۶ -
انواع سوئیچ‌ها	- ۲۲۶ -
پروتکل مدیریت ساده شبکه (SNMP – Simple Network Management Protocol)	- ۲۲۷ -
عملکرد و مزایای SNMP	- ۲۲۸ -
کاربردهای SNMP	- ۲۲۸ -
SNMP و سایر پروتکل‌ها	- ۲۲۸ -
فایروال‌ها (Firewalls)	- ۲۲۹ -
نحوه عملکرد فایروال‌ها	- ۲۲۹ -
نقاط دسترسی (Access Points)	- ۲۳۰ -
عملکرد نقاط دسترسی	- ۲۳۱ -
انواع نقاط دسترسی	- ۲۳۱ -
مزایا و اهمیت نقاط دسترسی	- ۲۳۲ -
شبکه‌های بی‌سیم (Wireless Networking)	- ۲۳۳ -

۲۳۳ -	اتصال شبکه‌های بی‌سیم به شبکه‌های سیمی
۲۳۴ -	استانداردهای شبکه بی‌سیم
۲۳۵ -	بازه‌های فرکانسی (Frequency Ranges)
۲۳۵ -	استانداردهای ۸۰۲.۱۱ (802.11 Standards)
۲۳۵ -	توضیح تخصصی: آنتن‌های MIMO
۲۳۶ -	خلاصه استانداردها و سرعت‌ها
۲۳۶ -	انتشار سیگنال‌های بی‌سیم (Wireless Signal Propagation)
۲۳۷ -	آنتن‌های بی‌سیم (Wireless Antennas)
۲۳۸ -	محل قرارگیری دستگاه‌های بی‌سیم (Wireless Device Placement)
۲۳۸ -	تداخل (Interference)
۲۳۸ -	امنیت شبکه‌های بی‌سیم (Wireless Security)
۲۳۹ -	SSID
۲۳۹ -	رمز عبور نقاط دسترسی (Access Point Passwords)
۲۳۹ -	کنترل دسترسی بی‌سیم (Wireless Access Control)
۲۴۰ -	رمزنگاری شبکه‌های بی‌سیم (Wireless Encryption)
۲۴۱ -	(Wired Equivalent Privacy (WEP
۲۴۱ -	توضیح تخصصی: WEP و آسیب‌پذیری‌ها
۲۴۱ -	(Wi-Fi Protected Access (WPA
۲۴۱ -	(Wi-Fi Protected Access v2 (WPA2
۲۴۱ -	توضیح تخصصی: AES و CCMP
۲۴۱ -	(Wi-Fi Protected Access v3 (WPA3
۲۴۲ -	استفاده از VPN برای افزایش امنیت
۲۴۴ -	فصل ۱۰
۲۴۴ -	سیستم عامل
۲۴۴ -	مدیریت دیسک
۲۴۴ -	مدیریت حافظه
۲۴۵ -	مدیریت پردازش و زمان‌بندی
۲۴۵ -	مدیریت برنامه‌ها
۲۴۵ -	مدیریت دستگاه‌ها
۲۴۶ -	کنترل دسترسی و حفاظت
۲۴۶ -	انواع سیستم‌عامل‌ها
۲۴۶ -	سیستم‌عامل‌های دسکتاپ

سیستم عامل های موبایل	۲۴۷
سیستم عامل های سرور	۲۴۷
سیستم عامل های تعبیه شده (Embedded)	۲۴۷
مجازی سازی (Virtualization) و سرورهای مجازی (Virtual Servers)	۲۴۸
هایپروایزرها (Hypervisors)	۲۴۹
انواع هایپروایزرها:	۲۴۹
کاربرد مجازی سازی در محیط های سازمانی	۲۴۹
تاریخچه مجازی سازی و تحولات آن در دهه گذشته	۲۵۰
بررسی کامل انواع هایپروایزرها و مقایسه مزایا و معایب آن ها	۲۵۱
هایپروایزر نوع اول (Type 1 / Bare-metal Hypervisor)	۲۵۱
هایپروایزر نوع دوم (Type 2 / Hosted Hypervisor)	۲۵۱

جزئیات عملکرد ماشین های مجازی و تعامل آن ها با سخت افزار ۲۵۲

مزیت تعامل با سخت افزار: ۲۵۲

فصل ۱۱ - ۲۵۶ -

فایل ها و سیستم های فایل (Files and Filesystems) - ۲۵۶ -

نمونه های معروف سیستم فایل - ۲۵۶ -

عملکرد سیستم فایل و نقش سیستم عامل - ۲۵۶ -

ساختار فایل ها و سازمان دهی داده ها - ۲۵۷ -

انواع سیستم فایل و کاربرد آن ها - ۲۵۷ -

تعامل سیستم فایل با سخت افزار و نرم افزار - ۲۵۸ -

فایل ها و پوشه ها (Files and Folders) - ۲۵۸ -

نام فایل ها و پسوندها (Filenames and Extensions) - ۲۵۸ -

تعامل سیستم فایل ها با سخت افزار و نرم افزار - ۲۶۰ -

ویژگی های سیستم فایل (Filesystem Features) - ۲۶۰ -

فشرده سازی (Compression) - ۲۶۰ -

نحوه عملکرد فشرده سازی: - ۲۶۰ -

توضیح تخصصی: - ۲۶۰ -

رمزگذاری (Encryption) - ۲۶۱ -

ژورنالینگ (Journaling) - ۲۶۱ -

ویژگی های مهم سیستم فایل ها - ۲۶۱ -

تعامل با کاربران و نرم افزارها - ۲۶۲ -

انواع سیستم فایل ها (Filesystem Types) - ۲۶۲ -

NTFS - ۲۶۲ -

- ۲۶۲ -	FAT32
- ۲۶۳ -	ext4
- ۲۶۳ -	سیستم فایل های اپل (Apple Filesystems)
- ۲۶۴ -	سیستم عامل و مدیریت برنامه ها (Operating Systems and Applications)
- ۲۶۴ -	برنامه ها (Applications)
- ۲۶۴ -	فایل اجرایی (Executable File):
- ۲۶۵ -	فرآیندها (Processes)
- ۲۶۵ -	ابزارهای نظارت بر فرآیندها
- ۲۶۵ -	خدمات (Services)
- ۲۶۶ -	تعامل فرآیندها، خدمات و سیستم عامل
- ۲۶۶ -	درایورها (Drivers)
- ۲۶۶ -	رابط ها (Interfaces)
- ۲۶۶ -	رابط گرافیکی کاربر (GUI – Graphical User Interface)
- ۲۶۷ -	رابط خط فرمان (CLI – Command Line Interface)
- ۲۶۷ -	نقش رابط ها و درایورها در عملکرد سیستم
- ۲۶۸ -	ابزارهای سیستم عامل (Utilities)
- ۲۶۸ -	زمان بندی وظایف (Task Scheduling)
- ۲۶۹ -	نرم افزارها و نقش آن ها در کامپیوترها (Software and Its Role in Computers)
- ۲۶۹ -	نرم افزارهای بهره دوری (Productivity Software)
- ۲۷۰ -	نرم افزارهای همکاری (Collaboration Software)
- ۲۷۰ -	نرم افزارهای کسب و کار (Business Software)
- ۲۷۱ -	نرم افزارهای بهره دوری (Productivity Software)
- ۲۷۲ -	نرم افزارهای همکاری (Collaboration Software)
- ۲۷۲ -	نرم افزارهای کسب و کار (Business Software)
- ۲۷۳ -	نرم افزارهای نصب شده به صورت محلی
- ۲۷۴ -	نرم افزارهای میزبانی شده روی شبکه محلی (Local Network–Hosted Applications)
- ۲۷۴ -	نرم افزارهای میزبانی شده در فضای ابری (Cloud–Hosted Applications)
- ۲۷۵ -	معماری نرم افزار (Application Architecture)
- ۲۷۵ -	نرم افزارهای یک لایه (One–Tier Applications)
- ۲۷۶ -	نرم افزارهای دو لایه (Two–Tier Applications)
- ۲۷۶ -	نرم افزارهای سه لایه (Three–Tier Applications)
- ۲۷۷ -	نرم افزارهای n–لایه (n–Tier Applications)
- ۲۷۹ -	فصل ۱۲

نحوه عملکرد وب - ۲۷۹ -

- ۲۷۹ - پروتکل HTTP و HTTPS
- ۲۷۹ - فرآیند دسترسی به وب
- ۲۷۹ - معماری دو لایه ای وب
- ۲۷۹ - سازگاری مرورگرها
- ۲۸۰ - جزئیات تخصصی مرورگرها
- ۲۸۰ - زبان HTML
- ۲۸۰ - مرورگرها و امنیت
- ۲۸۰ - انواع درخواست های HTTP
- ۲۸۱ - نکات کاربردی برای توسعه دهندگان وب
- ۲۸۱ - پیکربندی مرورگرهای وب
- ۲۸۱ - حافظه پنهان مرورگر (Web Cache)
- ۲۸۲ - اهمیت کش و کوکی ها در عملکرد و امنیت
- ۲۸۲ - تنظیمات دیگر مرورگرها
- ۲۸۳ - مرور خصوصی (Private Browsing)
- ۲۸۳ - نکات تخصصی درباره مرور خصوصی
- ۲۸۳ - غیر فعال کردن اسکریپت های سمت کلاینت (Deactivate Client-Side Scripting)
- ۲۸۳ - نحوه پیکربندی مسدودکننده اسکریپت در Chrome
- ۲۸۴ - اهمیت مرور خصوصی و کنترل اسکریپت ها در امنیت وب
- ۲۸۴ - افزونه ها و افزودنی های مرورگر (Browser Add-Ons)
- ۲۸۵ - پنجره های پاپ آپ (Pop-Ups)
- ۲۸۶ - سرورهای پروکسی (Proxy Servers)
- ۲۸۷ - گواهی های دیجیتال (Digital Certificates)
- ۲۸۷ - نقش گواهی های دیجیتال در HTTPS
- ۲۸۷ - هشدارهای مرتبط با گواهی های دیجیتال

فصل ۱۳ - ۲۹۰ -

سازگاری نرم افزارها (Software Compatibility) - ۲۹۰ -

- ۲۹۱ - اهمیت سازگاری نرم افزار در سازمان ها
- ۲۹۱ - بهترین شیوه های نصب نرم افزار (Software Installation Best Practices)
- ۲۹۱ - مجوزهای نرم افزاری (Software Licensing)
- ۲۹۲ - انواع مجوزهای نرم افزار مالکیتی
- ۲۹۲ - مدل های پرداخت و اشتراک

۲۹۲ -	کلیدهای محصول (Product Key / Serial Number)
۲۹۳ -	زبان‌های برنامه‌نویسی و دسته‌بندی‌های آن‌ها
۲۹۳ -	کدهای تفسیر شده
۲۹۳ -	زبان‌های اسکریپتی
۲۹۴ -	زبان‌های نشانه‌گذاری
۲۹۴ -	کدهای کامپایل شده (Compiled Code)
۲۹۵ -	زبان‌های تخصصی (Specialized Languages)
۲۹۵ -	زبان‌های اسمبلی
۲۹۵ -	زبان‌های پرس و جو
۲۹۶ -	شناسایی زبان‌های برنامه‌نویسی (Identifying Languages)
۲۹۶ -	زبان‌های تفسیر شده (Interpreted Languages)
۲۹۷ -	زبان‌های کامپایل شده (Compiled Languages)
۲۹۷ -	زبان‌های پرس و جو (Query Languages)
۲۹۷ -	زبان‌های اسمبلی (Assembly Languages)
۲۹۸ -	((Pseudocode
۳۰۰ -	فلوچارت‌ها (Flowcharts)
۳۰۰ -	نمادهای اصلی فلوچارت
۳۰۲ -	فلوچارت‌ها (Flowcharts)
۳۰۲ -	نمادهای اصلی فلوچارت
۳۰۳ -	متغیرها و آرایه‌ها (Variables and Arrays)
۳۰۴ -	متغیرها (Variables)
۳۰۴ -	آرایه‌ها (Arrays)
۳۰۵ -	انواع داده‌ها (Data Types)
۳۰۵ -	داده‌های متنی (Text Data)
۳۰۵ -	کدپستی (ZIP Codes)
۳۰۵ -	داده‌های بولی (Boolean Data)
۳۰۵ -	توابع (Functions)
۳۰۶ -	اشیاء (Objects)
۳۰۶ -	پایگاه داده‌ها (Databases)
۳۰۶ -	پایگاه داده‌ها در مقابل فایل‌های تخت (Databases vs. Flat Files)
۳۰۷ -	مراحل اصلی کار با داده‌ها در پایگاه داده‌ها
۳۰۹ -	ساختار بندی داده‌ها (Structuring Data)

- ۳۰۹ - (Structured Data داده‌های ساختاریافته)
- ۳۰۹ - (Relational Databases پایگاه داده‌های رابطه‌ای)
- ۳۱۰ - (Unstructured Data داده‌های بدون ساختار)
- ۳۱۰ - منابع داده‌های بدون ساختار
- ۳۱۰ - تحلیل و استفاده از داده‌های بدون ساختار
- ۳۱۱ - (Relational Databases پایگاه داده‌های رابطه‌ای)
- ۳۱۱ - (Database Keys کلیدهای پایگاه داده)
- ۳۱۱ - (Primary Key کلید اصلی)
- ۳۱۱ - (Foreign Key کلید خارجی)
- ۳۱۳ - (SQL زبان پرس‌وجوی ساختاریافته)
- ۳۱۳ - (DDL زبان تعریف داده‌ها)
- ۳۱۴ - (Data Manipulation Language – DML زبان دستکاری داده‌ها)
- ۳۱۵ - (Database Access Methods روش‌های دسترسی به پایگاه داده)
- ۳۱۵ - SQL نوشتن دستورات
- ۳۱۵ - (Query and Report Builders ابزارهای ساخت پرس‌وجو و گزارش)
- ۳۱۵ - (Exporting Data ارسال داده‌ها)
- ۳۱۵ - (Programmatic Interactions تعامل برنامه‌ای)

فصل ۱۴ - - ۳۱۸ - مثلث CIA (CIA Triad) - - ۳۱۸ -

- ۳۱۹ - (Confidentiality محرمانگی)
- ۳۲۱ - (Integrity صحت اطلاعات)
- ۳۲۲ - (Availability دسترسی‌پذیری)
- ۳۲۴ - (Device Security امنیت دستگاه‌ها)
- ۳۲۵ - (Antivirus Software نرم‌افزارهای ضد ویروس)
- ۳۲۵ - وظایف نرم‌افزار ضد ویروس
- ۳۲۵ - (Host Firewalls فایروال‌های میزبان)
- ۳۲۵ - عملکرد فایروال‌های میزبان
- ۳۲۵ - (Passwords رمزهای عبور)
- ۳۲۶ - (Updates and Patching به‌روزرسانی و پیچ)
- ۳۲۶ - (Safe Web Browsing Practices رعایت اصول مرور امن وب)
- ۳۲۷ - مقایسه فایروال میزبان و شبکه
- ۳۲۷ - روش‌های پیشرفته احراز هویت

- سناریوهای واقعی از شکست امنیتی به دلیل عدم به روزرسانی - ۳۲۸ -
- ابزارهای مدیریت متمرکز امنیت دستگاه‌ها - ۳۲۸ -
- امنیت نرم افزار (Software Security) - ۳۲۹ -
- منابع نرم افزار (Software Sources) - ۳۲۹ -
- حذف نرم افزار (Removal of Software) - ۳۲۹ -
- حریم خصوصی (Privacy) - ۳۳۰ -
- انواع اطلاعات خصوصی - ۳۳۱ -
- انتظار از حریم خصوصی - ۳۳۱ -
- سیاست‌ها و روش‌های امنیتی (Security Policies and Procedures) - ۳۳۱ -
- سیاست‌ها و چارچوب‌های امنیتی - ۳۳۲ -
- کنترل دسترسی (Access Control) - ۳۳۳ -
- شناسایی (Identification) - ۳۳۳ -
- احراز هویت (Authentication) - ۳۳۴ -
- مجوزدهی (Authorization) - ۳۳۴ -
- احراز هویت و مجوزدهی در دنیای دیجیتال - ۳۳۴ -
- حسابرسی و نظارت (Accounting) - ۳۳۴ -
- طراحی سیستم‌های کنترل دسترسی - ۳۳۵ -
- عوامل احراز هویت (Authentication Factors) - ۳۳۵ -
- چیزی که می‌دانید (Something You Know) - ۳۳۶ -
- چیزی که هستید (Something You Are) - ۳۳۶ -
- چیزی که دارید (Something You Have) - ۳۳۶ -
- احراز هویت مبتنی بر مکان (Location-Based Authentication) - ۳۳۷ -
- احراز هویت چند عاملی (Multifactor Authentication – MFA) - ۳۳۷ -
- ورود یکپارچه (Single Sign-On – SSO) - ۳۳۷ -
- مجوزدهی و مدل‌های کنترل دسترسی (Authorization and Access Control Models) - ۳۳۸ -
- اصل حداقل امتیاز (Principle of Least Privilege) - ۳۳۸ -
- مدل‌های مجوزدهی (Authorization Models) - ۳۳۸ -
- انواع حساب‌ها در سیستم‌های کنترل دسترسی (Account Types in Access Control Systems) - ۳۴۰ -
- حساب‌های کاربری عادی (User Accounts) - ۳۴۰ -
- حساب‌های مدیر سیستم (Administrator Accounts) - ۳۴۰ -
- حساب‌های مهمان (Guest Accounts) - ۳۴۱ -
- حساب‌های مشترک یا عمومی (Shared/Generic Accounts) - ۳۴۱ -

- ۳۴۱ - _____ (حساب‌های سرویس Service Accounts)
- ۳۴۲ - _____ (عدم انکار Nonrepudiation)
- ۳۴۲ - _____ (امضای دیجیتال Digital Signatures)
- ۳۴۴ - _____ (سیاست‌های رمز عبور Password Policies)
- ۳۴۴ - _____ (طول رمز عبور Password Length)
- ۳۴۴ - _____ (پیچیدگی رمز عبور Password Complexity)
- ۳۴۴ - _____ (انقضای رمز عبور Password Expiration)
- ۳۴۴ - _____ (تاریخچه رمز عبور Password History)
- ۳۴۴ - _____ (بازنشانی رمز عبور Password Resets)
- ۳۴۵ - _____ (عدم استفاده مجدد رمز عبور Password Reuse)
- ۳۴۵ - _____ (مدیران رمز عبور Password Managers)
- ۳۴۶ - _____ (رمزنگاری Cryptography)
- ۳۴۶ - _____ (رمزگذاری داده‌ها Encrypting Data)
- ۳۴۶ - _____ (رمزگشایی داده‌ها Decrypting Data)
- ۳۴۶ - _____ (کاربردهای رمزنگاری Uses of Encryption)
- ۳۴۷ - _____ (داده‌های ذخیره‌شده Data at Rest)
- ۳۴۷ - _____ (داده‌های در حال انتقال Data in Transit)

مقدمه

کتابی که پیش روی شماست، یکی از پایه‌ای‌ترین و مقدماتی‌ترین منابع برای آشنایی با مفاهیم اولیه کامپیوتر و فناوری اطلاعات (IT) است. این اثر به‌گونه‌ای تدوین شده که نقطه‌ی آغازین ورود به دنیای فناوری محسوب شود؛ به عبارت دیگر، می‌توان آن را قدم اول هر مسیر آموزشی در حوزه رایانه و IT دانست. مطالب این کتاب با زبانی ساده و قابل درک برای علاقه‌مندان، دانشجویان و هنرجویان تنظیم شده است و به‌عنوان پیش‌نیاز بسیاری از دوره‌ها و آموزش‌های تخصصی‌تر عمل می‌کند. بنابراین، مطالعه آن به شما کمک می‌کند تا بنیانی محکم برای یادگیری‌های بعدی خود بسازید و با مفاهیم کلیدی این حوزه به شکلی روان و کاربردی آشنا شوید.

امید است این کتاب بتواند برای شما، چه در آغاز راه یادگیری و چه به‌عنوان مرور مفاهیم اولیه، سودمند واقع شود و دریچه‌ای روشن به دنیای گسترده فناوری اطلاعات بگشاید.

اگر در حال آماده شدن برای آزمون (IT Fundamentals+) ITF+ هستید، ممکن است با حجم زیادی از اطلاعات روبرو شوید که گیج‌کننده باشد. این آزمون طیف بسیار گسترده‌ای از موضوعات را پوشش می‌دهد و ممکن است هفته‌ها طول بکشد تا هر کدام را به‌طور کامل مطالعه کنید. خوشبختانه، نیازی به این کار نیست. این کتاب طراحی شده است تا به شما کمک کند بر دانش خاصی تمرکز کنید که برای قبولی در آزمون های مبانی فناوری اطلاعات مثل CompTIA شرکت کنید.

آزمون ITF+

این گواهینامه را برای سه گروه پیشنهاد می‌کند:

- دانشجویانی که قصد شروع یک حرفه در فناوری اطلاعات را دارند
- حرفه‌ای‌هایی که در زمینه‌هایی کار می‌کنند که نیازمند درک فناوری اطلاعات است
- افراد شاغل در بخش فروش، بازاریابی و عملیات در شرکت‌های متمرکز بر IT

این آزمون شش حوزه اصلی دانش را پوشش می‌دهد:

۱. مفاهیم و اصطلاحات (IT Concepts and Terminology)

- شامل شناخت مفاهیم پایه‌ای IT و اصطلاحات رایج در صنعت فناوری اطلاعات

۲. زیرساخت (Infrastructure)

- شامل سخت‌افزار، شبکه‌ها، سرورها و سایر اجزای فیزیکی یا مجازی که IT روی آنها اجرا می‌شود

۳. برنامه‌ها و نرم‌افزار (Applications and Software)

- شامل نرم‌افزارهای کاربردی و نحوه استفاده از آنها

۴. مفاهیم توسعه نرم‌افزار (Software Development Concepts)

- شامل اصول پایه‌ای برنامه‌نویسی و چرخه عمر نرم‌افزار

۵. مبانی پایگاه داده (Database Fundamentals)

- شامل مفاهیم ذخیره، بازیابی و مدیریت داده‌ها

۶. امنیت (Security)

- شامل مباحث پایه‌ای امنیت اطلاعات، رمزنگاری و محافظت از داده‌ها

مخاطبین هدف این دوره چه کسانی هستند؟

این دوره به گونه‌ای طراحی شده است که طیف وسیعی از علاقه‌مندان و متخصصان فعال در حوزه فناوری اطلاعات را پوشش دهد. محتوای آموزشی از مبانی پایه شروع شده و تا موضوعات پیشرفته و کاربردی در محیط‌های enterprise ادامه می‌یابد. بنابراین برای افراد تازه کار و همچنین حرفه‌ای‌هایی که قصد تثبیت دانش و پر کردن خلاءهای علمی خود را دارند، کاملاً مناسب است.

- تازه‌واردان به دنیای لینوکس: افرادی که هیچ پیش‌زمینه‌ای ندارند و می‌خواهند یادگیری لینوکس را از پایه‌ترین مفاهیم به صورت اصولی و کاربردی آغاز کنند.
- جامعه توسعه‌دهندگان و مهندسين نرم‌افزار: برنامه‌نویسان، توسعه‌دهندگان وب و مهندسين سين نرم‌افزار که برای توسعه، استقرار (Deploy) و عیب‌یابی (Debug) برنامه‌های خود نیاز به تسلط بر محیط سرورهای لینوکس و خط فرمان (Terminal) دارند.
- متخصصان DevOps و ابر (Cloud): کارشناسان DevOps، مهندسين سين (SRE) Site Reliability و متخصصان Cloud که اسکریپت‌نویسی، اتوماسیون، مدیریت زیرساخت به‌عنوان کد (IaC) و کار با سرویس‌های ابری مانند AWS، Azure و GCP در هسته مرکزی فعالیت آن‌ها قرار دارد.
- متخصصان و مدیران شبکه: مدیران شبکه، مهندسين سين زیرساخت IT، کارشناسان NOC و آنالیزورهای شبکه که برای مدیریت روترها، سوئیچ‌ها، فایروال‌ها و سرویس‌های تحت شبکه (مانند DNS, DHCP, Proxy) به لینوکس به‌عنوان یک ابزار حیاتی نیاز دارند.
- حرفه‌ای‌های امنیت سایبری: کارشناسان تست نفوذ (Penetration Testers)، هکرها (Ethical Hackers)، متخصصان امنیت اطلاعات (SOC Analysts) و پاسخ به حوادث (Incident Responders) که برای تحلیل تهدیدات، بررسی لاگ‌ها و استفاده از ابزارهای امنیتی، نیازمند تسلط عمیق بر سیستم عامل لینوکس هستند.
- تیم‌های پشتیبانی فنی و عملیات: تکنسین‌های پشتیبانی (Help Desk)، متخصصان صین پشتیبانی سرور و اپراتورهای دیتاسنتر که وظیفه عیب‌یابی، مانیتورینگ سلامت سرویس‌ها و انجام عملیات اولیه را بر عهده دارند.
- مشاوران و مدیران فناوری اطلاعات: مشاوران IT و شبکه، مدیران فنی و مدیران ارشد فناوری اطلاعات (CTOs) که برای تصمیم‌گیری‌های استراتژیک، انتخاب پلتفرم‌های مناسب و درک قابلیت‌های سیستم عامل لینوکس نیاز به دانش کافی دارند.
- دانشجویان و پژوهشگران: دانشجویان مقاطع مختلف در رشته‌های کامپیوتر، فناوری اطلاعات، مهندسی نرم‌افزار و شبکه که می‌خواهند دانش آکادمیک خود را با مهارت‌های عملی و مورد نیاز بازار کار تکمیل کنند.

فصل یکم

فصل ۱

سیستم‌های نشانه‌گذاری (Notational Systems)

کامپیوترها برای ذخیره و پردازش داده‌ها به صورت **دودویی (Binary)** طراحی شده‌اند. اما این فرمت معمولاً برای انسان‌ها یا نرم‌افزارها مناسب و راحت نیست. سیستم‌های نشانه‌گذاری به ما راه‌هایی ارائه می‌دهند تا از فناوری‌های ذخیره داده‌های دودویی برای نمایش اعداد، متن و سایر فرمت‌های داده‌ای استفاده کنیم.

• دودویی (Binary)
• هگزادسیمال (Hexadecimal)
• دهدهی (Decimal)
• نمایش داده‌ها (Data Representation)

بیت (Bit)

بیت (Bit) کوچک‌ترین و بنیادی‌ترین واحد اطلاعات در دنیای رایانه‌ها و سامانه‌های دیجیتال است. واژه‌ی «بیت» در واقع کوتاه شده‌ی عبارت **Binary Digit** به معنای «رقم دودویی» است و همان‌طور که از نامش برمی‌آید، تنها می‌تواند یکی از دو مقدار ممکن را در خود نگه دارد: صفر یا یک. همین دو مقدار ساده، یعنی صفر و یک، پایه و اساس کل دنیای فناوری دیجیتال را شکل می‌دهند. شاید در نگاه اول تصور شود که داشتن تنها دو حالت بسیار محدود و ناکافی است، اما در عمل با ترکیب همین دو حالت ساده می‌توان بی‌نهایت داده، از ساده‌ترین اعداد تا پیچیده‌ترین تصاویر سه‌بعدی و حتی ویدئوهای با کیفیت ۸K را در رایانه‌ها ذخیره و پردازش کرد. قدرت واقعی بیت‌ها در همین ترکیب و کنار هم قرار گرفتن‌شان نهفته است. وقتی چند بیت کنار هم قرار می‌گیرند، تعداد حالات ممکن به صورت نمایی افزایش پیدا می‌کند. به عنوان مثال یک بیت می‌تواند دو حالت داشته باشد، دو بیت چهار حالت، سه بیت هشت حالت و هشت بیت یا همان یک بایت می‌تواند ۲۵۶ حالت مختلف را نمایش دهد. این افزایش نمایی سبب می‌شود که با تعداد نسبتاً کمی بیت بتوان مجموعه بزرگی از داده‌ها را نمایش داد.

اگر بخواهیم تاریخچه‌ی شکل‌گیری مفهوم بیت را بررسی کنیم، باید به نیمه‌ی قرن بیستم و کارهای کلود شانون (**Claude Shannon**) در حوزه‌ی نظریه اطلاعات بازگردیم. شانون در سال ۱۹۴۸ در مقاله‌ی مشهور خود تحت عنوان «نظریه‌ی ریاضی اطلاعات» مفهوم بیت را به عنوان واحد سنجش اطلاعات معرفی کرد. او نشان داد که هر پیام را می‌توان با استفاده از دنباله‌ای از انتخاب‌های دودویی بازنمایی کرد. این انتخاب‌ها می‌توانند پاسخ به سؤالاتی ساده باشند مانند «بله/خیر»، «روشن/خاموش»، «وجود دارد/وجود ندارد». همین ایده‌ی بنیادین باعث شد که بیت به واحد اصلی و استاندارد سنجش و ذخیره‌ی اطلاعات در علوم کامپیوتر و ارتباطات بدل شود. امروزه وقتی درباره‌ی ظرفیت حافظه‌ها، سرعت شبکه‌ها یا کلیدهای رمزنگاری صحبت می‌کنیم، همه‌ی این مفاهیم بر حسب بیت و بایت بیان می‌شوند.

بیت در عمل چگونه ذخیره می‌شود؟ پاسخ به این سوال بستگی به فناوری مورد استفاده در سخت‌افزار دارد. در هارد دیسک‌های مغناطیسی سنتی (HDD)، سطح دیسک از موادی مغناطیسی پوشیده شده است که می‌توانند خاصیت مغناطیسی بگیرند یا نداشته باشند. هد خواندن و نوشتن با تغییر وضعیت مغناطیسی نقاط ریز سطح دیسک، مقدار بیت‌ها را ثبت می‌کند. اگر در نقطه‌ای خاص میدان مغناطیسی وجود داشته باشد، آن را به عنوان «۱» در نظر می‌گیرند و اگر میدان وجود نداشته باشد، «۰» ذخیره می‌شود. در حافظه‌های حالت جامد یا همان SSD ها، مکانیزم کمی متفاوت است. در اینجا به جای مغناطیس از بار الکتریکی استفاده می‌شود. سلول‌های حافظه‌ی فلش می‌توانند الکترون ذخیره کنند یا خالی باشند. وجود بار الکتریکی در یک سلول به منزله‌ی مقدار «۱» و نبود آن نشان‌دهنده‌ی مقدار «۰» خواهد بود. در حافظه‌های موقتی مانند RAM نیز همین منطق برقرار است. با این تفاوت که داده‌ها تنها تا زمانی که برق وجود داشته باشد حفظ می‌شوند. به محض قطع جریان برق، بیت‌ها به حالت صفر بازمی‌گردند و تمام اطلاعات ذخیره‌شده از بین می‌رود.

بیت‌ها در دنیای رایانه‌ها به تنهایی کمتر استفاده می‌شوند و معمولاً در قالب گروه‌های بزرگ‌تر معنا پیدا می‌کنند. همان‌طور که گفته شد، رایج‌ترین گروه‌بندی، بایت است که از هشت بیت تشکیل شده است. دلیل انتخاب عدد هشت به عنوان استاندارد، توازن خوبی است که میان توانایی نمایش

- این دو بیت را می‌توان برای ذخیره اعداد صحیح از ۰ تا ۳ استفاده کرد.

به هر ترکیب دودویی یک **معادل عددی دهدهی (Decimal Equivalent)** اختصاص داده می‌شود:

مقدار دهدهی	مقدار دودویی
0	00
1	01
2	10
3	11

جدول ۱

داده‌های هگزادسیمال (Hexadecimal Data)

داده‌های هگزادسیمال یا Hexadecimal یکی از سیستم‌های عددی مهم در علوم کامپیوتر هستند که پایه و اساس نمایش داده‌ها و آدرس‌دهی حافظه به شمار می‌روند. این سیستم بر پایه عدد ۱۶ طراحی شده است و هر رقم آن می‌تواند یکی از ۱۶ مقدار ممکن را نشان دهد. از صفر تا پانزده. برای نمایش مقادیر ۱۰ تا ۱۵ از حروف A تا F استفاده می‌شود؛ به این ترتیب، A معادل ده، B معادل یازده، C معادل دوازده، D معادل سیزده، E معادل چهارده و F معادل پانزده است. این شیوه نمایش باعث می‌شود که مقادیر بزرگ‌تر از ۹ تنها با یک رقم نمایش داده شوند و نمایش داده‌ها کوتاه‌تر و خواناتر شود. استفاده از هگزادسیمال باعث می‌شود رشته‌های طولانی دودویی که برای انسان دشوار هستند، به فرم ساده و قابل درک تبدیل شوند.

سیستم هگزادسیمال نقش واسطه‌ای میان داده‌های دودویی و نمایش انسانی آن‌ها دارد. در واقع، هر بایت داده که از هشت بیت تشکیل شده است، می‌تواند با دو رقم هگزادسیمال نمایش داده شود. به این ترتیب، رشته‌های طولانی از صفر و یک که در حافظه ذخیره شده‌اند، به شکل قابل فهم‌تری برای برنامه‌نویسان و مهندسان نمایش داده می‌شوند. این ویژگی باعث می‌شود که هگزادسیمال به ابزاری ضروری برای کار با حافظه، دیباگ برنامه‌ها، طراحی سخت‌افزار و تحلیل سیستم‌های دیجیتال تبدیل شود.

یکی از دلایل اصلی استفاده از هگزادسیمال، کارایی و خوانایی آن در مقایسه با داده‌های دودویی است. در حالی که نمایش یک عدد بزرگ در قالب دودویی ممکن است به ده‌ها یا حتی صدها بیت نیاز داشته باشد، همان عدد در هگزادسیمال با تعداد کمتری رقم نمایش داده می‌شود. این ویژگی باعث صرفه‌جویی در فضا و زمان پردازش می‌شود و همچنین تحلیل و درک داده‌ها را برای انسان ساده‌تر می‌کند. مزیت دیگر استفاده از هگزادسیمال، قابلیت تبدیل آسان بین سیستم‌های عددی است. هر رقم هگزادسیمال معادل دقیق چهار بیت دودویی است. به عنوان مثال، رقم هگزادسیمال C معادل ۱۱۰۰ در دودویی است و رقم F معادل ۱۱۱۱. این ارتباط مستقیم بین هگزادسیمال و دودویی باعث می‌شود که تبدیل داده‌ها سریع و بدون خطا انجام شود و مهندسان و برنامه‌نویسان بتوانند داده‌های حافظه را به سرعت تحلیل کنند.

نمونه تبدیل اعداد

برای روشن‌تر شدن تفاوت میان سیستم‌های دهدهی، دودویی و هگزادسیمال، مثال‌هایی ارائه می‌شود:

مقدار دهدهی	مقدار دودویی	مقدار هگزادسیمال
0	0	0
5	101	5
10	1010	A
15	1111	F
123	1111011	7B
255	11111111	FF

جدول ۲

- در یک ترموستات هوشمند، سنسور دما ورودی فراهم می‌کند تا سیستم تصمیم بگیرد دما را تنظیم کند.

انواع ورودی (Types of Input) در محاسبات و فناوری اطلاعات

ورودی‌ها در سیستم‌های کامپیوتری به داده‌ها یا فرمان‌هایی گفته می‌شود که برای پردازش، تحلیل یا ذخیره به سیستم ارائه می‌شوند. بدون ورودی، هیچ پردازش یا خروجی‌ای تولید نمی‌شود و چرخه اطلاعاتی سیستم مختل خواهد شد. به طور کلی، ورودی‌ها را می‌توان به دو دسته اصلی تقسیم کرد: ورودی انسانی (Human Input) و ورودی ماشینی یا غیر انسانی (Non-Human Input). هر یک از این دسته‌ها دارای ویژگی‌ها، دستگاه‌ها و فناوری‌های مخصوص به خود هستند که در ادامه به تفصیل شرح داده می‌شوند.

ورودی انسانی (Human Input)

ورودی انسانی زمانی رخ می‌دهد که کاربران به صورت مستقیم داده‌ها یا فرمان‌ها را وارد سیستم می‌کنند. این داده‌ها می‌توانند به شکل متنی، عددی، صوتی، تصویری یا حتی حرکتی باشند. سیستم‌های کامپیوتری برای دریافت این داده‌ها از انواع مختلف دستگاه‌ها استفاده می‌کنند که هر کدام مکانیزم و کاربرد خاص خود را دارند.

الف) کیبورد (Keyboard)

کیبورد یکی از رایج‌ترین و قدیمی‌ترین دستگاه‌های ورودی است که برای وارد کردن داده‌های متنی و عددی استفاده می‌شود. کاربران با فشردن کلیدها اطلاعات را وارد سیستم می‌کنند و هر کلید با یک کد باینری در کامپیوتر نمایش داده می‌شود. CPU این کدها را پردازش کرده و به نرم‌افزار یا سیستم مربوطه ارسال می‌کند.

مثال عملی: تایپ کردن یک آدرس ایمیل، وارد کردن رمز عبور، نوشتن متن مقاله در نرم‌افزار Word یا وارد کردن داده‌های عددی در یک جدول Excel.

نکته آموزشی: در سوالات ITF+ ممکن است از شما خواسته شود تفاوت بین ورودی متنی و عددی را تشخیص دهید. کیبورد قادر است هر دو نوع داده را دریافت کند و به سیستم منتقل نماید.

ب) ماوس (Mouse)

ماوس دستگاهی است که حرکت آن روی سطح باعث تغییر موقعیت نشانگر روی صفحه نمایش می‌شود. کلیک کردن دکمه‌های ماوس فرمان‌ها را به سیستم ارسال می‌کند و امکان تعامل دقیق کاربر با رابط گرافیکی فراهم می‌شود.

مثال عملی: انتخاب یک آیکن روی دسکتاپ، کشیدن و رها کردن فایل‌ها بین پوشه‌ها، حرکت دقیق در بازی‌های کامپیوتری یا استفاده از ابزارهای گرافیکی برای طراحی.

اصطلاح تخصصی: Pointer (نشانگر) – نماد گرافیکی که موقعیت ماوس را روی صفحه نمایش نشان می‌دهد و حرکت آن توسط کاربر کنترل می‌شود.

ج) صفحه لمسی (Touchscreen)

با پیشرفت تلفن‌های هوشمند و تبلت‌ها، صفحات لمسی به یکی از رایج‌ترین دستگاه‌های ورودی تبدیل شده‌اند. کاربران با لمس صفحه، کشیدن انگشت یا استفاده از ژست‌های حرکتی (Gestures) داده‌ها را وارد سیستم می‌کنند. فناوری صفحه لمسی علاوه بر دقت، امکان تعامل مستقیم و طبیعی با دستگاه را فراهم می‌کند.

مثال عملی: باز کردن اپلیکیشن با لمس آیکن، اسکرول کردن صفحات وب، بزرگ‌نمایی تصاویر با حرکت دو انگشت یا کشیدن یک عکس در بازی‌ها.

اصطلاح تخصصی: Gesture Recognition (تشخیص ژست‌ها) – فناوری تشخیص حرکات دست و انگشت برای شناسایی ورودی و اجرای فرمان‌های دیجیتال.

د) ورودی صوتی (Voice Input)

ورودی صوتی به کاربران اجازه می‌دهد با گفتار خود داده یا فرمان‌ها را وارد سیستم کنند. سیستم صوتی باید صدا را دریافت، آن را به سیگنال دیجیتال تبدیل و پردازش کند تا فرمان یا داده مورد نظر به شکل قابل استفاده در بیاید. فناوری ورودی صوتی به ویژه در دستگاه‌های هوشمند و دستیارهای صوتی کاربرد دارد.

مثال عملی: استفاده از دستیارهای هوشمند مانند Siri، Alexa یا Google Assistant برای باز کردن اپلیکیشن‌ها، جستجو در اینترنت، ارسال پیام، ایجاد یادآوری یا کنترل دستگاه‌های خانگی هوشمند.

ورودی در دنیای واقعی

ورودی در دنیای واقعی نقش بسیار حیاتی در عملکرد سیستم‌های اطلاعاتی و فناوری دارد. سیستم‌ها بدون دریافت داده‌های دقیق و به موقع، قادر به پردازش درست و تولید خروجی قابل اعتماد نخواهند بود. اهمیت ورودی‌ها در کاربردهای مختلف IT و زندگی روزمره مشهود است و نمونه‌های متعددی نشان می‌دهند که دقت، سرعت و صحت داده‌های ورودی مستقیماً بر کیفیت عملکرد سیستم تأثیر می‌گذارد.

۱. سیستم‌های بانکی

در سیستم‌های بانکی، ورودی دقیق و صحیح برای اطمینان از صحت تراکنش‌های مالی حیاتی است. داده‌هایی مانند شماره حساب، مبلغ تراکنش و رمز عبور از جمله ورودی‌های حیاتی محسوب می‌شوند. هر خطا در ورود این داده‌ها می‌تواند منجر به اشتباهات مالی، برداشت‌های نادرست یا اختلال در حساب مشتریان شود. سیستم‌های بانکی برای دریافت ورودی‌ها از روش‌های مختلفی مانند کیبورد، کارت‌های بانکی با تراشه، دستگاه‌های ATM و حتی اپلیکیشن‌های موبایل استفاده می‌کنند. این ورودی‌ها باید به سرعت و با دقت کامل پردازش شوند تا امنیت تراکنش‌ها تضمین شود و تجربه کاربری مناسب برای مشتریان ایجاد گردد.

۲. بازی‌های ویدیویی

در بازی‌های ویدیویی، ورودی‌ها شامل کیبورد، ماوس، کنترلر و صفحات لمسی هستند که حرکات و فرمان‌های بازیکن را به سیستم منتقل می‌کنند. اهمیت این ورودی‌ها در پاسخ سریع و دقیق سیستم به عملکرد بازیکن است. تأخیر در پردازش ورودی یا خطا در دریافت آن می‌تواند تجربه کاربری را کاهش دهد و باعث نارضایتی بازیکنان شود. برای مثال، حرکت کاراکترها، انتخاب ابزارها، شلیک یا انجام حرکات ترکیبی در بازی‌ها به دقت بالای ورودی‌ها وابسته است. توسعه‌دهندگان بازی‌ها برای بهینه‌سازی این ورودی‌ها از الگوریتم‌های پیشرفته و پردازش سریع داده‌ها استفاده می‌کنند تا تعامل کاربر با بازی طبیعی و بدون تأخیر باشد.

۳. ترموستات‌های هوشمند و خانه‌های هوشمند

در سیستم‌های خانه هوشمند، ورودی‌ها توسط حسگرها و دستگاه‌های هوشمند جمع‌آوری می‌شوند. این ورودی‌ها می‌توانند شامل دما، رطوبت، حرکت افراد، روشنایی و حتی صدا باشند. بر اساس این داده‌ها، سیستم قادر است تصمیم‌گیری خودکار انجام دهد، مانند تنظیم دمای محیط، کنترل روشنایی، فعال یا غیرفعال کردن سیستم‌های امنیتی و صرفه‌جویی انرژی. اهمیت ورودی‌ها در این سیستم‌ها در ایجاد راحتی و صرفه‌جویی انرژی برای کاربران مشهود است. بدون دریافت داده‌های دقیق از محیط، سیستم نمی‌تواند تصمیمات مؤثر و بهینه اتخاذ کند و کارایی خانه هوشمند کاهش می‌یابد.

۴. سیستم‌های فروشگاه‌های و انبارداری

در سیستم‌های فروشگاه‌های و انبارداری، ورودی‌ها شامل اسکن بارکد، ورود دستی کالاها و داده‌های حسگرهای موجودی است. این ورودی‌ها برای مدیریت دقیق موجودی، پیشگیری از کمبود یا اضافه موجودی و تحلیل روند فروش ضروری هستند. به عنوان مثال، هر کالایی که وارد انبار می‌شود باید به سیستم معرفی گردد تا اطلاعات موجودی به روز شود. اسکن بارکد سرعت و دقت ورود داده‌ها را افزایش می‌دهد و خطاهای انسانی را کاهش می‌دهد. همچنین، داده‌های حسگرهای موجودی می‌توانند اطلاعاتی درباره تعداد واقعی کالاها، وضعیت انبار و سطح تقاضا ارائه دهند. استفاده از ورودی‌های دقیق در این سیستم‌ها موجب بهینه‌سازی مدیریت انبار، کاهش هزینه‌ها و افزایش رضایت مشتریان می‌شود.

اصطلاحات تخصصی

•	Input Device دستگاه ورودی: هر سخت‌افزاری که داده‌ها را به سیستم می‌رساند.
•	Keyboard کیبورد: دستگاه ورودی متنی و عددی.
•	Mouse ماوس: دستگاه ورودی موقعیت‌یاب و انتخابگر.
•	Touchscreen صفحه لمسی: ورودی لمسی و ژست حرکتی.
•	Voice Input ورودی صوتی: ورودی گفتاری.
•	Sensor حسگر: دستگاه تشخیص تغییرات محیطی.
•	IoT Sensors حسگرهای اینترنت اشیا: حسگرهایی که داده را به سیستم‌های اینترنتی ارسال می‌کنند.
•	Database Query پرس‌وجوی پایگاه داده: استخراج داده از پایگاه داده‌ها.
•	Network Input ورودی شبکه: دریافت داده از طریق شبکه‌های کامپیوتری.

معایب

۱. نیاز به پردازش برای فشرده‌سازی و بازگشایی: CPU و RAM مصرف می‌شود و ممکن است در سیستم‌های قدیمی باعث کندی شود.
۲. احتمال کاهش کیفیت: در فشرده‌سازی Lossy، مانند JPEG و MP3، بخشی از داده‌ها حذف شده و کیفیت کاهش می‌یابد.
۳. پیچیدگی در مدیریت داده‌ها: برای بازیابی و پردازش باید ابتدا داده‌ها بازگشایی شوند.

مثال‌های عملی ذخیره‌سازی فشرده

فشرده‌سازی فایل‌های متنی

فرض کنید یک سازمان میلیون‌ها سند متنی دارد که باید روی سرور ذخیره شود. با استفاده از الگوریتم ZIP، می‌توان حجم فایل‌ها را تا ۷۰٪ کاهش داد. بدون آنکه اطلاعات از دست برود. این کاهش حجم باعث می‌شود فضای ذخیره‌سازی کمتری نیاز باشد و عملیات پشتیبان‌گیری سریع‌تر انجام شود.

فشرده‌سازی تصاویر و ویدئو

در سرویس‌هایی مانند YouTube یا Netflix، میلیون‌ها ساعت ویدئو باید ذخیره و ارسال شود. با فشرده‌سازی ویدئو با H.264 و H.265، حجم فایل‌ها کاهش می‌یابد و کاربران می‌توانند با پهنای باند محدود، ویدئو را بدون تأخیر مشاهده کنند. مشابه آن، تصاویر PNG و JPEG در وبسایت‌ها استفاده می‌شوند تا صفحات سریع‌تر بارگذاری شوند.

فشرده‌سازی داده‌های پایگاه داده

در بانک‌ها یا سیستم‌های فروشگاهی، پایگاه داده‌ها شامل میلیون‌ها رکورد هستند. با استفاده از فشرده‌سازی در سطح پایگاه داده، حجم دیتابیس کاهش یافته و عملیات جستجو و انتقال داده‌ها بهینه می‌شود.

نکات تخصصی و اصطلاحات کلیدی

- **Lossless Compression** فشرده‌سازی بدون افت کیفیت: داده‌ها به طور کامل قابل بازیابی هستند، مانند ZIP و PNG.
- **Lossy Compression** فشرده‌سازی با افت کیفیت: بخشی از داده‌ها حذف می‌شوند تا حجم کمتر شود، مانند MP3 و JPEG.
- **Compression Ratio** نسبت فشرده‌سازی: نسبت اندازه فایل اصلی به اندازه فایل فشرده.
- **Encoding** رمزگذاری داده: فرایند تبدیل داده‌ها به قالب فشرده برای ذخیره‌سازی.
- **Decompression** بازگشایی داده: فرایند بازگرداندن داده فشرده به حالت اولیه برای استفاده.

ذخیره‌سازی فشرده به ویژه در سیستم‌های دارای محدودیت فضای ذخیره‌سازی یا پهنای باند محدود اهمیت دارد. سرویس‌های ابری، شبکه‌های تحویل محتوا، سیستم‌های آرشیوی و پایگاه داده‌های بزرگ به شدت از این تکنیک بهره می‌برند. انتخاب الگوریتم مناسب بسته به نوع داده، هدف فشرده‌سازی و نیاز به کیفیت نهایی متفاوت است. برای مثال، تصاویر پزشکی یا فایل‌های حساس بانکی معمولاً از فشرده‌سازی Lossless استفاده می‌کنند تا هیچ اطلاعاتی از دست نرود، در حالی که محتوای رسانه‌ای مانند ویدئو و موسیقی می‌تواند از فشرده‌سازی Lossy بهره‌مند شود.

نکات مهم در ذخیره‌سازی برای ITF+

۱. تفاوت حافظه موقت و دائم:
 - RAM: موقت و سریع
 - HDD/SSD: دائم و قابل بازیابی
۲. انتخاب نوع ذخیره‌سازی مناسب:
 - داده‌های بزرگ و آرشیوی HDD
 - داده‌های مهم و نیازمند سرعت بالا SSD
 - داده‌های اشتراکی و قابل دسترسی از راه دور Cloud Storage
۳. واحدهای اندازه‌گیری ذخیره‌سازی:

- داده‌های عمومی مانند شماره تلفن دفتر مرکزی شرکت، حساسیت کمتری دارند.

۲. ارزیابی ریسک‌ها (Risk Assessment)

در این مرحله، سازمان باید تهدیدات و آسیب‌پذیری‌هایی که می‌توانند امنیت داده‌ها را به خطر بیندازند، شناسایی کند. تحلیل ریسک شامل ارزیابی احتمال وقوع تهدید و تاثیر آن بر کسب‌وکار است.

مثال:

- آسیب‌پذیری نرم‌افزارها یا سرورهای ذخیره‌سازی
- حملات فیشینگ و مهندسی اجتماعی
- دسترسی غیرمجاز کارکنان یا سوءاستفاده از تجهیزات ذخیره‌سازی

۳. کنترل دسترسی (Access Control)

کنترل دسترسی شامل تعیین سطح دسترسی کاربران و دستگاه‌ها به داده‌ها است. هدف این است که فقط افرادی که به داده‌ها نیاز دارند بتوانند به آن‌ها دسترسی پیدا کنند و بقیه محدود شوند.

مثال:

- مدیران سیستم می‌توانند به همه اطلاعات دسترسی داشته باشند.
- کارمندان فروش تنها به اطلاعات مشتریان خود دسترسی دارند.

۴. رمزگذاری داده‌ها (Data Encryption)

رمزگذاری فرآیندی است که داده‌ها را به شکل غیرقابل فهم برای افراد غیرمجاز تبدیل می‌کند. تنها کسانی که کلید رمزگذاری را دارند می‌توانند داده‌ها را به شکل اصلی بازگردانند.

مثال‌ها:

- رمزگذاری اطلاعات کارت اعتباری مشتریان هنگام ذخیره‌سازی یا انتقال
- استفاده از پروتکل HTTPS برای حفاظت از داده‌ها در وب

۵. پشتیبان‌گیری منظم (Regular Backup)

نسخه‌های پشتیبان داده‌ها به سازمان این امکان را می‌دهند که در صورت خرابی سیستم، حمله سایبری یا از دست رفتن داده‌ها، آن‌ها را بازیابی کند.

مثال:

- ذخیره نسخه پشتیبان سرورهای مالی شرکت در یک مکان امن جدا از شبکه اصلی
- استفاده از سرویس‌های ابری برای نگهداری نسخه‌های پشتیبان

۶. نظارت و بررسی امنیتی (Monitoring and Auditing)

نظارت مداوم بر فعالیت‌های کاربران و سیستم‌ها برای شناسایی رفتارهای مشکوک یا حملات احتمالی ضروری است.

مثال‌ها:

- استفاده از سیستم‌های SIEM (Security Information and Event Management) که فعالیت‌ها را ثبت و تحلیل می‌کنند
- بررسی لاگ‌های سیستم برای شناسایی تلاش‌های غیرمجاز

فصل ۴

واحدهای اندازه‌گیری - (Units of Measure)

اهمیت واحدهای اندازه‌گیری در فناوری اطلاعات

در دنیای مدرن، داده‌ها و اطلاعات به قلب هر سازمان و کسب‌وکار تبدیل شده‌اند. حجم داده‌های ذخیره شده، سرعت پردازش و انتقال آن‌ها، کیفیت خدمات و تصمیم‌گیری‌های کسب‌وکار را تحت تأثیر قرار می‌دهد. بنابراین، درک درست واحدهای اندازه‌گیری، به‌ویژه برای متخصصان فناوری اطلاعات (IT) و مهندسان سیستم، از اهمیت بالایی برخوردار است. این واحدها به ما کمک می‌کنند تا:

- حجم داده‌ها و ظرفیت ذخیره‌سازی را ارزیابی کنیم
- سرعت انتقال داده‌ها در شبکه را بسنجیم
- توان پردازشی سیستم‌ها و پردازنده‌ها را محاسبه کنیم

واحدهای اندازه‌گیری در سه حوزه اصلی طبقه‌بندی می‌شوند:

۱. واحدهای ذخیره‌سازی داده (Storage Units)

۲. واحدهای توان عملیاتی (Throughput Units)

۳. واحدهای سرعت پردازش (Processing Speed Units)

در ادامه هر یک از این حوزه‌ها با جزئیات کامل توضیح داده می‌شوند و مثال‌های کاربردی ارائه می‌شود.

۱. واحدهای ذخیره‌سازی داده (Storage Units)

کامپیوترها داده‌ها را به صورت **باینری (Binary Data)** ذخیره می‌کنند، یعنی مجموعه‌ای از ۰ و ۱‌ها. داده‌ها به این صورت برای پردازش توسط کامپیوتر آماده می‌شوند. کوچک‌ترین واحد داده‌ای **بیت (Bit)** است که می‌تواند تنها دو مقدار داشته باشد: ۰ یا ۱.

- **Bit:** کوچک‌ترین واحد داده‌ای که تنها می‌تواند ۰ یا ۱ باشد.
- در حافظه‌ها و دیسک‌ها، هر بیت به یک بخش کوچک از حافظه یا سطح مغناطیسی اختصاص داده می‌شود.
- در **RAM** و **SSD**، بیت‌ها با استفاده از بار الکتریکی ذخیره می‌شوند. به طوری که ۱ به معنای وجود بار و ۰ به معنای عدم وجود بار است.

بایت‌ها (Bytes)

از آنجایی که انسان‌ها با اعداد و حروف راحت‌تر ارتباط برقرار می‌کنند، کامپیوترها داده‌ها را به صورت **بایت (Byte)** گروه‌بندی می‌کنند. هر بایت شامل ۸ بیت است و می‌تواند ۲۵۶ مقدار مختلف را نمایش دهد (۰ تا ۲۵۵).

مثال عملی:

- یک فایل متنی که شامل ۱۰۰ حرف است، حداقل ۱۰۰ بایت حافظه نیاز دارد.
- اگر هر حرف با استفاده از یونیکد (Unicode) ذخیره شود، بسته به سیستم کدگذاری ممکن است هر حرف ۲ یا ۴ بایت فضای حافظه مصرف کند.

- هر یک از این واحدها **8 بیت** اولیه (یک بایت) را گسترش می دهد تا مدیریت حجم عظیم داده ها ساده تر شود.
- در عمل، فایل های چند گیگابایتی یا چند ترابایتی در حافظه های مدرن مانند **SSD** یا **HDD** رایج هستند و فهم مقیاس ذخیره سازی با این واحدها امکان پذیر می شود.

نکات آزمونی (Exam Tip)

در آزمون ITF+ ممکن است از شما خواسته شود تا بین واحدهای مختلف بایت تبدیل انجام دهید. به عنوان مثال:

- فایل ۱۶ گیگابایتی را می توان به واحدهای دیگر تبدیل کرد:

○ ۱۶۰۰ مگابایت (MB)

○ ۱۶۰۰،۰۰۰ کیلوبایت (KB)

○ ۱۶۰۰،۰۰۰،۰۰۰ بایت

توانایی انجام این محاسبات سریع، به شما در آزمون کمک زیادی می کند.

روش های انتقال داده در شبکه ها

در شبکه های کامپیوتری، داده ها با استفاده از سیگنال های دیجیتال که نشان دهنده بیت های ۰ و ۱ هستند، منتقل می شوند. این سیگنال ها بسته به نوع شبکه، روش و رسانه انتقال متفاوتی دارند. در **شبکه های سیمی (Wired Networks)**، داده ها از طریق سیم های مسی منتقل می شوند و سیگنال ها به شکل پالس های الکتریکی هستند که اطلاعات را از یک نقطه به نقطه دیگر انتقال می دهند. **شبکه های بی سیم (Wireless Networks)** از امواج رادیویی برای انتقال داده ها استفاده می کنند و سیگنال ها بدون نیاز به کابل از طریق هوا منتقل می شوند، که این امکان را می دهد تا دستگاه ها بدون اتصال فیزیکی به شبکه متصل شوند. همچنین، **شبکه های فیبر نوری (Fiber-Optic Networks)** از رشته های نوری شیشه ای یا پلاستیکی برای انتقال داده ها بهره می برند و اطلاعات را به صورت پالس های نور منتقل می کنند، که این روش سرعت بسیار بالا و تأخیر کم را برای انتقال حجم عظیمی از داده ها فراهم می کند. هر یک از این روش ها **مزایا** و **محدودیت** های خاص خود را دارند و بسته به نیاز شبکه، نوع داده و محیط استفاده انتخاب می شوند.

شبکه ها داده را با استفاده از سیگنال های دیجیتال که نشان دهنده بیت های ۰ و ۱ هستند، منتقل می کنند. این سیگنال ها بسته به نوع شبکه متفاوت اند:

۱. **شبکه های سیمی (Wired Networks)** با استفاده از سیم های مسی و انتقال پالس های الکتریکی.
۲. **شبکه های بی سیم (Wireless Networks)** انتقال داده با استفاده از امواج رادیویی و پالس های رادیویی.
۳. **شبکه های فیبر نوری (Fiber-Optic Networks)** انتقال پالس های نوری از طریق رشته های شیشه ای یا پلاستیکی.

۱. شبکه های سیمی (Wired Networks)

- **روش انتقال:** در این شبکه ها، داده ها از طریق سیم های مسی منتقل می شوند و سیگنال ها به شکل پالس های الکتریکی هستند. هر پالس نمایانگر بیت ۰ یا ۱ است.

مزایا:

- سرعت و توان عملیاتی بالا نسبت به برخی شبکه های بی سیم
- پایداری و کمترین اختلال ناشی از نویز محیط
- امنیت بیشتر به دلیل محدود بودن مسیر فیزیکی

اصطلاحات تخصصی

۱. Knowledge Base پایگاه داده‌ای شامل مستندات مشکلات و راه‌حل‌های رایج.
۲. Escalation ارجاع مشکل به متخصصان سطح بالاتر یا تیم‌های دیگر.
۳. Incident Tracking System سیستم ثبت رخداد‌های IT برای مدیریت و پیگیری مشکلات.
۴. Proxy Server سروری که درخواست‌های شبکه را از یک سیستم به سرورهای دیگر هدایت می‌کند.
۵. Configuration پیکربندی سخت‌افزار یا نرم‌افزار برای عملکرد مطلوب سیستم.

واسط‌های دستگاه‌های ورودی/خروجی (Input/Output Device Interfaces)

یکی از وظایف اصلی متخصصان فناوری اطلاعات (IT Professionals) مدیریت مجموعه‌ای تقریباً پیچیده از کابل‌ها، رابط‌ها و کانکتورها است. هنگامی که کاربران را در اتصال دستگاه‌هایشان به شبکه‌ها، تجهیزات جانبی (Peripherals) و نمایشگرهای گرافیکی (Graphic Displays) همراهی می‌کنید، باید بتوانید واسط مناسب برای هر موقعیت را شناسایی و کابل و کانکتور صحیح را انتخاب کنید. این مهارت نه تنها باعث صرفه‌جویی در زمان می‌شود، بلکه از آسیب به تجهیزات و کاهش کارایی سیستم جلوگیری می‌کند.

تعریف رابط دستگاه (Device Interface)

رابط دستگاه یا **Device Interface** نقطه ارتباط بین یک دستگاه ورودی یا خروجی و سیستم کامپیوتری است. این رابط می‌تواند شامل کانکتورها، پورت‌ها، کابل‌ها و پروتکل‌های ارتباطی باشد. رابط‌ها برای انتقال داده‌ها، قدرت و فرمان‌ها از کامپیوتر به دستگاه و بالعکس استفاده می‌شوند.

- مثال عملی: اتصال یک پرینتر USB به لپ‌تاپ، نیازمند شناسایی نوع پورت USB و کابل مناسب است.
- مثال عملی: اتصال مانیتور به کامپیوتر، ممکن است از HDMI، DisplayPort یا VGA استفاده شود و هر کدام محدودیت‌ها و مزایای خاص خود را دارند.

انواع رابط‌ها و کانکتورها (Interfaces and Connectors)

رابط‌ها نقش حیاتی در اتصال دستگاه‌های ورودی و خروجی به سیستم دارند و به دو دسته اصلی سیمی (Wired) و بی‌سیم (Wireless) تقسیم می‌شوند.

رابط‌های سیمی (Wired Interfaces)

- **USB (Universal Serial Bus):** پرکاربردترین رابط برای اتصال اکثر دستگاه‌های جانبی است. نسخه‌ها شامل USB 2.0 (تا ۴۸۰ Mbps)، USB 3.0/3.1 (تا ۵-۱۰ Gbps) و USB-C (دوطرفه و توان بالاتر) هستند. مزیت USB در نصب آسان، انتقال سریع داده و پشتیبانی از توان دستگاه‌ها است.
- **Thunderbolt:** رابط سریع برای انتقال داده و ویدئو با سرعت بالا، نسل‌های ۳ و ۴ تا ۴۰ Gbps، مزایای آن شامل پهنای باند بالا، امکان اتصال چند دستگاه و پشتیبانی از ویدئو با کیفیت ۴K و ۸K است.
- **HDMI (High-Definition Multimedia Interface):** انتقال تصویر و صدا با کیفیت بالا، مناسب برای مانیتورها و تلویزیون‌ها. مزیت HDMI پشتیبانی از رزولوشن بالا و صدا چندکاناله است.
- **DisplayPort:** مخصوص نمایشگرهای حرفه‌ای، پشتیبانی از رزولوشن‌های بالا و نرخ تازه‌سازی سریع. مزایا شامل کیفیت تصویر فوق‌العاده و امکان Daisy Chaining نمایشگرها است.
- **VGA (Video Graphics Array):** رابط قدیمی آنالوگ، محدود در رزولوشن و کیفیت تصویر نسبت به HDMI و DisplayPort، اما هنوز در برخی سیستم‌ها کاربرد دارد.
- **Ethernet (RJ-45):** اتصال شبکه سیمی برای انتقال داده با سرعت‌های ۱۰۰ Mbps، ۱ Gbps و ۱۰ Gbps. مزیت آن اتصال پایدار، کمترین تأخیر و امنیت بالاست.

معایب

- هزینه بالاتر نسبت به USB
- پشتیبانی محدود از سوی تولیدکنندگان سخت افزار
- کاهش محبوبیت پس از USB 2.0 و ۳.۰
- سازگاری کمتر با دستگاه های عمومی

نکات تخصصی +ITF درباره FireWire

۱. شناخت FireWire 400 و FireWire 800 باید تفاوت سرعت و کانکتور آن ها را بدانید.
۲. تشخیص کانکتورها: 4-pin برای دوربین ها، ۶-pin برای کامپیوترها و ۹-pin برای نسخه ۸۰۰.
۳. VoIP و FireWire: بر خلاف تلفن های VoIP که از Ethernet و RJ-45 استفاده می کنند، FireWire کاربردی در VoIP ندارد.
۴. سوالات آزمون +ITF: اغلب پرسیده می شود که FireWire برای چه کاربردهایی استفاده می شد (پاسخ: دوربین ها و تجهیزات چندرسانه ای).
۵. دانستن اینکه FireWire امروزه کمتر استفاده می شود، اما آشنایی با آن در آزمون CompTIA ضروری است.

(Serial ATA (SATA

رابط (Serial ATA (SATA در ذخیره سازی داده

SATA (Serial Advanced Technology Attachment) یک رابط سخت افزاری پر کاربرد برای اتصال دستگاه های ذخیره سازی مانند هارد دیسک ها (HDDs)، درایوهای حالت جامد (SSDs) و درایوهای نوری (Optical Drives) به مادربرد است. این فناوری جایگزین استاندارد قدیمی تر **PATA (Parallel ATA)** شد و به دلیل سرعت بالاتر، کابل های باریک تر و قابلیت های بیشتر، به عنوان استاندارد اصلی در سیستم های مدرن شناخته می شود.

چرا SATA معرفی شد؟

- در گذشته، سیستم ها برای اتصال دستگاه های ذخیره سازی از رابط **PATA/IDE** استفاده می کردند. کابل های PATA بزرگ، حجیم و دارای محدودیت سرعت بودند. با رشد نیاز به انتقال سریع تر داده و استفاده از درایوهای کوچک تر و پرسرعت تر، استاندارد SATA معرفی شد. این تغییر باعث شد:
- سرعت انتقال داده ها چندین برابر افزایش یابد.
 - کابل های کوچک تر جریان هوا را در کیس بهبود دهند.
 - امکان پشتیبانی از Hot Swapping فراهم شود.

انواع SATA

SATA در چند شکل و کاربرد مختلف ارائه شده است:

SATA داخلی

- **تعریف:** اتصال مستقیم هاردها و SSD های داخلی به مادربرد.
- **ویژگی ها:** کابل باریک، رابط L شکل برای جلوگیری از اتصال اشتباه.
- **کاربرد:** نصب سیستم عامل و ذخیره سازی دائمی داده ها در کیس.

(eSATA (External SATA

- **تعریف:** نسخه خارجی SATA که برای اتصال درایوهای ذخیره سازی بیرونی طراحی شده است.
- **مزایا:** سرعت بالاتر از USB 2.0 و FireWire در زمان معرفی.
- **کاربرد:** اتصال هاردهای اکسترنال حرفه ای در محیط های کاری.

- **UEFI (Unified Extensible Firmware Interface):** نسخه مدرن BIOS با امکانات پیشرفته و رابط گرافیکی.

جدول مزایا و معایب انواع فرم فاکتور مادربردها

فرم فاکتور	ابعاد تقریبی	مزایا	معایب
ATX	305×244mm	توسعه پذیری بالا	اندازه بزرگ
Micro-ATX	244×244mm	قیمت پایین تر، مناسب کیس کوچک	اسلات های کمتر
Mini-ITX	170×170mm	بسیار کوچک و کم مصرف	محدودیت در ارتقا

جدول ۳۰

۲. واحد پردازش مرکزی (CPU – Central Processing Unit)

تعریف و عملکرد

CPU یا همان «مغز کامپیوتر» وظیفه پردازش داده ها، اجرای دستورالعمل ها و مدیریت منطق برنامه ها را دارد.

ویژگی های کلیدی

- **سرعت کلاک (Clock Speed):** با گیگاهرتز (GHz) اندازه گیری می شود.
- **هسته ها (Cores):** هر هسته می تواند به صورت مستقل عملیات پردازشی انجام دهد.
- **Threading:** قابلیت اجرای چندین دستور به صورت موازی.
- **Cache:** حافظه داخلی بسیار سریع برای ذخیره داده های موقت.

نکات +ITF

- **Overclocking:** افزایش سرعت پردازنده بالاتر از مقدار استاندارد.
- **Instruction Set (ISA):** مجموعه دستورالعمل هایی که CPU پشتیبانی می کند x86 ARM.

جدول مقایسه CPU ها

ویژگی	CPU دسکتاپ	CPU لپ تاپ	CPU سرور
سرعت کلاک	بالا	متوسط	متوسط
مصرف انرژی	بالا	کم	زیاد
هسته ها	4-16	2-8	32+
کاربرد	بازی و نرم افزار سنگین	قابل حمل	پردازش های سنگین سازمانی

جدول ۳۱

۳. حافظه دسترسی تصادفی (RAM – Random Access Memory)

تعریف و نقش

RAM حافظه کوتاه مدت کامپیوتر است. تمام داده ها و دستورالعمل هایی که CPU در حال پردازش آن هاست به طور موقت در RAM ذخیره

می شوند.

ویژگی ها

- **Volatile:** با خاموش شدن سیستم، اطلاعات RAM پاک می شود.
- **سرعت بالا:** بسیار سریع تر از حافظه های ذخیره سازی.
- **انواع:** DDR3، DDR4، DDR5.

اهمیت زیادی دارد، زیرا در محیط واقعی IT شما ممکن است با انواع مختلف پردازنده‌ها در لپ‌تاپ، دسکتاپ، سرور، دستگاه‌های موبایل و حتی تجهیزات اینترنت اشیا (IoT) روبه‌رو شوید.

در سطح بازار عمومی، نام دو شرکت بیشتر از همه شناخته شده است: **Intel** و **AMD** اما در دنیای گسترده محاسبات، شرکت‌های دیگری همچون **ARM**، **Apple**، **Qualcomm**، **IBM** و **NVIDIA** حتی برخی سازندگان منطقه‌ای نقش مهمی ایفا می‌کنند.

. شرکت Intel اینتل

تاریخچه کوتاه

اینتل (Intel Corporation) در سال ۱۹۶۸ تأسیس شد و از همان ابتدا تمرکز اصلی آن بر روی ساخت تراشه‌های حافظه و سپس پردازنده‌های عمومی بود. پردازنده ۸۰۸۶ این شرکت، پایه‌گذار معماری x86 شد که هنوز هم در اکثر رایانه‌های شخصی استفاده می‌شود.

سری پردازنده‌ها

- **Core i Series (i3, i5, i7, i9)** پردازنده‌های مصرفی برای لپ‌تاپ و دسکتاپ.
- **Celeron و Pentium:** سری ارزان‌تر برای کاربران عمومی.
- **Xeon** پردازنده‌های مخصوص سرورها و ایستگاه‌های کاری (Workstations).
- **Atom** پردازنده‌های کم‌مصرف برای دستگاه‌های کوچک و اینترنت اشیا.

فناوری‌های کلیدی

- **Hyper-Threading** اجرای همزمان چندین Thread در یک هسته.
- **Turbo Boost** افزایش موقت سرعت کلاک برای بهبود عملکرد.
- **vPro** قابلیت‌های امنیتی و مدیریتی برای سازمان‌ها.

نکات+ITF

- معماری x86 و x64 در اصل توسط اینتل معرفی شد.
- سازگاری گسترده نرم‌افزارها با پردازنده‌های اینتل یکی از مزیت‌های مهم است.

شرکت AMD ای‌ام‌دی Advanced Micro Devices

AMD در سال ۱۹۶۹ تأسیس شد و سال‌ها به عنوان رقیب مستقیم اینتل فعالیت کرده است. این شرکت ابتدا پردازنده‌های سازگار با x86 تولید می‌کرد و سپس با معرفی معماری Zen و سری Ryzen توانست سهم بزرگی از بازار را باز پس بگیرد.

سری پردازنده‌ها

- **Ryzen (3, 5, 7, 9)** پردازنده‌های دسکتاپ و لپ‌تاپ با تمرکز بر کارایی و قیمت مناسب.
- **Threadripper** مخصوص کاربران حرفه‌ای و محاسبات سنگین.
- **EPYC** پردازنده‌های سروری با تعداد هسته بسیار بالا.
- **Athlon** پردازنده‌های اقتصادی.

فناوری‌های کلیدی

- **Simultaneous Multi-Threading (SMT)** مشابه Hyper-Threading اینتل.

۵. **گیمینگ (Gaming):** لپ‌تاپ‌های گیمینگ با کارت‌های گرافیک قدرتمند و سیستم خنک‌کننده پیشرفته طراحی می‌شوند تا تجربه بازی‌های ویدئویی سنگین را در قالب قابل حمل ارائه دهند.

مزایای لپ‌تاپ‌ها

- در مقایسه با رایانه‌های رومیزی، لپ‌تاپ‌ها مزایای قابل توجهی دارند:
- **قابلیت حمل بالا:** اصلی‌ترین مزیت لپ‌تاپ، امکان استفاده در هر مکان است.
 - **طراحی یکپارچه:** همه اجزای مورد نیاز (نمایشگر، کیبورد، تاچ‌پد، باتری و بلندگو) در یک دستگاه جمع شده‌اند.
 - **مصرف انرژی بهینه:** لپ‌تاپ‌ها معمولاً نسبت به دسکتاپ‌ها انرژی کمتری مصرف می‌کنند.
 - **اتصال بی‌سیم داخلی:** اغلب لپ‌تاپ‌ها مجهز به Wi-Fi و بلوتوث هستند.
 - **باتری داخلی:** امکان استفاده بدون اتصال به برق.
 - **مدل‌های متنوع:** از لپ‌تاپ‌های اقتصادی و سبک تا مدل‌های حرفه‌ای با توان پردازشی بسیار بالا در بازار موجود است.

معماری لپ‌تاپ‌ها

لپ‌تاپ‌ها همانند دسکتاپ‌ها از مجموعه‌ای از اجزای سخت‌افزاری تشکیل شده‌اند، اما این اجزا به‌گونه‌ای طراحی شده‌اند که **کوچک‌تر، سبک‌تر و کم‌مصرف‌تر** باشند. معماری لپ‌تاپ شامل بخش‌های زیر است:

۱. **پردازنده (CPU):** مغز لپ‌تاپ که وظیفه پردازش داده‌ها را بر عهده دارد. پردازنده‌های لپ‌تاپی (مانند Intel Core i5/i7 یا AMD Ryzen Mobile) معمولاً مصرف انرژی کمتری نسبت به نسخه دسکتاپ دارند.
۲. **حافظه RAM:** برای اجرای هم‌زمان برنامه‌ها و مدیریت داده‌های فعال استفاده می‌شود. ظرفیت آن معمولاً بین ۸ تا ۳۲ گیگابایت است.
۳. **فضای ذخیره‌سازی:** شامل HDD یا SSD است. امروزه اغلب لپ‌تاپ‌ها از SSD برای سرعت بالاتر بهره می‌برند.
۴. **کارت گرافیک (GPU):** در برخی لپ‌تاپ‌ها گرافیک مجتمع (Integrated) وجود دارد و در مدل‌های حرفه‌ای یا گیمینگ، کارت گرافیک مجزا (Dedicated) استفاده می‌شود.
۵. **نمایشگر (Display):** از ۱۳ اینچ تا ۱۷ اینچ با رزولوشن‌های مختلف (HD، Full HD، 4K).
۶. **سیستم ورودی:** شامل کیبورد و تاچ‌پد است. برخی لپ‌تاپ‌ها قابلیت لمس (Touchscreen) دارند.
۷. **سیستم خنک‌کننده:** فن‌ها و هیت‌سینک‌ها وظیفه دفع حرارت CPU و GPU را بر عهده دارند.
۸. **باتری:** منبع انرژی اصلی لپ‌تاپ در حالت قابل حمل، معمولاً از نوع لیتیوم-یونی یا لیتیوم-پلیمر.
۹. **پورت‌ها و اتصالات:** شامل USB، Thunderbolt، HDMI، جک صدا، کارت‌خوان SD و ...

روش کارکرد لپ‌تاپ‌ها

روش کار لپ‌تاپ‌ها همانند سایر رایانه‌ها بر پایه چرخه پردازش اطلاعات است:

۱. **ورودی (Input):** کاربر داده‌ها را از طریق کیبورد، تاچ‌پد یا صفحه لمسی وارد می‌کند.
۲. **پردازش CPU (Processing):** داده‌ها را پردازش کرده و در صورت نیاز از RAM یا GPU کمک می‌گیرد.
۳. **خروجی (Output):** نتایج پردازش روی نمایشگر، بلندگو یا دستگاه‌های جانبی نمایش داده می‌شود.
۴. **ذخیره‌سازی (Storage):** داده‌ها به صورت موقت در RAM و به صورت دائمی در HDD/SSD نگهداری می‌شوند.
۵. **مدیریت انرژی:** سیستم عامل و سخت‌افزار با همکاری هم مصرف انرژی را مدیریت می‌کنند تا عمر باتری بهینه شود.

ویژگی‌های لپ‌تاپ‌ها:

- **قابل حمل بودن:** می‌توان آن‌ها را به راحتی از مکانی به مکان دیگر منتقل کرد.

TCP/IP چیست؟

TCP/IP مجموعه‌ای از پروتکل‌هاست که اساس ارتباطات اینترنتی و شبکه‌های مدرن را تشکیل می‌دهد. این معماری در اصل برای شبکه‌ی **ARPANET** (پیش‌زمینه اینترنت امروزی) در دهه ۱۹۷۰ طراحی شد و بعدها به استاندارد جهانی برای ارتباط بین کامپیوترها و دستگاه‌های شبکه تبدیل گردید.

نام **TCP/IP** از دو پروتکل اصلی گرفته شده است:

- **TCP (Transmission Control Protocol):** پروتکل کنترل انتقال که وظیفه‌ی تضمین تحویل صحیح و کامل داده‌ها را برعهده دارد.
 - **IP (Internet Protocol):** پروتکل اینترنت که مسئول آدرس‌دهی، مسیریابی و ارسال بسته‌های داده از مبدأ به مقصد است.
- در واقع **TCP/IP** یک **مدل معماری شبکه** است که مشابه مدل **OSI**، به لایه‌های مختلف تقسیم می‌شود و هر لایه وظایف خاص خود را دارد. این مدل چهار لایه اصلی دارد:
۱. لایه دسترسی به شبکه (Network Access)
 ۲. لایه اینترنت (Internet)
 ۳. لایه انتقال (Transport)
 ۴. لایه کاربرد (Application)

تاریخچه TCP/IP

- دهه ۱۹۶۰: شروع تحقیقات در آژانس پروژه‌های تحقیقاتی پیشرفته آمریکا (ARPA) برای ایجاد یک شبکه مقاوم در برابر خطا.
- ۱۹۷۴: وینت سرف (Vint Cerf) و رابرت کان (Robert Kahn) مقاله‌ای منتشر کردند که برای اولین بار مفهوم **TCP/IP** را معرفی کرد.
- ۱۹۸۳: **TCP/IP** به صورت رسمی جایگزین پروتکل **NCP** در **ARPANET** شد و از این تاریخ به عنوان روز تولد اینترنت مدرن یاد می‌شود.
- دهه ۱۹۹۰: **TCP/IP** به استاندارد جهانی شبکه‌ها و اینترنت تبدیل شد و همه سیستم‌عامل‌ها (از **UNIX** گرفته تا ویندوز) آن را پیاده‌سازی کردند.

کاربردهای TCP/IP

امروزه تقریباً تمام ارتباطات دیجیتال بر پایه **TCP/IP** انجام می‌شود. برخی کاربردها:

- **اینترنت جهانی:** ستون فقرات اینترنت مبتنی بر **TCP/IP** است.
- **شبکه‌های محلی (LAN):** حتی در دفاتر کوچک، دستگاه‌ها برای ارتباط داخلی از **TCP/IP** استفاده می‌کنند.
- **اینترنت اشیا (IoT):** سنسورها و دستگاه‌های هوشمند داده‌ها را بر اساس **IP** منتقل می‌کنند.
- **شبکه‌های بی‌سیم (Wi-Fi, 4G/5G):** پروتکل‌های پایه همچنان **TCP/IP** هستند.
- **خدمات ابری (Cloud Services):** تبادل داده بین کاربران و سرورهای ابری با **TCP/IP** انجام می‌شود.
- **ارتباطات چندرسانه‌ای:** پخش ویدئو، تماس صوتی اینترنتی (**VoIP**)، کنفرانس آنلاین.

مزایای TCP/IP

- **مقیاس‌پذیری بالا:** از شبکه‌های کوچک تا اینترنت جهانی پشتیبانی می‌کند.
- **انعطاف‌پذیری:** روی انواع رسانه‌ها (کابل مسی، فیبر نوری، بی‌سیم، ماهواره‌ای) قابل استفاده است.
- **سازگاری چندسکویی:** توسط همه سیستم‌عامل‌ها و سخت‌افزارهای شبکه پشتیبانی می‌شود.
- **قابلیت اطمینان:** **TCP** تحویل مطمئن داده‌ها را تضمین می‌کند.
- **پروتکل باز و استاندارد:** هیچ شرکت خاصی مالک آن نیست؛ یک استاندارد جهانی و عمومی است.

نحوه استفاده از آدرس‌های IP در شبکه

- یک سیستم با آدرس IP خود به طور یکتا در شبکه شناسایی می‌شود.
- اگر سیستم مستقیماً به اینترنت متصل باشد، آدرس IP عمومی آن باید یکتا باشد تا هیچ سیستم دیگری در جهان از آن استفاده نکند. مشابه شماره تلفن همراه که در دنیا تکراری نیست.
- سیستم‌هایی که به شبکه‌های خصوصی مانند شبکه خانگی یا شرکتی متصل هستند، می‌توانند از IP Address خصوصی (Private IP Address) استفاده کنند.
- روتر یا فایروال مسئول ترجمه این آدرس‌های خصوصی به آدرس‌های عمومی هنگام ارتباط با اینترنت است.

آدرس‌های IP در ارتباطات شبکه

در هر ارتباط شبکه، دو آدرس وجود دارد:

- Source Address (آدرس مبدأ): مشخص‌کننده سیستمی است که اطلاعات را ارسال می‌کند.
- Destination Address (آدرس مقصد): مشخص‌کننده سیستمی است که اطلاعات را دریافت می‌کند.

توضیح:

هنگام تبادل داده بین دو سیستم، آدرس‌های مبدأ و مقصد بسته‌ها با هر ارسال و دریافت جابه‌جا می‌شوند.

مثال:

- کاربری با IP 10.12.0.1 به یک سرور وب با IP 10.51.1.2 داده ارسال می‌کند.
- در ارسال: منبع = کاربر، مقصد = سرور وب
- در پاسخ سرور: منبع = سرور وب، مقصد = کاربر

روش‌های تخصیص IP Address

آدرس‌های IP می‌توانند به دو روش اختصاص داده شوند:

۱. Static IP (آدرس ثابت)

- شما به صورت دستی آدرس IP را در تنظیمات سیستم مشخص می‌کنید.
- مسئولیت انتخاب آدرس یکتا و مناسب برای شبکه با شماست.

۲. Dynamic IP (آدرس پویا) با استفاده از DHCP:

- DHCP (Dynamic Host Configuration Protocol) به شما اجازه می‌دهد یک محدوده آدرس IP مشخص کنید و سرور DHCP به صورت خودکار آدرس‌ها را به سیستم‌ها اختصاص می‌دهد.
- معمولاً سرورها با آدرس‌های Static و دستگاه‌های کاربران با آدرس‌های Dynamic تنظیم می‌شوند.

توضیح:

- اگر سیستم نتواند DHCP پیدا کند، از APIPA (Automatic Private IP Addressing) استفاده می‌کند.
- آدرس‌های APIPA با 169.254.x.x شروع می‌شوند. وجود چنین آدرسی در شبکه به معنای مشکل در اتصال DHCP است و نباید در شبکه‌های بزرگ از آن استفاده شود.

جمع‌بندی نکات کلیدی برای ITF+

- هر سیستم دو آدرس دارد: IP Address و MAC Address.
- IP Address برای شناسایی سیستم در شبکه و مسیریابی داده‌ها استفاده می‌شود.

۳. نقاط دسترسی Mesh :

- برای شبکه‌های بزرگ یا محوطه‌های وسیع طراحی شده‌اند.
- نقاط دسترسی با هم ارتباط برقرار می‌کنند و شبکه یکپارچه بی‌سیم ایجاد می‌کنند.

مزایا و اهمیت نقاط دسترسی

- اتصال آسان دستگاه‌های بی‌سیم: بدون نیاز به کابل کشی جداگانه
- پوشش گسترده: ایجاد شبکه در فضاهای بزرگ و چند طبقه
- مدیریت مرکزی (برای نقاط دسترسی مدیریت شده): پیکربندی و نظارت ساده
- امنیت پیشرفته: استفاده از WPA3، فایروال داخلی و احراز هویت کاربران

نکات عملی و امتحانی

- مودم‌ها (Modems):
 - برای تبدیل سیگنال‌های آنالوگ به دیجیتال و بالعکس استفاده می‌شوند.
 - امروزه معمولاً برای اتصال اینترنت کابل و DSL استفاده می‌شوند.
- فایروال‌ها (Firewalls):
 - دستگاه‌های امنیتی که ترافیک ورودی و خروجی شبکه را محدود می‌کنند.
 - نقش آن‌ها جلوگیری از دسترسی غیرمجاز و محافظت از شبکه است.

۱. تاریخچه شبکه‌های بی‌سیم:

- ظهور Wi-Fi و استانداردهای مختلف آن
- پیشرفت فناوری و افزایش سرعت و برد

۲. امنیت در نقاط دسترسی:

- انواع پروتکل‌های امنیتی (Wi-Fi (WEP, WPA, WPA2, WPA3)
- احراز هویت و کنترل دسترسی به شبکه

۳. راه‌اندازی شبکه بی‌سیم سازمانی:

- طراحی پوشش سیگنال، محل نصب نقاط دسترسی، مدیریت کانال‌ها
- مثال‌های عملی برای محیط‌های اداری و صنعتی

۴. ادغام نقاط دسترسی با سایر دستگاه‌های شبکه:

- اتصال به سوئیچ‌ها و روترها
- هماهنگی با فایروال‌ها و سیستم‌های مانیتورینگ

۵. نقاط دسترسی پیشرفته:

- Mesh Network و کنترل کننده مرکزی
- مدیریت پهنای باند، اولویت‌بندی دستگاه‌ها و کاهش تداخل

۶. سناریوهای عملی:

- شبکه‌های خانگی با چندین دستگاه
- شبکه‌های سازمانی با دسترسی امن برای کارکنان و مهمانان

۷. چالش‌ها و محدودیت‌ها:

- تداخل سیگنال‌ها، محدوده پوشش، مشکلات امنیتی
- نیاز به به‌روزرسانی‌های منظم و مدیریت مداوم

شبکه‌های بی‌سیم (Wireless Networking)

رایج‌ترین استاندارد بی‌سیم در استفاده امروز فناوری **Wi-Fi** است. **Wi-Fi** مجموعه‌ای از استانداردها است که توسط **انجمن مهندسان برق و الکترونیک (IEEE – Institute of Electrical and Electronics Engineers)** ایجاد شده و جزئیات فنی نحوه ارتباط دستگاه‌های بی‌سیم با یکدیگر و با نقاط دسترسی بی‌سیم را توصیف می‌کند. استفاده از یک استاندارد کاملاً ضروری است؛ زیرا بدون وجود استاندارد، دستگاه‌های بی‌سیم «زبان» یکسانی برای ارتباط نداشتند. **استانداردسازی** باعث می‌شود هر دستگاه **Wi-Fi** بتواند با هر شبکه **Wi-Fi** در سراسر جهان کار کند.

توضیح تخصصی IT:

۱. Wi-Fi

- فناوری است که جایگزین کابل‌ها و سیم‌های شبکه سیمی شده و ارتباطات بی‌سیم را از طریق **فرستنده‌ها و گیرنده‌های رادیویی** ممکن می‌کند.
- هر دستگاهی که از **Wi-Fi** پشتیبانی می‌کند دارای **رادیو ترنسسیور (Radio Transceiver)** است که قادر به ارتباط بر روی یک یا چند باند استاندارد **Wi-Fi** است.
- این دستگاه‌ها شامل:

- تلفن‌های هوشمند
- لپ‌تاپ‌ها
- کنسول‌های بازی ویدئویی
- سنسورهای متصل به اینترنت (مانند دتکتور دود هوشمند)

۲. رادیو ترنسسیور (Radio Transceiver):

- تراشه‌ای است که داده‌های دیجیتال را به سیگنال‌های رادیویی تبدیل می‌کند و بالعکس.
- شامل **فرستنده، گیرنده و آنتن** است و مسئول برقراری ارتباط بی‌سیم بین دستگاه و نقطه دسترسی می‌باشد.

اتصال شبکه‌های بی‌سیم به شبکه‌های سیمی

اکثر شبکه‌های **Wi-Fi** نیز به شبکه‌های سیمی متصل هستند که خود آن‌ها به اینترنت وصل می‌شوند. این اتصال به دستگاه‌های بی‌سیم اجازه می‌دهد با دستگاه‌ها و سیستم‌های سیمی در هر نقطه‌ای از اینترنت ارتباط برقرار کنند.

- **شبکه‌های خانگی و کسب‌وکار:** از نقاط دسترسی بی‌سیم برای انجام اتصال استفاده می‌کنند.
- **شبکه‌های سازمانی:** ممکن است از نقاط دسترسی سقفی و پیشرفته استفاده کنند که سیگنال را در فضاهای بزرگ و چند طبقه منتشر می‌کنند.
- **شبکه‌های کوچک خانگی/دفتر کار کوچک (SOHO – Small Office/Home Office):** ممکن است از نقاط دسترسی رومیزی استفاده کنند که ساده‌تر و مناسب فضای محدود هستند.

هر دو نوع نقطه دسترسی شامل **آنتن‌های قدرتمند، فرستنده‌ها و گیرنده‌ها** هستند که امکان پخش سیگنال‌های **Wi-Fi** در مناطق وسیع را فراهم می‌کنند و همچنین با کابل به شبکه سیمی سستی متصل می‌شوند. دستگاه‌های بی‌سیم در محدوده سیگنال می‌توانند با نقطه دسترسی ارتباط برقرار کنند و از طریق آن به شبکه‌های دیگر متصل شوند.

توضیح تخصصی IT:

۱. شبکه‌های SOHO و Enterprise:

- **SOHO** شبکه کوچک خانگی یا دفتر کار کوچک که برای تعداد محدودی دستگاه طراحی شده است.
- **Enterprise** شبکه سازمانی بزرگ که نیازمند **مدیریت متمرکز، امنیت پیشرفته و نقاط دسترسی متعدد** است.

نحوه عملکرد وب

مرورگرهای وب نرم افزارهایی هستند که ما برای دسترسی به وبسایتها از آنها استفاده می کنیم. این مرورگرها پروتکل انتقال ابرمتن یا **Hypertext Transfer Protocol (HTTP)** را می شناسند و به ما کمک می کنند صفحات وب را مشاهده کنیم. زمانی که می خواهیم یک صفحه وب را ببینیم، مرورگر به سرورهای وبی که اطلاعات مورد نظر ما را ذخیره کرده اند متصل می شود و سپس یک اتصال HTTP یا HTTPS برقرار می کند تا محتوای وب را به رایانه ما منتقل کند و مرورگر آن را برای ما نمایش دهد.

پروتکل HTTP و HTTPS

HTTP پروتکلی است که انتقال اطلاعات بین مرورگر و سرور وب را مدیریت می کند. HTTP مبتنی بر متن ساده است و دستورات و پاسخها را به صورت قابل خواندن توسط انسان منتقل می کند. نسخه امن آن یعنی **HTTPS (Hypertext Transfer Protocol Secure)** از یک لایه امنیتی به نام **SSL/TLS** استفاده می کند تا داده ها در مسیر انتقال رمزگذاری شوند و از دسترسی غیرمجاز جلوگیری شود. این امنیت برای سایت هایی که اطلاعات حساس مانند اطلاعات کارت اعتباری یا داده های شخصی کاربران را مدیریت می کنند ضروری است.

فرآیند دسترسی به وب

تصویر ۲۴.۱ (در متن اصلی) نحوه عملکرد این فرآیند را نمایش می دهد. وقتی یک کاربر نهایی می خواهد وارد یک وبسایت شود، ابتدا مرورگر وب را روی رایانه خود باز می کند و URL یا آدرس سایت مورد نظر را در نوار آدرس مرورگر وارد می کند. سپس مرورگر سرور وب مناسب که صفحه مورد نظر را میزبانی می کند، شناسایی کرده و یک **درخواست HTTP GET** به آن سرور ارسال می کند.

درخواست HTTP GET یک دستور استاندارد است که از مرورگر به سرور ارسال می شود تا محتوا یا اطلاعات خاصی دریافت شود. سرور وب درخواست را پردازش می کند، تصمیم می گیرد چه محتوایی باید به کاربر نشان داده شود و سپس صفحه وب را به کاربر بازمی گرداند. محتوای وبی که به کاربر بازمی گردد معمولاً به زبان **HTML (Hypertext Markup Language)** نوشته شده است. مرورگر HTML را می خواند و آن را به صفحه ای که کاربر در مرورگر خود مشاهده می کند تبدیل می کند.

معماری دو لایه ای وب

اگر این فرآیند برای شما آشناست، این یک نمونه از **برنامه های دو لایه ای (Two-Tier Applications)** است. همان طور که در فصل ۲۳ کتاب تحت عنوان «معماری و تحویل برنامه ها» توضیح داده شده است، سیستم کاربر نهایی یک لایه و سرور وب دوم را تشکیل می دهد. در معماری دو لایه، معمولاً رابط کاربری و منطق برنامه در سیستم کاربر نهایی قرار دارد و داده ها روی سرور ذخیره می شوند و از طریق درخواست های شبکه منتقل می شوند.

سازگاری مرورگرها

برای اکثر موارد، برنامه های وب مدرن باید با تمامی مرورگرهای امروزی کار کنند. با این حال، ممکن است با برنامه ای مواجه شوید که در مرورگر خاصی به درستی کار نمی کند. اگر در مشاهده یک وبسایت رفتار غیرعادی مشاهده کردید، یک روش عیب یابی مفید این است که سایت را در مرورگر دیگری باز کنید و ببینید مشکل حل می شود یا خیر. برنامه های وب که معمولاً با مشکلات سازگاری مرورگر مواجه می شوند، اغلب یک لیست از مرورگرهایی که با سایت آنها به درستی کار می کنند را منتشر می کنند.

- **C++ و C** زبان‌های سطح پایین با سرعت بالا، مناسب برای توسعه سیستم‌های عامل، نرم‌افزارهای سیستمی، بازی‌های رایانه‌ای و برنامه‌های نیازمند پردازش سنگین.
- **Java** زبانی شیء‌گرا که ابتدا به بایت‌کد (Bytecode) کامپایل شده و سپس توسط ماشین مجازی جاوا (JVM) اجرا می‌شود. این روش ترکیبی از کامپایل و تفسیر است.
- **Go** زبان توسعه یافته توسط گوگل، با تمرکز بر سرعت و کارایی بالا و مدیریت همزمانی (Concurrency).
- **Julia** زبانی که بیشتر در محاسبات علمی و تحلیل داده‌های پیچیده و سنگین استفاده می‌شود.
- **FORTRAN** یکی از قدیمی‌ترین زبان‌های کامپایل شده که برای محاسبات علمی و عددی طراحی شده است.

نکته مهم برای امتحان:

در زبان‌های تفسیر شده، کامپوتر کد منبع را مستقیماً با استفاده از **مفسر** اجرا می‌کند. در حالی که در زبان‌های کامپایل شده، ابتدا برنامه باید با **کامپایلر** به یک فایل اجرایی تبدیل شود. کدهای کامپایل شده معمولاً سریع‌تر از کدهای تفسیر شده اجرا می‌شوند، زیرا دیگر نیازی به ترجمه لحظه‌ای دستورات به زبان ماشین نیست.

زبان‌های تخصصی (Specialized Languages)

علاوه بر زبان‌های تفسیر شده و کامپایل شده، دو دسته زبان دیگر وجود دارند که کاربرد آن‌ها محدود به شرایط و استفاده‌های خاص است. این زبان‌ها شامل **زبان‌های اسمبلی (Assembly Languages)** و **زبان‌های پرس و جو (Query Languages)** هستند.

زبان‌های اسمبلی

زبان اسمبلی به برنامه‌نویسان اجازه می‌دهد تا کدی بنویسند که مستقیماً با **سخت‌افزار (Hardware)** تعامل داشته باشد، بدون آنکه نیاز به استفاده از زبان‌های تفسیر شده یا کامپایل شده باشد. هر پردازنده، **معماری (Architecture)** خاص خود را دارد و بنابراین زبان اسمبلی برای هر نوع پردازنده متفاوت است.

نوشتن کد در زبان اسمبلی به دلیل پیچیدگی و وابستگی به سخت‌افزار، نسبتاً نادر است. زبان اسمبلی شبیه به **زبان ماشین (Machine Language)** است، اما نه کاملاً، زیرا برنامه‌نویس هنوز می‌تواند از علائم و نمادهایی برای نوشتن دستورها استفاده کند که انسان آن‌ها را راحت‌تر می‌فهمد.

امروزه برنامه‌نویسان معمولاً فقط زمانی از زبان اسمبلی استفاده می‌کنند که با سخت‌افزار تخصصی مانند **دستگاه‌های تعبیه شده (Embedded Devices)** یا **اینترنت اشیا (IoT – Internet of Things)** کار می‌کنند.

توضیح تخصصی:

- **Assembly Language** زبان سطح پایین نزدیک به زبان ماشین که هر دستور آن تقریباً یک عملیات سخت‌افزاری را مستقیماً کنترل می‌کند.
- **Embedded Systems** سیستم‌های کامپیوتری کوچک و تخصصی که برای انجام وظایف خاص طراحی شده‌اند، مانند کنترلرهای صنعتی، ساعت‌های هوشمند یا دستگاه‌های پزشکی.
- **IoT Devices** دستگاه‌های متصل به اینترنت که داده‌ها را جمع‌آوری، پردازش و ارسال می‌کنند، مانند حسگرهای هوشمند، دوربین‌های امنیتی و سیستم‌های خانه هوشمند.

مزیت اصلی استفاده از زبان اسمبلی، **کنترل کامل بر سخت‌افزار و بهینه‌سازی دقیق سرعت و حافظه** است، اما این کار نیازمند تخصص بالایی است و برنامه‌نویسی با آن زمان‌بر و پیچیده است.

زبان‌های پرس و جو

زبان‌های پرس و جو برای **پرسش و مدیریت داده‌ها در پایگاه داده‌ها (Databases)** استفاده می‌شوند. اصلی‌ترین زبان در این دسته، **SQL (Structured Query Language)** است که استاندارد صنعت برای تعامل با پایگاه داده‌های رابطه‌ای محسوب می‌شود.

سیاست‌های رمز عبور (Password Policies)

یکی از مهم‌ترین جنبه‌های امنیت اطلاعات در سازمان‌ها، سیاست‌های رمز عبور (Password Policies) است. این سیاست‌ها به تیم‌های IT اجازه می‌دهند تا کنترل‌های فنی (Technical Controls) مشخصی برای انتخاب و نگهداری رمز عبور کاربران اعمال کنند. اجرای سیاست‌های مناسب رمز عبور به کاهش ریسک دسترسی غیرمجاز و تقویت امنیت سیستم کمک می‌کند.

طول رمز عبور (Password Length)

یکی از ساده‌ترین و رایج‌ترین کنترل‌ها در زمینه رمز عبور، تعیین حداقل طول رمز عبور است. این کنترل مشخص می‌کند که رمز عبور حداقل چند کاراکتر باید داشته باشد. طول بیشتر رمز عبور باعث افزایش پیچیدگی و کاهش احتمال حدس زدن آن توسط مهاجمان می‌شود.

پیچیدگی رمز عبور (Password Complexity)

سازمان‌ها همچنین می‌توانند نیازمندی‌های پیچیدگی رمز عبور را اعمال کنند. این کنترل‌ها کاربران را مجبور می‌کنند تا رمز عبور خود را با ترکیبی از انواع مختلف کاراکترها انتخاب کنند، مانند:

- حروف بزرگ (Uppercase Letters)
- حروف کوچک (Lowercase Letters)
- اعداد (Digits)
- کاراکترهای ویژه (Special Characters)

هرچه ترکیب کاراکترها بیشتر باشد، رمز عبور سخت‌تر حدس زده می‌شود و امنیت افزایش می‌یابد.

انقضای رمز عبور (Password Expiration)

- انقضای رمز عبور کاربران را ملزم می‌کند که رمزهای عبور خود را به صورت دوره‌ای تغییر دهند.
- مثال: تعیین دوره انقضای ۱۸۰ روز، به این معنی که کاربران باید هر شش ماه رمز عبور خود را تغییر دهند.
- در حال حاضر، بسیاری از سازمان‌ها دیگر الزام به انقضای دوره‌ای رمز عبور ندارند و تنها زمانی تغییر را درخواست می‌کنند که رمز عبور به خطر افتاده (Compromised) باشد.

تاریخچه رمز عبور (Password History)

- تاریخچه رمز عبور به سازمان‌ها اجازه می‌دهد تا از استفاده مجدد رمزهای عبور قدیمی جلوگیری کنند.
- سیستم‌ها رمزهای عبور قبلی کاربران را ذخیره می‌کنند.
- این کنترل مشخص می‌کند که چه تعداد رمز عبور قدیمی برای هر کاربر به یاد سپرده می‌شود.

بازنشانی رمز عبور (Password Resets)

هر سازمان باید اجازه دهد کاربران به سرعت و به صورت امن رمز عبور خود را تغییر دهند.

- این امکان به کاربران اجازه می‌دهد تا در صورت نگرانی از سوءاستفاده یا لو رفتن رمز عبور، رمز خود را به سرعت تغییر دهند.
- هشدار: فرآیند بازنشانی رمز عبور باید با دقت طراحی شود. اگر فرآیند مناسب نباشد، ممکن است مهاجمان با بازنشانی غیرمجاز (Unauthorized Password Reset) به سیستم دسترسی پیدا کنند.

عدم استفاده مجدد رمز عبور (Password Reuse)

- تیم‌های IT باید به کاربران توصیه کنند که رمز عبور خود را در سایت‌ها و سیستم‌های مختلف دوباره استفاده نکنند.
- اگر رمز عبور در چند سایت استفاده شود و یکی از آن سایت‌ها هک شود، مهاجم ممکن است همان رمز را در سایت‌های دیگر آزمایش کند.
- این توصیه، اگرچه سخت برای اجرا، اما افزایش امنیت قابل توجهی دارد.

مدیران رمز عبور (Password Managers)

- مدیریت رمزهای عبور منحصر به فرد برای هر سایت دشوار است. مدیران رمز عبور (Password Managers) ابزارهایی هستند که این مشکل را حل می‌کنند:
 - این ابزارها گنجینه‌های رمز عبور امن (Secure Password Vaults) هستند که معمولاً توسط مکانیزم‌های بیومتریک (Biometric Security) محافظت می‌شوند.
 - رمزهای عبور قوی و منحصر به فرد تولید و ذخیره می‌شوند.
 - هنگام ورود به سایت‌ها، به صورت خودکار رمزها را پر می‌کنند، بنابراین کاربران نیازی به به خاطر سپردن همه رمزها ندارند.
- مثال: نرم‌افزار LastPass یکی از محبوب‌ترین مدیران رمز عبور است که امکان ایجاد و ذخیره رمزهای عبور قوی را فراهم می‌کند.

اصطلاحات تخصصی IT در سیاست‌های رمز عبور

۱. Password Policies سیاست‌های رمز عبور: مجموعه‌ای از قوانین و کنترل‌ها برای ایجاد و مدیریت رمزهای عبور امن.
۲. Password Complexity پیچیدگی رمز عبور: الزام به استفاده از ترکیب انواع مختلف کاراکترها برای افزایش امنیت.
۳. Password Expiration انقضای رمز عبور: الزام به تغییر دوره‌ای رمز عبور برای کاهش ریسک نفوذ.
۴. Password History تاریخچه رمز عبور: جلوگیری از استفاده مجدد رمزهای عبور قدیمی توسط کاربران.
۵. Password Resets بازنشانی رمز عبور: فرآیندی برای تغییر سریع رمز عبور توسط کاربران.
۶. Password مدیران رمز عبور: ابزارهای ذخیره و مدیریت امن رمزهای عبور، اغلب با پشتیبانی بیومتریک.

رمزنگاری (Cryptography)

رمزنگاری یکی از مهم‌ترین کنترل‌های امنیتی (Security Controls) است که می‌توانیم برای محافظت از محرمانگی داده‌ها (Data Confidentiality) استفاده کنیم.

رمزنگاری (Encryption) از عملیات ریاضی (Mathematical Operations) برای تبدیل اطلاعات به فرمتی استفاده می‌کند که تنها توسط کاربران مجاز قابل خواندن باشد.

نکته امتحانی

ریاضیات پشت رمزنگاری بسیار پیچیده است، اما در امتحان ITF+ نیاز نیست که جزئیات ریاضی را بدانید. کافی است اصول پایه‌ای رمزنگاری و کاربردهای آن برای حفاظت از سازمان خود را درک کنید.

رمزگذاری داده‌ها (Encrypting Data)

- در رمزگذاری، ما ابتدا با اطلاعات متن ساده (Plain Text) شروع می‌کنیم.
- متن ساده: اطلاعاتی که به صورت عادی قابل خواندن هستند و هر کسی می‌تواند آن را ببیند.
- مثال: پاراگراف اول این فصل که هنوز رمزگذاری نشده است.
- سپس از الگوریتم رمزنگاری (Encryption Algorithm) همراه با کلید رمزنگاری (Encryption Key) برای رمزگذاری داده‌ها استفاده می‌کنیم.
- الگوریتم رمزنگاری: فرمول ریاضیاتی که برای تبدیل متن ساده به متن رمزگذاری شده استفاده می‌شود.
- کلید رمزنگاری: در واقع "رمز عبور" داده‌ها است.
- پس از رمزگذاری، متن ساده به متن رمزگذاری شده یا Ciphertext تبدیل می‌شود.
- Ciphertext: داده‌ای که بدون کلید رمزگشایی، کاملاً غیرقابل خواندن است و برای هر کسی که به آن دسترسی داشته باشد، فقط به شکل حروف و کاراکترهای نامفهوم ظاهر می‌شود.

رمزگشایی داده‌ها (Decrypting Data)

- برای تبدیل متن رمزگذاری شده (Ciphertext) به متن ساده:
- از الگوریتم رمزگشایی (Decryption Algorithm) و کلید رمزگشایی (Decryption Key) استفاده می‌کنیم.
- بدون داشتن کلید رمزگشایی صحیح (Correct Decryption Key)، عملیات رمزگشایی انجام نمی‌شود.
- حفاظت از کلید رمزگشایی (Protecting the Key) حیاتی است؛ تا زمانی که کاربران غیرمجاز به کلید دسترسی نداشته باشند، داده‌ها امن باقی می‌مانند.

کاربردهای رمزنگاری (Uses of Encryption)

رمزنگاری در دو محیط اصلی استفاده می‌شود:

۱. داده‌های ذخیره‌شده (Data at Rest)

۲. داده‌های در حال انتقال (Data in Transit)

داده‌های ذخیره‌شده (Data at Rest)

- داده‌های ذخیره‌شده: داده‌هایی که در حال حاضر بر روی دیسک یا دستگاه ذخیره شده‌اند.
- می‌توان فایل‌های منفرد، دیسک‌های کامل یا محتوای دستگاه‌های موبایل را رمزگذاری کرد.
- مثال: اگر شخصی به یکی از این فایل‌ها یا دستگاه‌ها دسترسی پیدا کند، بدون کلید رمزگشایی، به داده‌ها دسترسی نخواهد داشت.
- رمزگذاری کامل دیسک (Full-Disk Encryption – FDE): فناوری که در برخی سیستم‌عامل‌ها تعبیه شده و به صورت خودکار تمام داده‌های یک دستگاه را رمزگذاری می‌کند.
- کاربرد: لپ‌تاپ‌ها، تبلت‌ها، گوشی‌های هوشمند و سایر دستگاه‌های قابل حمل که ممکن است گم یا سرقت شوند.
- مزیت: اگر دستگاه به سرقت رود، داده‌ها بدون کلید رمزگشایی غیرقابل دسترسی هستند.

داده‌های در حال انتقال (Data in Transit)

- داده‌های در حال انتقال: داده‌هایی که در شبکه در حال حرکت هستند.
- حفاظت از این داده‌ها با استفاده از رمزنگاری نیز امکان‌پذیر است.

مثال‌ها:

۱. HTTP vs HTTPS

- استفاده از HTTP: داده‌ها بدون رمزگذاری منتقل می‌شوند و افراد می‌توانند فعالیت شبکه شما را رصد کنند.
- استفاده از HTTPS: داده‌ها رمزگذاری می‌شوند و از جاسوسی و سرقت اطلاعات جلوگیری می‌شود.
- ۲. ایمیل‌ها و برنامه‌های موبایل: رمزگذاری داده‌ها هنگام ارسال پیام‌ها به سرورها.
- ۳. شبکه خصوصی مجازی (VPN): رمزگذاری کل اتصال شبکه برای محافظت از داده‌ها هنگام حرکت در شبکه عمومی.

نکته امتحانی

- رمزنگاری متن ساده را به متن رمزگذاری شده (Ciphertext) تبدیل می‌کند.
- حفاظت از داده‌های ذخیره‌شده (Data at Rest) و داده‌های در حال انتقال (Data in Transit) را فراهم می‌کند.
- رمزنگاری (Encryption): فرآیند تبدیل متن ساده به متن رمزگذاری شده که توسط افراد غیرمجاز قابل خواندن نیست.
- رمزگشایی (Decryption): استفاده از کلید رمزگشایی برای تبدیل متن رمزگذاری شده به متن ساده.
- رمزنگاری داده‌های ذخیره‌شده: رمزگذاری فایل‌ها یا پوشه‌ها، یا استفاده از رمزگذاری کامل دیسک (FDE) برای کل دستگاه.
- رمزنگاری داده‌های در حال حرکت: رمزگذاری هنگام انتقال در شبکه، استفاده از HTTPS برای وب و VPN برای اتصال شبکه امن.

اصطلاحات تخصصی IT در رمزنگاری

۱. **Cryptography رمزنگاری**: هنر و علم محافظت از اطلاعات با استفاده از روش‌های ریاضی برای اطمینان از محرمانگی، صحت و عدم انکار داده‌ها.
۲. **Encryption رمزگذاری**: تبدیل متن ساده به متن رمزگذاری شده با استفاده از الگوریتم و کلید.
۳. **Ciphertext متن رمزگذاری شده**: داده‌ای که بدون کلید قابل خواندن نیست.
۴. **Decryption رمزگشایی**: فرآیند بازگرداندن متن رمزگذاری شده به متن ساده.
۵. **Data at Rest داده‌های ذخیره‌شده**: داده‌هایی که روی دیسک یا دستگاه ذخیره شده‌اند.
۶. **Data in Transit داده‌های در حال انتقال**: داده‌هایی که در شبکه منتقل می‌شوند.
۷. **Full-Disk Encryption رمزگذاری کامل دیسک (FDE)** - رمزگذاری تمام داده‌های یک دستگاه برای محافظت در صورت گم شدن یا سرقت.
۸. **HTTPS (Hypertext Transfer Protocol Secure)** نسخه امن پروتکل HTTP برای رمزگذاری ترافیک وب.
۹. **VPN (Virtual Private Network)** شبکه خصوصی مجازی برای رمزگذاری کل اتصال شبکه و محافظت از داده‌ها در مسیر.

contact me:

HosseinSeilani

Designer, Developer and Linux sysadmin

seilany.ir

learninghive.ir

emperor-os.ir

Hubuntu.ir

predator-os.ir

telegram: @seilany



Founder and Developer of Emperor-OS, Hubuntu and Predator-OS. I bring significant experience as a Linux/Windows sysadmin and graphical web design, UX/UI to the Open Source Community.



Emperor-OS



Predator-OS