COMPUTER NETWORKING — CACS303

Complete Exam Cheat Sheet — Units 1 to 7

BCA III/V | Last-Hour Revision Reference

UNIT 1 — INTRODUCTION

1.1-1.2 Network as Infrastructure & Applications

- Computer Network: Interconnected autonomous computers that share resources (data, hardware, software) and communicate using agreed rules (protocols).
- Applications: Resource sharing, communication (email/VoIP/video-conf), e-commerce, distributed computing, remote access, IoT, cloud services, entertainment (streaming/gaming).

1.3 Network Architecture

- Client-Server: Centralised server provides services to multiple clients — easier management, single point of failure.
- Peer-to-Peer (P2P): Every node is both client and server — no central control, more resilient, harder to secure/manage.

1.4 Types of Computer Networks

Type	Coverage	Example
PAN (Personal Area Network)	~few metres	Bluetooth, USB
LAN (Local Area Network)	Building/campus	Office/home Wi-Fi/Ethernet
MAN (Metropolitan Area Network)	A city	Cable TV network, WiMAX
WAN (Wide Area Network)	Country/globe	The Internet, leased lines

1.5 Protocols and Standards

- Protocol: A formal set of rules governing format, timing, sequencing, and error control of data communication.
- Standard: Agreed specification ensuring interoperability — De facto (industry-adopted, e.g. early Ethernet) vs De jure (legally/officially standardised by bodies like ISO, IEEE, ITU-T, IETF).

1.6 The OSI Reference Model (7 Layers, top→bottom)

#	Layer	Key Function	PDU
7	Application	Network services to end-user apps (HTTP, FTP, SMTP)	Data
6	Presentation	Translation, encryption, compression	Data
5	Session	Establishes/manages/terminates sessions, dialog control	Data
4	Transport	End-to-end delivery, segmentation, reliability (TCP/UDP)	Segment
3	Network	Logical addressing & routing (IP)	Packet
2	Data Link	Framing, MAC addressing, error/flow control on a link	Frame
1	Physical	Raw bit transmission over medium (voltage, light, radio)	Bit

Note: Mnemonic (top→bottom): All People Seem To Need Data Processing.

1.7 The TCP/IP Protocol Suite (4 Layers)

Layer	Corresponds to OSI	Key Protocols
Application	Application + Presentation + Session	HTTP, FTP, SMTP, DNS, TELNET
Transport	Transport	TCP, UDP
Internet	Network	IP, ICMP, ARP, RARP
Network Access (Link)	Data Link + Physical	Ethernet, Wi-Fi, PPP

1.8-1.9 OSI vs TCP/IP — Comparison & Critiques

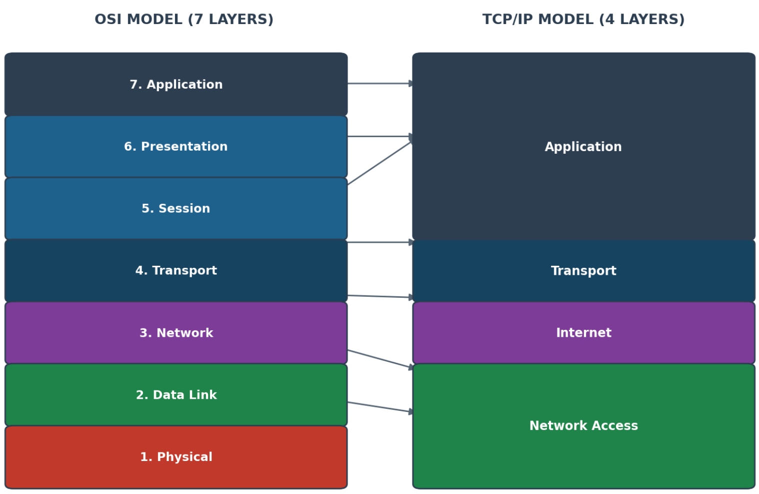

Figure 1.1: OSI's 7 layers mapped onto TCP/IP's 4 layers

Aspect	OSI Model	TCP/IP Model
Layers	7 (strict, generic)	4 (practical, protocol-specific)
Development	Model first, then protocols	Protocols first (Internet), model described after
Usage	Mainly conceptual/teaching reference	Actually implemented — powers the Internet
Coupling	Layers strictly independent	Layers more tightly coupled to specific protocols

- Critiques of OSI: Overly complex; Session & Presentation layers rarely used separately in practice; designed before protocols existed, so poor fit to real implementations; slow standardisation vs. the fast-moving Internet.
- Critiques of TCP/IP: Not a general model (tied to its own protocols); doesn't clearly distinguish service/interface/protocol concepts; Network Access layer is not really 'one' layer; less useful for describing non-IP technologies.

UNIT 2 — THE PHYSICAL LAYER

2.1 Functions of Physical Layer

- Bit representation/encoding, data rate (bits/sec), synchronization of bits, line configuration, physical topology, transmission mode (simplex/half-duplex/full-duplex).

2.2 Data and Signals

- Analog signal: Continuous, infinite values over time (e.g. sine wave). Digital signal: Discrete levels (0/1).
- Transmission Impairments: Attenuation (signal weakens with distance, measured in dB), Distortion (signal shape changes — differing propagation speeds), Noise (thermal, induced, crosstalk, impulse).

Formula	Meaning
Nyquist: $C = 2B \log_2 L$	Max data rate for a noiseless channel (B=bandwidth, L=signal levels)
Shannon: $C = B \log_2(1+SNR)$	Max data rate (capacity) for a noisy channel

- Performance measures: Bandwidth, Throughput, Latency (propagation + transmission + queuing + processing delay), Jitter, Bandwidth-delay product.

2.3 Data Transmission Media

Category	Examples	Key Trait
Guided (Wired)	Twisted Pair, Coaxial Cable, Fibre-Optic	Signal travels along a solid medium
Unguided (Wireless)	Radio waves, Microwave, Infrared	Signal propagates through free space/air
Satellite	GEO, MEO, LEO satellites	Long-distance wireless relay via orbiting relay stations

2.4 Bandwidth Utilization

• Multiplexing: Combines multiple signals onto one channel — FDM (Frequency Division), TDM (Time Division: sync/statistical), WDM (Wavelength Division, for fibre).

• Spreading: Spreads a signal over a wider bandwidth for security/robustness — FHSS (Frequency Hopping), DSSS (Direct Sequence).

2.5 Switching

Type	How it Works	Trait
Circuit Switching	Dedicated end-to-end path reserved before data transfer (e.g. traditional telephone)	Fixed delay, guaranteed bandwidth, wasteful if idle
Message Switching	Entire message stored and forwarded hop-by-hop (store-and-forward)	No dedicated path; can cause high delay/storage need
Packet Switching	Message split into packets, routed independently, reassembled at destination	Efficient bandwidth use; basis of the Internet

2.6 Telephone, Mobile & Cable Networks for Data

• Telephone network (PSTN): Originally circuit-switched voice; DSL/ADSL added for data over the same copper local loop.

• Mobile network: Cellular structure with base stations/cell towers; generations 2G→5G progressively add data capability and speed.

• Cable network: Uses coaxial/hybrid fibre-coax originally built for TV; DOCSIS standard enables broadband Internet over the same cable.

UNIT 3 — THE DATA LINK LAYER

3.1 Functions of Data Link Layer

• Framing, physical/MAC addressing, flow control, error control, access control (media sharing), reliable node-to-node delivery.

3.2 Data Link Control

• Framing: Marks start/end of frames — methods: character count, byte/character stuffing (flag bytes), bit stuffing (0-insertion after five 1s).

• Flow Control: Prevents fast sender overwhelming slow receiver — Stop-and-Wait (send one frame, wait for ACK), Sliding Window (send multiple frames within a window).

• Error Control: Detect/retransmit corrupted or lost frames — ARQ techniques: Stop-and-Wait ARQ, Go-Back-N ARQ, Selective-Repeat ARQ.

3.3 Error Detection and Correction

Technique	Type	Idea
Parity Check (VRC)	Detection	Add 1 bit so total 1s is even/odd; detects odd number of bit errors
Checksum	Detection	Sum of data segments (1's complement); mismatch = error
Cyclic Redundancy Check (CRC)	Detection	Polynomial division remainder appended; very strong burst-error detection
Hamming Code	Correction	Adds redundant parity bits at specific positions to locate & fix single-bit errors

3.4 HDLC & PPP

• HDLC (High-Level Data Link Control): Bit-oriented protocol; frame = Flag-Address-Control-Data-FCS-Flag; supports Normal Response Mode, Asynchronous Response Mode, Asynchronous Balanced Mode.

• PPP (Point-to-Point Protocol): Used for direct link between two nodes (e.g. dial-up/DSL); provides framing, LCP (link control), NCP (network control, e.g. for IP), authentication (PAP/CHAP).

3.5 Channel Allocation Problem

• Deciding how to allocate a single shared channel among multiple competing users/stations — static allocation (FDM/TDM, wasteful if traffic is bursty) vs dynamic allocation (based on demand).

3.6 Multiple Access Protocols

Category	Protocol	Key Idea
Random Access	ALOHA (Pure/Slotted)	Transmit whenever ready; collisions resolved by retransmission after random wait
Random Access	CSMA	'Listen before talk' — sense carrier before transmitting to reduce collisions
Random Access	CSMA/CD	CSMA + Collision Detection; abort & back off on collision (classic Ethernet)
Random Access	CSMA/CA	CSMA + Collision Avoidance (used in wireless, e.g. Wi-Fi, since collisions can't be reliably detected)
Controlled Access	Reservation	Stations reserve time slots in advance before transmitting
Controlled Access	Polling	A controller/primary station polls each secondary in turn for data
Controlled Access	Token Passing	A special 'token' frame circulates; only the token holder may transmit
Channelization	FDMA	Available bandwidth divided into distinct frequency bands per station
Channelization	TDMA	Bandwidth shared via fixed time slots per station
Channelization	CDMA	All stations transmit simultaneously using unique orthogonal codes

3.7 Wired LAN — Ethernet & FDDI

- Ethernet (IEEE 802.3): Uses CSMA/CD (legacy) or full-duplex switching (modern); frame includes Preamble, Destination/Source MAC, Type/Length, Data, FCS. Variants: 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T (Gigabit).
- FDDI (Fiber Distributed Data Interface): Token-passing ring topology over fibre-optic cable, dual counter-rotating rings for fault tolerance, 100 Mbps, mainly used as a legacy campus backbone.

3.8 Wireless LAN — IEEE 802.11x & Bluetooth

Standard	Detail
IEEE 802.11 family	Defines Wi-Fi; variants a/b/g/n/ac/ax differ in frequency band, modulation, and max speed
MAC Layer	Uses CSMA/CA with optional RTS/CTS handshake to reduce hidden-terminal collisions
Bluetooth (IEEE 802.15.1)	Short-range PAN technology; uses frequency-hopping spread spectrum (FHSS); master-slave 'piconet' structure

3.9 Token Bus, Token Ring & Virtual LAN

- Token Bus (IEEE 802.4): Physical bus, logical ring — token passed in a defined logical order among stations.
- Token Ring (IEEE 802.5): Physical ring topology; a token circulates and a station must hold it to transmit, guaranteeing no collisions.
- Virtual LAN (VLAN): Logically groups devices into separate broadcast domains regardless of physical location, using switches and 802.1Q tagging; improves security, manageability, and traffic isolation.

UNIT 4 — THE NETWORK LAYER

4.1 Functions of Network Layer

- Logical addressing, routing (path selection), packet forwarding, fragmentation/reassembly, congestion control, internetworking of heterogeneous networks.

4.2 Virtual Circuits vs Datagram Subnets

Aspect	Virtual Circuit	Datagram
Path	Fixed path set up before data transfer (connection-oriented)	Each packet routed independently (connectionless)
Ordering	Packets arrive in order	Packets may arrive out of order
Overhead	Setup/teardown phase needed	No setup; higher per-packet header/routing overhead
Example	ATM, MPLS	IP (the Internet)

4.3 IPv4 Addressing

- Address space: 32 bits → 2^{32} (~4.29 billion) addresses, written in dotted-decimal (e.g. 192.168.1.1).

Class	Leading Bits	Range (1st octet)	Default Mask	Use
A	0	1 – 126	255.0.0.0 (/8)	Very large networks
B	10	128 – 191	255.255.0.0 (/16)	Medium networks
C	110	192 – 223	255.255.255.0 (/24)	Small networks
D	1110	224 – 239	—	Multicast
E	1111	240 – 255	—	Reserved/experimental

- Classless Addressing (CIDR): Written as address/prefix (e.g. 192.168.1.0/26); allows arbitrary-size blocks, reduces address wastage vs classful.
- Subnetting: Borrowing host bits to create smaller sub-networks; each subnet has its own network ID, usable host range, and broadcast address.
- NAT (Network Address Translation): Maps many private internal addresses to one/few public addresses — conserves public IPv4 space; types: Static, Dynamic, PAT (Port Address Translation/overloading).

4.4 IPv4 Datagram Format & Fragmentation

- Key header fields: Version, Header Length (IHL), Type of Service, Total Length, Identification, Flags, Fragment Offset, TTL, Protocol, Header Checksum, Source/Destination IP.
- Fragmentation: A router splits a datagram into smaller fragments when it exceeds the outgoing link's MTU; Identification field ties fragments together, Fragment Offset marks position, reassembly occurs only at the final destination.

4.5 IPv6 Address Structure & Advantages over IPv4

- Structure: 128 bits, written as 8 groups of 4 hex digits separated by colons (e.g. 2001:0db8::1); supports zero-compression ('::').
- Advantages over IPv4: Vastly larger address space (2^{128}), simplified/streamlined header (faster routing), built-in IPSec support, no need for NAT, better multicast/anycast support, auto-configuration (SLAAC).

4.6 Routing Algorithms

Algorithm	Approach	Trait
Distance Vector Routing	Each router shares its full routing table (distance to each destination) with direct neighbours only; uses Bellman-Ford	Simple but slow convergence; 'count-to-infinity' problem (e.g. RIP)
Link State Routing	Each router floods link-state info to all routers in the area; each independently computes shortest paths using Dijkstra's algorithm	Faster convergence, more overhead/complexity (e.g. OSPF)

4.7 Internet Control Protocols

- ARP (Address Resolution Protocol): Resolves a known IP address to its corresponding MAC address on a local network.
- RARP (Reverse ARP): Resolves a known MAC address to an IP address (legacy — largely replaced by DHCP).
- ICMP (Internet Control Message Protocol): Carries error/diagnostic messages (e.g. Destination Unreachable, Time Exceeded); basis of ping and traceroute.

4.8 Routing Protocols & Addressing Modes

- OSPF (Open Shortest Path First): Interior Gateway Protocol; link-state; uses Dijkstra's algorithm; fast convergence; used within a single autonomous system (AS).
- BGP (Border Gateway Protocol): Exterior Gateway Protocol; path-vector based; used to route between different autonomous systems across the Internet backbone.
- Unicast: One sender → one specific receiver. Multicast: One sender → a specific group of receivers. Broadcast: One sender → all hosts on a network/subnet.

UNIT 5 — THE TRANSPORT LAYER

5.1 Functions of Transport Layer

- Provides process-to-process (end-to-end) delivery using port numbers; handles segmentation/reassembly, connection management, flow & error control, and multiplexing/demultiplexing of application data.

5.2 Elements of Transport Protocols

- Addressing: Port numbers identify the sending/receiving process (e.g. well-known ports 0-1023).
- Connection Establishment/Release: e.g. TCP's 3-way handshake (SYN, SYN-ACK, ACK) to open; FIN/ACK exchange to close.

- Flow Control & Buffering: Sliding-window mechanism prevents a fast sender from overwhelming receiver buffers.
- Error Control: Sequence numbers, acknowledgments, checksums, and retransmission timers ensure reliable delivery.
- Multiplexing/Demultiplexing: Combines multiple application streams onto one network connection (and separates them again) using port numbers.
- Crash Recovery: Mechanisms to resume or restart a transport connection correctly after a host/process failure.

5.3 User Datagram Protocol (UDP)

- User Datagram: Simple 8-byte header — Source Port, Destination Port, Length, Checksum — followed by data.
- UDP Operations: Connectionless, unreliable, no ordering guarantee, no flow/congestion control — minimal overhead, low latency.
- Uses of UDP: DNS queries, DHCP, streaming media, VoIP, online gaming, SNMP — anywhere speed matters more than guaranteed delivery.
- RPC (Remote Procedure Call): Lets a program invoke a procedure on a remote machine as if it were local; often built on top of UDP (or TCP) for lightweight request-response calls.

5.4 Principles of Reliable Data Transfer

- Building reliability: Achieved via checksums (detect corruption), sequence numbers (detect duplicates/reordering), acknowledgments (confirm receipt), and timers (detect & trigger retransmission of loss).
- Pipelined Reliable Data Transfer: Sender allowed to send multiple unacknowledged packets ('in flight') to fully utilise bandwidth-delay product, rather than stop-and-wait for each single packet.

Protocol	Window/Retransmission Behaviour
Go-Back-N (GBN)	Sender can have N unacked packets in flight; on a lost/errored packet, receiver discards all out-of-order packets and sender must resend everything from that point onward
Selective Repeat (SR)	Receiver buffers out-of-order (but correct) packets individually; sender retransmits only the specific lost/errored packet, improving efficiency over GBN

5.5 Transmission Control Protocol (TCP)

- TCP Services: Connection-oriented, reliable, byte-stream delivery, full-duplex, in-order delivery, flow & congestion control.
- TCP Features: 3-way handshake connection setup, sliding window flow control, cumulative/selective acknowledgments, retransmission timers, congestion control algorithms.

TCP Segment Header Field	Purpose
Source / Destination Port	Identify sending & receiving application processes
Sequence Number	Byte-stream position of first byte in this segment
Acknowledgment Number	Next byte the receiver expects
Header Length (Data Offset)	Size of the TCP header (accounting for options)
Flags (URG,ACK,PSH,RST,SYN,FIN)	Control bits for connection setup/teardown and data handling
Window Size	Number of bytes the receiver is willing to accept (flow control)
Checksum	Error detection over header + data
Urgent Pointer	Points to urgent data within the segment, if URG flag set

5.6 Principles of Congestion Control

- Congestion occurs when offered network load exceeds available capacity, causing rising delay & packet loss.
- TCP congestion control phases: Slow Start (exponential growth of congestion window from 1 MSS), Congestion Avoidance (linear/additive growth after reaching a threshold), Fast Retransmit (resend after 3 duplicate ACKs without waiting for timeout), Fast Recovery (halve window rather than restart from scratch after fast retransmit).
- AIMD (Additive Increase / Multiplicative Decrease): Core congestion-avoidance philosophy — increase window slowly, cut it sharply on detected loss.

UNIT 6 — THE APPLICATION LAYER

6.1 Functions of Application Layer

- Provides the interface between network services and end-user software — enabling file transfer, email, web browsing, remote login, name resolution, and network management directly usable by applications.

6.2 Application Layer Protocols & Ports

Protocol	Port(s)	Purpose
DNS	53	Resolves domain names to IP addresses
DHCP	67 (server) / 68 (client)	Automatically assigns IP configuration to hosts
WWW / HTTP	80	Transfers hypertext (web pages) — stateless request/response
HTTPS	443	HTTP secured via TLS/SSL encryption
TELNET	23	Unencrypted remote terminal/login access
FTP	20 (data) / 21 (control)	Transfers files between client and server
SMTP	25 (587 submission)	Sends/relays outgoing e-mail between servers
POP3	110	Downloads e-mail to a single client, typically removing it from server
IMAP	143	Manages e-mail on the server, supporting multi-device sync

6.3 Traffic Analyzer Tools

Tool / Concept	What it Does
SNMP (Simple Network Management Protocol)	Standard protocol for collecting & organising information about managed devices on a network
MRTG (Multi Router Traffic Grapher)	Polls devices via SNMP and generates HTML/graph reports of traffic/load over time
PRTG Network Monitor	Commercial all-in-one network monitoring tool — bandwidth, uptime, SNMP, sensors, alerting
Cisco Packet Tracer	Network simulation tool for designing, configuring, and testing virtual network topologies
Wireshark	Packet-capture/protocol-analyzer tool — inspects live traffic frame-by-frame for troubleshooting & security analysis

UNIT 7 — NETWORK SECURITY

7.1 A Model for Network Security

Security communication is modelled as a message passing from Sender to Receiver over an insecure channel, transformed by a security-related function (e.g. encryption) using secret information (a key), potentially assisted by a trusted third party (e.g. a key distributor or certificate authority), while defending against an opponent who may intercept, read, or modify the transmitted data.

A MODEL FOR NETWORK SECURITY

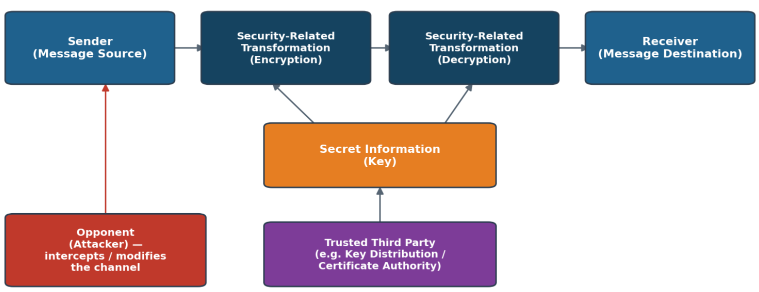

Figure 7.1: A general model for network security (Stallings)

• Core security goals (CIA triad): Confidentiality, Integrity, Availability — often extended with Authentication and Non-repudiation.

7.2 Principles of Cryptography

Type	Key Usage	Trait	Examples
Symmetric Key	Same single key for encryption & decryption, shared secretly in advance	Fast, but key distribution is a challenge	DES, 3DES, AES
Public (Asymmetric) Key	Key pair — public key encrypts, private key decrypts (or vice-versa for signatures)	Solves key-distribution problem; slower than symmetric	RSA, ECC, Diffie-Hellman

7.3 Public Key Algorithm — RSA

- Key generation: Choose two large primes p, q → n = p×q; compute φ(n) = (p-1)(q-1); choose public exponent e coprime to φ(n); compute private exponent d such that e×d ≡ 1 (mod φ(n)).
- Public key = (e, n); Private key = (d, n).
- Encryption: C = M^e mod n. Decryption: M = C^d mod n.
- Security rests on the practical difficulty of factoring the large number n back into its prime factors p and q.

7.4 Digital Signature Algorithm

- A digital signature lets a receiver verify the authenticity/integrity of a message and provides non-repudiation (sender cannot deny sending it).
- General process: Sender hashes the message → encrypts the hash with their own private key (the 'signature') → sends message + signature.
- Verification: Receiver hashes the received message independently, decrypts the signature with the sender's public key, and checks the two hash values match.
- DSA (Digital Signature Algorithm): A specific public-key algorithm (based on discrete logarithms) standardised by NIST specifically for producing digital signatures (encryption of data itself is not its purpose).

7.5 Communication Security

Mechanism	Purpose
IPSec (IP Security)	Suite of protocols (AH, ESP) securing IP traffic at the network layer — provides confidentiality, integrity, authentication; used heavily for VPNs
VPN (Virtual Private Network)	Creates an encrypted 'tunnel' across a public network (e.g. the Internet) so remote users/sites can securely access a private network as if directly connected
Firewall	Filters incoming/outgoing traffic based on rules (packet-filtering, stateful inspection, proxy/application-level) to block unauthorised access
Wireless Security	Protects Wi-Fi links via encryption/authentication standards — WEP (weak/legacy), WPA, WPA2, WPA3 (current recommended standard)

Last-Minute Quick Recall

✓ OSI = 7 layers (mnemonic: All People Seem To Need Data Processing); TCP/IP = 4 layers.
✓ Nyquist (noiseless) vs Shannon (noisy) — both give the theoretical maximum channel data rate.
✓ Circuit switching = dedicated path; Packet switching = independent, routed packets (basis of Internet).
✓ CSMA/CD = wired collision detection (Ethernet); CSMA/CA = wireless collision avoidance (Wi-Fi).
✓ Classful addressing: Class A/B/C = large/medium/small networks; CIDR/subnetting = classless, flexible sizing.
✓ Distance Vector (Bellman-Ford, e.g. RIP) = slow convergence; Link State (Dijkstra, e.g. OSPF) = fast convergence.
✓ UDP = fast, connectionless, unreliable; TCP = reliable, connection-oriented, congestion-controlled.
✓ TCP congestion control: Slow Start -> Congestion Avoidance -> Fast Retransmit -> Fast Recovery (AIMD).
✓ Well-known ports: DNS 53, HTTP 80, HTTPS 443, FTP 20/21, SMTP 25, POP3 110, IMAP 143, TELNET 23.
✓ Symmetric crypto = one shared key (fast); Asymmetric/Public-key crypto = key pair (solves distribution problem, e.g. RSA).
✓ RSA security = difficulty of factoring n = p x q back into its prime factors.
✓ Digital signature = hash + encrypt with sender's PRIVATE key; verify by decrypting with sender's PUBLIC key.
✓ IPSec/VPN secure data in transit; Firewalls filter traffic; WPA2/WPA3 secure Wi-Fi links.

— End of Cheat Sheet — Good Luck! —