**ASCII & Unicode:** represents characters and notations to binary no. that computer understands

* ASCII - 7 bits, Unicode - 8,16,32 bits
* Unicode takes up more memory but includes more characters (eg. non-English)

**LAN:**

Local Area Network - self-contained network spanning a small area eg. home /sch

**WAN:**

Wide Area Network - network spanning a large area, aften across multiple geographical locations eg. city/country/world

**Intranet:**

* Private network using Internet protocols and services to share info with limited no. of people Eg. company to employees
* Can be accessed from Internet but with restrictions
* (+) Keeps sensitive info private and secure
* (+) Convenient storing, organisation, sharing and collab of info

**Internet:**

* Largest global WAN linking every country in the world, public owned and operated
* Contains a large no. of Intranet
* OSI and TCP/IP models:
  + Explains how data communication is processed in software and hardware components, blueprint for soft and hardware developers to build a network
  + OSI - Open Systems Interconnection: Theoretical
  + TCP -  Transmission control protocol / IP - Internet Protocol: Implemented in development of Internet
  + Designed into layers with supported protocols
    - Protocol: set of rules governing exchange of data between devices
    - Simplifies network model
    - Enables programmers to specialize in particular layers
    - Provides design modularity
    - Allows production of standardised interfaces by networking vendors

**TCP/IP:**                                                                                                         **\*\*1 Byte = 8 bits**

* Communication only between adj layers, headers with relevant info added to data unit in senders process and removed in receiver’s process

* Application: provides high-level functionality to end users (Msg)
  + File transfer protocol: FTP, SSH
  + Email protocol:
    1. SMTP(send) , port no. 25/465/587
    2. POP3 (receive and store mail at client), port no. 143, 993 (secured)
    3. IMAP4 (receive and store mail at server, sync on multiple devices, allowing better organisation), port no. 110, 995 (secured)
  + Webpage protocol: HTTP, HTTPS
  + **DNS:** Domain Name System
    1. Translates domains given by user to IP address that computer processes
    2. A hierarchy of DNS servers searches the domain database to find corresponding IP
  + DHCP (Dynamic Host Configuration Protocol) server:
    1. Allocates unique IP addresses to clients in network
       - Static allocation: Network admin assigns IP to client, DHCP server passes it to client
       - Automatic allocation: DHCP server assigns permanent IP to client from its pool of IP addresses
       - Dynamic allocation: DHCP server leases reusable IP to client for a period of time
    2. DHCP Lease process:
       - Discover: client broadcast in network to all devices to look for DHCP server
       - Offer: DHCP server offers an IP
       - Request: client requests to release the address
       - Ack: DHCP server sends address to client for acknowledgement

* Transport: transmits msgs between any 2 prog (Segment)
  + Port no. : no. representing process running on a network
    1. Source and destination port embedded in header of every data segment
    2. Eg. HTTP 80, IMAP 143, DNS 53
  + Socket: identifier for application process on network
    1. Combi of IP address and port no.
  + Protocols:
    1. TCP: Transmission control protocol
       - 3-way handshake to establish connection before data transmission
         * Device A sends an SYN (synchronise) packet to Device B to establish connection
         * B responds with sending an SYN-ACK (synchronise - acknowledgement) packet back to A
         * A acknowledges this with sending an ACK packet of its own back to B
         * Data can only be transmitted after handshake is complete
       - Breaks up data into segments with sequential no. for reassembly at receiver (sequencing helps reordering into original order)
       - (+) security and validity of data
       - (+) congestion control
       - (-) Slow handshake for devices with high latency
       - (-) Cannot be used for broadcast/multicast transmission
       - Header:
         * Source and destination port no. (2 bytes each)
         * Seq no.
         * ACK no.
    2. UDP: Universal Datagram Protocol
       - Performance > ability to receive all data
       - Eg. Streaming media
       - (+) Connectionless: No waiting time for connection
       - (+) More efficient: no retransmission of lost packets required
       - (-) Missing Stability and reliability
       - (-) No flow control
       - Header:
         * Source and destination port no. (2 bytes each)

* Network: determines route between any 2 devices (Packet)\*can be from diff networks
  + Network device: router
    1. Uses IP address to send data packets to designated hosts
    2. Maintains a routing table
  + Network device: modem
    1. Internet only reads analog signals, computer only reads digital signals, modem converts data between the 2 transmission media
  + Switching: technique for transmitting data over network to destination network devices
  + Circuit switching network:
    1. 2 nodes establish dedicated communication channel (circuit) before transmission
    2. All packets follow same route to destination
    3. (+) Easier to reassemble packets at receiver end as they arrive in sending order (time-efficient)
    4. (-) Easy for packets to be intercepted during transmission as exact route of all packets are known (data insecurity)
  + Packet switching network:
    1. Each packets takes its best available route and travels independently to reach destination device
    2. All packets follow diff routes to destination
    3. (+) Efficient as each packet finds fastest route
    4. (+) More secure as multiple routes are harder to attack
    5. (-) Longer to reassemble packets at receiver end as packets arrive at diff orders than sending order
  + IP: see IP addressing   [protocol]

* Data link: transmits packets between devices in the same network (Frame)
  + Network device: switch
    1. Sends data frames to designated host
    2. Recognises host by MAC, maintains a MAC table
  + Protocol: Ethernet, MAC, WiFi, Bluetooth
  + Describes how devices format data for transmission within same LAN
  + MAC address: Media Access Control
    1. Physical address of device
    2. Unique for each machine, cannot be changed
    3. 6 bytes/48 bits
    4. 6 grps of 2 hexadecimal (0-9 and A-F) separated by colons or dashes

* Physical: transmits individual bits through a transmission medium (bit)
  + Wired:
    1. Twisted pair(current): center twisted pairs of wires

Coaxial cable(digital signal): center dielectric insulator outside centre core

1. Optic Fibre (lights pulses)

* Wireless:
  1. Satellite Network
  2. Cellular Network
* Protocol: USB, IrDA

**IP addressing:** logical address identifying each device on the network (can change frequently)

* IP responsible for routing indiv packet and addressing (used by routers)
* Devised by Internet Assigned Numbers Authority (IANA), American Registry of Internet Numbers (ARIN) assigns IP addresses to public, private and gov organizations
* 5 classes based on the section before the first dec. pt Eg. 192.149.252.76

* IPv4:
  + Older than v6, no. of addresses 2^32
  + 32 bits
  + Denery no. 0 - 255 separated by dots
    - Class A: 0 - 126 (gov)
    - Class B: 128 - 191 (large and medium sized companies)
    - Class C: 192 - 223 (other grps)
    - Class D: 224 - 239 (reserved for multicasting: grp communication where data transm. addressed to grp of destination computers simultaneously)
    - Class E: 240 - 255 (reserved for experimentation)
    - \*\*127: Assigned for loopback function, directs to local host, useful for socket programming
    - Classes A, B , C: Contains host ID
  + Network part: Identifies LAN in which device is located (IP address, subnet mask)
  + Host part: Identifies device in LAN (IP address, subnet mask complement)
  + Subnet mask
    - Subnets: divides larger networks into smaller, more efficient sub networks
    - 32 bit
    - Series of 1s first then 0s
    - 1 true, 0 false (binary: adding up doubled digits from 128 backwards)
    - No. of 1s = n: [IP]/n

* IPv6:
  + Newer than v4, no. of addresses 2^128
  + 128 bits
  + 8 grps of 4 hexadecimal (0-9 and A-F) separated by colons, shorted by omitting 0s and sections of consec. 0s (replace with ::)

**Communication protocols in a network needed to standardize format etc of data and signals such that diff devices are able to communicate smoothly.**

**Client server architecture:**

Client-Server Network:

* One or more devices act as server, other devices request service from server
* Server:
  + Centralized storage area for resources
  + Dedicated to provide service to other devices in the network only
  + Access control to resources on network
  + Filters network traffic
* Client:
  + Sends requests to server
  + Does not share any resources, access rights are defined by servers only
* (+) More secure as server and other clients unaffected by compromise of one client
* (+) Resources on server can be updated faster and more reliably
* (-) Server more vulnerable to cyberattack as its downfall leads to fall of whole network
* (-) Centralized server more expensive to build and requires professionals to maintain

Peer-to-peer Network: Eg. Blockchain

* Each device (peer) is able to share resources without going through a server
* All devices interact and share resources with others, sharing responsibility and capability
* (+）No dependency on a server/central computer
* (-) No centralised management, so backups and updates must be done individually

**WEB:**

Terms:

* Web page: doc written with HTML
* Website: grp of interlinked and well-structured web pages on same domain
* Web server: stores and delivers contents of web pages and websites to users
* Web browser: software - retrieves contents from web server to display on user’s device
* Web application: software - exists on server, runs with web browser through web page

Static websites: Always display the same contents

Dynamic websites: Web page processed by web application (+ database sometimes)

**Encryption:**  Process of encoding a message so only authorized parties can access it

* Sender uses a secret key and an encryption algorithm to encrypt a plaintext to a cipher text message
* Receiver uses a secret key and a decryption algorithm to decrypt the cipher text to the original plaintext message
* By itself, does not verify sender of msg or stop data from being deleted by attacker
* Symmetric:
  + One secret key shared between sender and receiver
  + Same encryption and decryption key
  + (+) Fast processing
  + (-) Low security once the key was intercepted
  + Commonly used: Advanced Encryption Standard (AES)
* Asymmetric:
  + One public key and one private key that are mathematically related
  + One cannot be derived from another
  + (+) Slower processing
  + (-) More secured as full key is not easily obtained
  + Commonly used: Rivest-Sharmir-Adleman (RSA)
  + Process:
    - The sender uses the receiver's public key to encrypt the message. This public key can be shared with anyone.
    - The receiver’s private key is the only key to decrypt the message.
    - Even if public key is intercepted, message is still kept secret as the private key held solely by the receiver is needed to decrypt the message.

**Electronic signature:** Equivalent to paper signature, an electronic record adopted by a person with the intent to sign a contract - can be replicated easily with eg. an image of the signature

**Digital signature:** The encryption and decryption technology that secures the data associated with a signed document and helps to verify the authenticity of the document

* (+) Allows for authentication that the message was created by the known sender
* (+) Ensures non-repudiation such that the sender cannot deny having sent the message
* (+) Ensures integrity of the message that it is not altered in transit
* Widely used on the Internet, Emails and blockchains.
* Technology Involved: Encryption (use of public key and private key), Hashing
* Sender Side:
  + The sender uses a hash algorithm to create a hashed version of the message
  + The sender uses its private key to encrypt the hash to the digital
  + signature
  + Both the message (encrypted or not) and the digital signature are
  + sent to the receiver
* Receiver Side:
  + The receiver uses the sender’s public key to decrypt the digital signature back to the sender’s version of hash
  + The receiver uses the same hash algorithm to create a new hash from the received message
  + If the two hashes match, it means the data is not altered and is sent by the known sender

**Hashing**

* Generating a short string of text (called hash, hash value or digest) from any size of data
* Unique hash for different data
* DIFF from encryption
* Impossible to recover the original data from hash, providing high confidentially/integrity
* Commonly used: SHA256 (Secure Hash Algorithm)

**Data Verification vs Data Validation**

* Data validation: check if the data is in valid format, eg. type check, length check
* Data verification: check if the data is what the user intends to give, eg. twice input of password, proofread before submission
* \*Login username and password belong to neither.
  + When the username has been taken and is required to choose another username it is considered as data validation.

**Identification vs Authorisation vs Authentication**

* Identification: user claims an identity, eg. username
* Authorisation: system validates the granted permission of an authenticated user to access the resources, eg. different system modules for students and staff
* Authentication: system validates the identity of a user, eg. username + password
  + Users need to prove their identity by providing some type of credentials.
  + \*Checking human/robot (CAPTCHA) is NOT authentication
  + Factors:
    - Something you know: password, secret Qns
    - Something you have: staff card, One-time-password
    - Something you are: fingerprint, iris, face, voice
  + Multi-Factor Authentication (MFA)
    - Uses more than one factor of authentication
    - eg. Staff card + password, OTP + password

**Cyber Attack**

* Malware: malicious software that aims to damage and/or gain unauthorised access to computer systems, Target: Computers
  + Self-replicating to infect other computers in the network:
    - Virus:
      * Attaches itself to another file or program and modifies them by inserting its own code
      * Remains dormant until executed by the user
      * Spreads by transfer of infected files over the network
      * Consequences: corrupted system software or stolen data
      * May lead to DOS as virus replicates to infect more computers
    - Worm:
      * Type of virus, works similarly to normal virus but need not attach to a file and can spread without any human intervention after activation, installed via security failures of target (host) computer
      * Consequences: Modified/deleted software, user data leaked to or backdoor installed for attacker computer, slowed user operations when there are too many copies of the worm on a single network
      * May lead to DDOS as multiple computers have replicating worms
      * May lead to ransomware when attacker gains control of the data

* Not self-replicating - only affects the computer it is downloaded on
  + Trojan Horse:
    - Appears disguised as legitimate program, must be executed by user to activate (eg. social engineering attack, fake antivirus/helpful program, drive-by/automatic download when visiting malicious website)
    - Once gaining access, it runs malicious codes to cause damage to the computer and hides very well
    - Consequences: poor device performance, frequent crashes, alterations to software and desktop settings, increase in browser pop-ups that download more malware into the device
  + Ransomware:
    - Infects with downloaded files (eg. social engineering attack) or shared networks, locks computer system or encrypts data using algorithms that are realistically impossible to crack, can take over user’s admin access
    - Forces the user to pay a ransom (usually cryptocurrency) to get the computer restored/unlocked or threaten to publish files
    - Consequences: Loss in money and/or data (ransom scam - no restoration even after paying) , stability and prices of certain currency/cryptocurrency eg. bitcoin
  + Adware:
    - Displays unwelcome information or advertisement on the computer,  installed through unsecured downloads or visiting malicious websites
    - Consequences: Browsing/processing speed slowed, settings changed, user data collected without his knowledge, customised ads which download other malware secretly when clicked
  + Spyware
    - Hidden program that secretly monitors user activity and transmits information to attackers without the user’s knowledge, installed through social engineering scams
    - Consequences: Sensitive/personal information stolen, more ads

* Target: Networks
  + Denial of Service (DOS): attacks the network traffic from one source to exhaust resources and bandwidth such that the system cannot fulfil legitimate requests
  + Distributed Denial of Service (DDOS): multiple compromised devices (botnet) to attack the system simultaneously to achieve similar results as DOS

* Social Engineering Attack: Use of deception and trickery to violate security guidelines or to convince users to provide data, Target: User’s human psychology
  + Often precursor to another type of attack
  + Phishing: (common technique for spoofing)
    - attacker sends a message (eg. email) that seems to come from a respected organization, claiming that the recipient needs to provide a private information to the sender for verification purposes
  + Spoofing:
    - attacker pretends to be someone else to conceal their identity, using fake IP addresses, MAC addresses, email etc, often triggers malware attacks
  + Spam:
    - users are flooded with email or messages that act as vehicles carrying advertisement material or viruses

* Protection Scheme as User (Focus: **Blocking/Preventing installations** of malware)
  + Maintain good digital hygiene, avoid suspicious links or websites, downloading from untrusted/pirated sources and connecting to untrusted public Wi-Fi, always verify authenticity before downloads or providing information to online personnel
    - ALL Social Engineering
  + Install a respected antivirus/antimalware software eg. Norton to scan incoming data and prevent malware installation
    - ALL Malware
  + Keep operating systems of devices updated so there will be less unpatched system flaws that may be exploited for attacks
    - ALL Malware
  + Backup important files regularly and store in a separate location so data can still be retrieved when computer is attacked, best in offline harddrive
    - ALL Malware and Social Engineering

* Protection Scheme as a Computing Professional (Devices can combine many security features, eg. Unified Threat Management (UTM)
  + Host-based: only protects device it is installed on (data link layer)
  + Network-based: installed on router/stand-alone/from cloud to protect the entire network (network layer) [Can use both host and network based at the same time]
  + Firewall (Focus: **Traffic and access control**)
    - Prevent unauthorized access from entering a private network, monitors and filters all incoming and outgoing network traffic based on its set of security rules (Access control list) that allow or deny permission
    - Rules based on software and hardware levels: eg. port (application), MAC (device), IP addresses (website), content (parental control)
    - Limitations:
      * Can be bypassed by hiding malware inside legitimate files or sources user exempted from firewall for normal usage
      * Cannot protect against internal attacks as it does not need to pass a firewall, eg. virus from an infected computer in the same network
      * May block legitimate programs from entering (not against running)
  + Proxy Server (Focus: **Online info protection, personal traffic control**)
    - Acts as intermediary (middle-man) for client requests seeking resources from other servers
    - Hides IP address and login details
    - Controls incoming and outgoing traffic at individual application level
    - Caching machine: stores a subset of data so future requests for them are served faster than possible by accessing the primary storage location
  + VPN: Virtual Private Network (Focus: **Online info protection, network traffic control**)
    - Unblocks censored websites
    - Adds encryption on any data transmitted in and out
    - Controls all traffic that going through the network
  + Intrusion Detection System (Focus: **Attack detection**)
    - Scans and monitors the network traffic or system for malicious activities
    - Sounds an alert when attack is detected
    - NO action taken against the attack
    - Detection Techniques:
      * Signature Based
        + Uses a predefined set of rules to identify unacceptable traffic
        + The rules can contain patterns and signatures provided by  software vendors to identify known security issues
        + (-) Cannot detect unknown attacks
      * Anomaly Based
        + Uses a database of unacceptable traffic patterns identified by analysing traffic flows
        + (-)  accuracy of profile, difficult to determine reason for alert
  + Intrusion Protection System (Focus: **Network traffic control**)
    - Scans and monitors the network traffic or system for malicious activities
    - Sounds an alert when attack is detected
    - Takes action to block unauthorised access or malicious packets from entering the system may drop packets, reset connections, or quarantine suspicious incoming data
    - (+) Fends off DOS, DDOS, virus, and worms
    - (-) Abnormal activity from a legitimate user may be regarded as malicious and lead to DOS