# Week 01

## Objectives

* Confidentiality
  + Data - confirms that private data is not available to unauthorised parties
  + Privacy - who to collect and store specific information and who could disclosure it to whom
* Integrity
  + Data -information changes and updates are done in a specific authorised manner
  + System – functions of the system are performed in unimpaired manner (no manipulation)
* Availability
  + System works according to credentials, and authorised uses could access specific services
* Authenticity – verification of users
* Accountability – security that generates the requirements for an action uniquely traced to a specific entity

## Vulnerabilities/ Threats/ Attacks

* Vulnerabilities
  + Corrupt(loss of integrity)
  + Leaky (loss of confidentiality)
  + Unavailability/ very slow (loss of availability)
* Threats
  + Likelihood to exploit any of the CIA
  + Potential security harm to assets
* Attacks
  + Passive – learn/ make use of information (no effect on system resources)
    - Release of message content
    - Analysis
  + Active – alter system resources/ operations
    - Replay
    - Masquerade
    - Modification of info
    - Denial of service
  + Insider – breach from an insider using brute force methods
  + Outsider – breach from an outsider

## Attack Surface

* Network attack surface -> vulnerabilities over enterprise network, WAN, or internet
* Software attack surface -> vulnerabilities in application, utility, or OS code
* Human attack surface -> vulnerabilities such as social engineering, human error, and insider attack

## Security Principles

1. **Economy of Mechanism** 🡪 security measures in hardware and software should be simple and small
   * Simplicity of security frameworks eases the understanding for users and enables efficient development and verifications
2. **Fail-safe Defaults** 🡪 access should be based on permission rather than exclusion
   * Default situations have minimum access rights
3. **Complete Mediation** 🡪 every access should be checked against access control mechanisms
   * The results of the previous authorisation checks are saved with different performance improvement techniques
4. **Open Design** 🡪 security mechanism design(cryptographic algorithm) should be open so system is scrutinized by multiple parties
   * Security relies on the cryptographic keys remaining a secret
5. **Separation of Privilege** 🡪 multiple privileges are required to access the restricted source
   * Using multiple conditions to satisfied to access restricted resources or to perform actions
6. **Least Privilege** 🡪 every program and user of the system operates on the least of the required privileges to function properly
   * To restrict the abuse of privileges and to minimise the damage caused by the corporatisation of an application or user
7. **Least Common Mechanism** 🡪 with multiple users, the resource/ functions shared by more than one user is minimised
   * Sperate users should have separate channels to access the resources
8. **Psychological Acceptability** 🡪 user interfaces should be well-designed and intuitive
   * Security measures should not interfere with the work of users while granting access to authorised personnel
9. **Work Factor** 🡪 security scheme should be made in comparison with the resources of an attacker
   * Cost of security measurement should be according to the type of resource
10. **Compramised Recording** 🡪 better to record the details of an intrusion than to create more sophisticated measures for prevention
    * The log of the access resources is maintained to check when a threat is observed

### Hacker Types

* + White Hackers 🡪 security professionals who use hacking to expose vulnerabilities
  + Amateurs 🡪 entry-level hackers
    - * Hackers/crackers 🡪 illegal activity for financial gain
      * Hacktivists 🡪 illegal activity for political gain
      * Script kiddies 🡪 illegal activity without knowledge
      * State-sponsored 🡪 advanced hackers

## Penetration Testing

* + Testing the security of a system from a POV of an attacker
  + Prevent compromises
  + Initial engagement 🡪 scoping 🡪 testing 🡪 reporting 🡪 follow up
  + Severity rating for any issue found

### Tests Basis

* + Whitebox Testing
    - * Full information on the target shared with testers
      * Test to confirm the internal vulnerability assessment and management controls.
      * Identifying the software vulnerabilities and misconfigurations in the system
    - Blackbox Testing
      * Internals of the target are not shared with the testers
      * Performed from an external attacker perspective
      * Identifying ways to access internal IT assets

### Attack Stages

* + Reconnaissance and Footprinting
    - * A large part of info gathering is done by passive attacks (public records/ OSINT)
      * Understand the target using a variety of things like identifying network layout, domain, servers and infrastructure details
      * Gives an overview to the pen tester about how network and assets work (anything with an IP)
      * Through this pen, testers can identify additional info that may be overlooked/unknown.
  + Scanning and Enumeration
    - * Identifying target and weak points for attackers.
      * Scanning an organisation's network to find entry points.
      * Slow, sometimes lasting months, as attackers search for vulnerabilities.
      * Enumeration, a counting process, establishes an active connection to the target host.
      * Mainly used to search for attacks and threats.
      * Collects usernames, hostnames, IP addresses, passwords, configurations, etc.
  + Gaining access
    - * Attackers deliver targeted malware to vulnerable systems and people.
      * They map defences and create a battle plan for targeted information.
      * Penetration tests exploit system vulnerabilities to determine unauthorised access and malicious activity.
      * Testers validate, attack, and exploit vulnerabilities using manual techniques, human intuition, and their backgrounds.
  + Maintaining access
    - * Identifying network weaknesses.
      * Gaining access and escalating privileges.
      * Privileged access is crucial for attackers' freedom.
      * Network is taken over, allowing intruders to control it.
      * Malware can be beneficial during this stage; therefore, installation of a rootkit may be necessary.
      * Data Exfiltration is conducted, simulating hacker actions.
  + Covering tracks
    - * Hide or delete evidence of access.
      * Cover up continued access.
      * Use malware to prevent logging or misreporting system information.

## Intruders Motivation

* + Casual snooping 🡪 Inquisitive crackers(those who access resources without permission) seeking unknown information.
  + Disruption 🡪 prevent or inhibit legitimate users from using the system
  + Espionage 🡪 extracting information from a system (commercial info)
  + Use of resources 🡪 use of compromised resources to attack other networks
  + Making a statement 🡪 social/political etc.

# Week 2

## Networking

* + Network 🡪
    - * Set of technologies that connect computers
      * Allows communication and collaboration
      * Collection of computers and devices are connected
    - Uses 🡪
      * Simultaneous access to data
      * Resource sharing
      * Personal communication
      * Easy data backup
    - Types 🡪
      * WAN – large geo area
      * LAN – connection in the same geo area
      * MAN – connection in a small specific area

### Architecture

* + Centralised (client/server) 🡪
    - * One primary device providing service
      * One server connected to multiple clients
      * E.g., websites, most things on the internet
    - DE-centralised (Peer-to-peer/ Ad Hoc) 🡪
      * All devices connected
      * No central entity to control communication
      * E.g., Bluetooth, NFC

## OSI Security Architecture

* + Security attack 🡪 action that compromises the security of info
  + Security mechanism 🡪 process design to detect, prevent, and recover from an attack
  + Security service 🡪
    - * Enhances data processing systems and information transfers.
      * Counters security attacks using security mechanisms.

### OSI Model (PDNTSPA)

* + Application (S) 🡪 interact with end users
    - * Application software access network service and format to application
  + Presentation (S) 🡪 coding of the data
    - * Includes file formats and characters
      * Encryption of data
  + Session (S) 🡪 maintain communication between computers
    - * Create, maintain and disconnect communications between processes
  + Transport (S) 🡪 break data into packets and transmit over the network
    - * Flow control and error checking
  + Network (S) 🡪 logical implementation of network
    - * TCP/IP networking, logical addressing takes familiar for of IP
  + Data Link (H) 🡪 framing received data from the Network layer for transmission over the Physical Layer.
    - * Controlling access to the physical medium.
      * Detecting and correcting transmission errors.
  + Physical (H) 🡪 physical operations of network
    - * Translate binary data from computer language to transport medium language

### TCP/IP Model

The DoD developed a suite of protocols,

* at both the Network and Transport layers of the OSI Reference Model,
* governing all Internet activity and providing a reliable,
* fault-tolerant network infrastructure.
  + Application layer 🡪 provide standardised data exchange (payload – actual application data)
    - * Combine the functions of the Application, Presentation and Session layers of OSI
    - Transport layer 🡪 maintain communication across the network
      * OSI transport layer
    - Network layer (internet layer) 🡪 connects independent networks to transport data packets across networks
      * OSI network layer
    - Data link layer (network interface layer) 🡪 contains protocols, i.e. network components that connect network hosts or nodes
      * Combination of OST data layer and physical layer

#### Internet packet encapsulation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Application packet |  | Application layer |
|  |  | TCP Header | TCP data |  | Transport Layer |
|  | IP header |  | IP Data |  | Network Layer |
| Frame Header |  | Frame Data |  | Frame Footer | Link Layer |

## Protocols

* + Connectionless 🡪 Sends data as soon as enough data is available.
    - * User datagram Protocol (UDP)
  + Connection-oriented 🡪 Comprises set-up, transmission, and tear-down phases with a reliable connection stream
    - * Create a virtual circuit-switched network
      * Transmission control protocol (TCP)

### Packet content

Control information for packet:

* + Headers: Contains information about the packet, including origin, destination IP addresses, protocol type, sequence number, and acknowledgement.
  + Footers: Contains error-checking data and timestamp at the end of the packet.

## Domain Name System (DNS)

* **Application-layer protocol** mapping domain names to IP addresses.
* Provides a distributed internet database.
* Stores Address (A) record (IP with host), Mail exchange (MX) record, and Name server (NS) records.

### DNS Caching

* Overloading root zone (network traffic) due to traversing the DNS tree path for each query.
* DNS servers cache results for a specified time, specified by ANS reply's time-to-live field.
* Some operating systems maintain DNS caches like Windows and Linux.
* Privacy issues associated with DNS queries, typically issued over UDP on port 53.
  + 16-bit request identifier in payload.

|  |  |
| --- | --- |
| **UDP** | **TCP** |
| * Smaller packet sizes (8 bytes). * No connection creation and maintenance. * More control over data sent. * Doesn't compensate for packet loss. * Doesn't guarantee orderly packet delivery. * Doesn't check network busyness. | * Packet size as 20 bytes * Reliable and connection-based. * Protects Sqn no. against loss, duplication and reordering. * Retransmissions and timeouts protect against loss. * TCP packets have a header section with a flags field. * Considers four possible fags: SYN, ACK, FIN, RST. |

### Three-Way Handshake TCP Packet Exchange

• Initiating system sends SYN packet to destination.

• Destination sends SYN-ACK acknowledging first packet receipt.

• The first system sends ACK to confirm receipt. 🡺 Data transfer begins.

#### IPV4 (class C IP address)

* 32 bits binary address / Dotted decimal
* 192.168.10.0 is the Network Address
* 192.168.10.255 is the Broadcast address
* Hosts can have any IP between 192.168.10.1 to 192.168.10.254
* Network part 🡪 1st three dots
* Host part 🡪 last three decimal numbers

**Dynamic Host Configuration Protocol (DHCP)** 🡪 simplify the configuration of each user’s computer.

**MAC Address** 🡪 48-bit number represented in Hex

**Address Resolution Protocol (ARP) 🡪**

• Connects network to the data layer by converting IP addresses to MAC.

• Broadcasts requests and caches responses.

**Network Interface**

• Network interfaces are physical devices that determine the network interface card used by the system.

• They are considered both physical and data link layer interfaces.

• Network interfaces include Ethernet cards and WiFi adapters.

• Packets are transmitted between the multiple interfaces of a computer.

• Most LANs 9Including Ethernet and Wifi) broadcast frames.

• Each network interface receives the intended frames.

• Hackers can sniff traffic by configuring the network interface to read all frames (promiscuous mode/ monitor mode).

# Week 03

## Sniffers

• Allows viewing of email passwords, web passwords, FTP credentials, email contents, and transferred files.

• In promiscuous mode, a network adapter can sniff all traffic regardless of the destination address.

• In normal mode, the adaptor drops or ignores unintended packets.

### Sniffers Threats to Protocols

• Telnet allows easy sniffing of keystrokes.

• HTTP sends information clearly without protection, which is a target for sniffing.

• SMTP(Simple Mail Transfer Protocol) is simple but doesn't include sniffing protection.

• POP (Post Office Protocol) retrieves email from servers but doesn't include sniffing protection.

• FTP sends and receives files in clear transmission.

|  |  |
| --- | --- |
| **Passive Sniffing** | **Active Sniffing** |
| * Eavesdropping or minoring the transmissions. * Learning or using system information without affecting resources. * Easy to conduct. * Detection difficult | * Sending Crafted Packets for Sensitive Data Extraction. * It involves injecting malicious code, which allows attackers to take control or steal sensitive information. |

## Application Layer Attacks

### HTTP Authentication (Passive attack)

* Simple challenge and response mechanism for a server to request a user ID and password.
* Client passes authentication information in the Authorization header.
* Insecure as full credentials are sent in the clear.

#### DNS Pharming

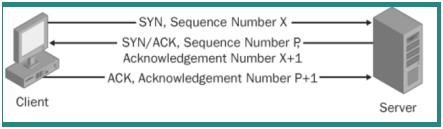
* The attacker attempts to change the IP of a server.

#### DNS Cache Poisoning Overview

* Involves redirecting attacker's domain nameserver to target domain's nameserver, assigning fake IP address.
* Second variant redirects unrelated domain nameserver to fake nameserver.
* Third variant "racing" real nameserver to give false records.
* Cache poisoning occurs when a name server
  + disregards identifiers,
  + has predictable ids,
  + accepts unsolicited DNS records.

### Session Hijacking Overview

* Builds on network sniffing.
* Aims to observe traffic and sessions and take over authenticated sessions.
* Occurs when attackers use valid sessions for unauthorised access.
* Targets authentication at the start of a session.
* Relies on understanding of message flow over the Internet.
* Attacker controls or modifies hosts' communications by positioning themselves between parties.
* Monitors packet flow using sniffing techniques.
* Analyses and predicts packet sequence.
* Severs connection between parties.
* Seizes control of the session.
* Performs packet injection into the network.



### Identifying an active session

For a successful session hijack

🡪 locate and identify a session

🡪 determine or guess the correct sequence number

🡪 Inject data into the session before the client sends its next packet

Sequence number:

* + Starting sequence number assigned randomly if the operating system completes a 3-way handshake.
  + Predictable sequence number allows an attacker to initiate a legitimate server connection and open a second connection from a forged address.

Session hijack categories:

* + Man in the middle attack
  + Blind hijack attacks
  + Session theft attacks

#### Man in the Middle Attack (MiTM)

* Attacker intercepts all communications between hosts.
* Positions themselves to manipulate client-server communications.
* Targets protocols relying on public key exchange (ARP, DNS).

#### Blind Hijack Attack

* Injects malicious commands into communications.
* The attacker can only do data injection and not see the responses.
* Despite limitations, the method remains effective.

#### Session Replay Attack

* The attacker creates new or reuses old sessions.
* Not intercepting or injecting data into existing communications.
* Common at application level, like Web applications.

**Port Scanning**

* Ping Scan: Sends a single ICMP (Internet Control Message Protocol) echo request from the source to the destination device.
  + Active devices respond with an ICMP echo reply.
* Connect Scan: Connects to target IP address and port in a complete TCP handshake.
  + Reliable but noisy.
* SYN Scan: Gathers information about open ports without completing the TCP handshake.
* FIN Scan: Sends a FIN packet to the target, indicating whether the port is listening (no response).

#### Port Knocking

* Involves attempting to connect to blocked ports in a specific order.
* Slightly vulnerable to replay attacks.
* Can be recorded and repeated for the same open port.
* Secure against brute force attacks due to 65536k combinations.
* Time-dependent knock sequence can protect against replay attacks.

## Network Layer Attacks

### IP Vulnerabilities

* Unencrypted Transmission Overview 🡪 Potential **eavesdropping** at intermediate hosts.
* No Source Authentication 🡪 Sender can **spoof source address** to reinforce tracing packets back to attackers.
* No Integrity Checking 🡪 Modifies entire packet, header, and payload.
* Enables content forgeries, redirections, and **man-in-the-middle attacks**.
* No Bandwidth Constraints 🡪 Large packets are injected to launch **DoS attacks**.

### IP Spoofing Attacks

* Intruder sends packets from one IP address to another.
* The server may inadvertently behave maliciously if it perceives it as receiving messages from the actual source.
* Two forms: Blind Spoofing and Non-Blind Spoofing.
  + Blind Spoofing: Spoofs IP address without ACK sequence pattern knowledge.
  + Non-Blind Spoofing: Spoofs IP after correct ACK sequence identification.
* Successful attacks require the spoofed IP to not exist with another network user.
* Non-Blind Spoofing
  + Attackers usually conduct Denial of Service on genuine clients, rendering them unavailable.
  + Attackers analyse network packets using packet sniffers, determine ACK sequence patterns, and spoof the IP of an actual client.

## Data Link Layer Attack

### MAC Flooding (Active sniffing attack)

* Aims to feed switch with fake MAC addresses to all ports.
* Causes overload of Content Addressable Memory (CAM), leading to switch failure.
* CAM is used to build a lookup table, tracking MAC addresses on switch ports.
* Allows lookup to ensure correct port and host traffic.

**MAC Filtering**

* Network administrator creates block or allow lists of MAC addresses.
* Used in Wireless Networks to restrict device connection.

### MAC Spoofing

* Attack impersonates another machine.
* Uses packet sniffer to identify target machine's MAC address.
* Reconfigure the rogue machine's MAC address.
* Turns off or unplugs target machine.
* Wireless Networks example: easy to spoof MAC address, making security control ineffective.

### ARP Spoofing

* Updated ARP table upon ARP response.
* Untracked requests and unauthenticated ARP announcements.
* Trust between machines.
* Rogue machines can spoof other machines.

### ARP Poisoning

* A method of bypassing a switch for sniffing on an IPv4 network.
* Involves an attacker attaching to a network with a valid IP address and spoofed MAC address from the switch ARP table.
* An active sniffing attack on IPv4 networks.
* An ARP cache updates every time it receives an ARP reply.
* The attacker first needs to prevent the client from sending new data.
* The attacker can inject data or DOS the Client.

## Denial of Service Attack

### DOS Attacks

* Commonly prevents legitimate user access to systems.
* Aims to disrupt service delivery.
* Consumes resources and may disrupt servers and services.
* Considers physical limitations of computers.
  + Factors include user number, file size, transmission speed, and stored data.
* Exploits programming defects, causing crashes.

### Distributed Denial of Service Attacks

• Aims to

* + prevent valid users from accessing network resources.
  + amplify a DoS attack by using multiple hosts.

• Uses multiple intermediary hosts to generate traffic to disrupt server farms or entire network segments.

• DDoS attacks are difficult to detect due to traffic from multiple IP addresses.

• Uses hundreds or thousands of systems with primary and secondary victims.

• Attacks can be complex to track back to source.

• Defence is complex and has a higher impact than DoS attacks.

### DoS/ DDoS Attacks:

* Ping of Death (PoD)
  + Systems struggle with handling oversized packets.
  + Attackers send fragments, victims reassemble.
  + IP protocol's maximum size limit causes system crashes.
* Teardrop Attack
  + Packets sent in the malformed state with illegal offset values overlap.
  + Victim system reconstructs message.
  + Potential crash or lock if the system is unprepared.
* Land Dos
  + Sends packet to victim's system with same source, destination, and port.
  + Unprocessed systems can crash.
* SYN Food Threat Overview
  + Uses forged packets with SYN flag set.
  + Overwhelms the system when the victim receives packets.
  + Consumes connection resources, causing no resources for legitimate connections.
* ICMP flood
  + Either Smurf attack or Ping flood
  + Smurf Attack
    - Large traffic is directed to the network broadcast address.
    - Attacker configuring packet with the intended victim as the source.
    - All hosts respond to the victim, not attack.
  + Ping Food Attack
    - Involves sending large packets to victim to overwhelm the victim.
    - Simple, targeted attack.
* Reflected Attack
  + Spoofing or forging packets or request source addresses.
  + Sending requests to multiple systems.
  + Scaled-up version of ping flood attack.
* DHCP Starvation (Dynamic Host Configuration Protocol)
  + Attackers can exhaust DHCP servers' address space for an indefinite period.
  + Tools like The Gobbler can be used for this DoS attack.
* HTTP flood
  + Bombard servers with HTTP requests
  + Slowloris: A Potent Variant
    - Monopolizes by sending non-complete HTTP requests.
    - Consumes web server's connection capacity.
    - Utilizes legitimate HTTP traffic.

## Botnets and IoT

**Botnet Overview**

* Consists of infected computers and devices.
* Infected with DDoS attack software.
* Can extend globally.

#### Botnet Attacks

* DDoS attacks: Attacks based on DDoS's functionality and infected systems.
* Click fraud: Attacks where attackers infect large systems to generate revenue.
* Stealing information: Attacks to steal information from unsuspecting users' systems.

|  |  |
| --- | --- |
| Physical | Hardware hijacking, Lock picking, Physical access attacks, wiretapping, and interception |
| Data | Sniffing (passive/active), MAC spoofing, WEP cracking |
| Network | IP attacks, routing attacks, ARP poisoning, MAC flooding, ICMP attacks (Smurf) |
| Transportation | Port scanning, DoS attacks, service enumeration, flag manipulation |
| Session | Session hijacking, SYN attacks, PW attacks |
| Presentation | NetBIOS attack, clear text attack, protocol attack |
| Application | Application attacks, buffer overflows, exploit code, malicious software (Trojans, virus, worms) |

# Week 4

## Cryptography – The Math

### Cryptography and Nonce

* Cryptography is enhanced by adding randomness.
* Nonce, a random number generator, acts as a placeholder variable in mathematical functions.
* During execution, a nonce is replaced with a random number.
* Nonce produces a unique number each time used.

### Initializations Vectors in Encryption

* Random values used in algorithms to prevent pattern creation.
* Used with keys and doesn't need encryption during destination.
* If not used, identical plaintext values with the same key create the same ciphertext.
* Provides attackers with patterns for breaking encryption methods and key discovery.

## Cryptography Overview

### Cryptography Terms

* Cryptanalysis techniques for deciphering messages without enciphering details.
* Unencrypted information: plaintext or cleartext.
* Encrypted information: scrambled ciphertext.
* Encryption: scrambling plaintext into ciphertext.
* Decryption: unscrambling ciphertext into plaintext.
* Cryptographic algorithm/cipher: a scheme.

Plain text 🡪 Encryption 🡪 Ciphertext 🡪 Decryption 🡪 Plain text

### Cryptography Overview

* Method of storing and transmitting data in an unreadable format.
* Protects sensitive information by encoding it into an unreadable format.
* Effective in protecting sensitive information stored on media or transmitted through untrusted network paths.

### Cryptography Goals

* Hide information from unauthorised individuals.
* Hackers can break algorithms and reveal encoded information.
* Realistic goal: make information acquisition too time-consuming for attackers.

### Cryptosystems

* Confidentiality
  + Types of cryptosystems
    - Symmetric key 🡪 shared key for all users
    - Asymmetric key 🡪 individual combination of private and public key for each user
  + Types of data
    - Data at rest 🡪 reside in a permanent location to access
    - Data in transit 🡪 data being transmitted across the network (2 systems)
* Integrity
  + Allows:
    - Verification of the received message to be sent
    - Ensure stored data is created and accessed time is not altered
  + Message integrity 🡪 digital signatures( encrypted message digest) created on transmission
  + Enforced by both **public and private secret keys**
* Authentication
  + Verification of the identity claimed by the system users (main function)
* Non-repudiation
  + Ensure the recipient, the sender, created the message, not someone else
  + Prevent the sender from claiming not to send messages

### Capabilities

❐ Privacy or confidentiality ❐ Certification

❐ Integrity ❐ Timestamping

❐ Entity authentication or identification ❐ Witnessing

❐ Message authentication ❐ Ownership

❐ Signature ❐ Anonymity

❐ Access control ❐ Non-repudiation

### Cryptographic Functions and Ciphers

• Each cypher has specific characteristics that determine its desirable or undesirable use.

• Evaluating a cypher involves considering its intended use, whether for data security in transit or at rest.

• Different cyphers solve different problems better than others.

• Additional decisions about key size, operational mode, etc., are made after selecting a cypher.

### Confusion and Diffusion in Cryptographic Algorithms

• Cryptographic algorithms use two basic operations: confusion and diffusion.

• Confusion occurs when the relationship between the plain text and the key is complex.

• Diffusion occurs when a change in the plain text results in multiple changes spread throughout the cypher text.

### Steganography

• Steganography is a method of hiding data in another media type, concealing its existence.

• The message is not encrypted but hidden.

• Encrypted messages draw attention and are ideal for steganographic transmission due to their large size.

### The Strength of the Cryptosystem

• The strength of an encryption method comes from the algorithm, key secrecy, key length, initialisation vectors, and how they work together within the cryptosystem.

• Breaking a cryptosystem can be accomplished by a brute force attack.

## Cryptographic Systems

* Operation to be used for transforming plain text to cipher text
  + Substitution
  + Transposition
* Keys used
  + Asymmetric
  + Symmetric
* Plain text process method
  + Block cypher
  + Caeser cypher

### Substitution Ciphers

• Replace letters of plaintext with other letters, numbers, or symbols.

• Use a key to dictate the substitution process.

• Keyword mixed alphabet cypher uses a cypher alphabet minus duplicates.

• Simple substitution cypher allows any letter to map to any other letter uniquely.

### Caesar Ciphers

• Simplest and earliest known use of a substitution cypher.

• Replace each alphabet letter with the letter standing three places further down the alphabet.

• Shift each letter to the right by a specific number in the message to generate the cypher text.

• Vigenere Cipher adopted from Caesar 🡪 multiple cypher text for each plain letter.

### Transposition Ciphers

• Use an encryption algorithm to rearrange the letters of a plain-text message.

• The decryption algorithm reverses the encryption transformation to retrieve the original message.

### Symmetric Encryptions Overview

• Uses two instances of the same key for encryption and decryption.

• Keys, or secret keys, can perform both processes.

• Each user must keep the key secret and protect it.

• Intruders can decrypt intercepted messages if the key is compromised.

• Security depends on user protection of the key.

• Symmetric cryptosystems provide confidentiality but cannot provide authentication or nonrepudiation.

#### Strengths:

• High speed of operation, often 1,000 to 10,000 times faster than asymmetric.

• Hard to break with sizeable key sizes.

#### Weaknesses:

• Requires a secure mechanism for key delivery.

• Unique keys are required for each user pair, potentially overwhelming key management.

• Provides confidentiality but not authenticity or non-repudiation.

### Asymmetric Encryptions Overview

• Asymmetric encryptions, also known as public key systems, require two keys: one public key known to everyone and the other private key only used by the owner.

• Both keys are mathematically related.

• If one key encrypts a message, the other must be decrypted.

• Each user requires two keys, one public and one private.

• For 100 people, 200 keys would be required.

• The number of asymmetric keys is calculated using the equation N ∗ 2 number of keys.

* Strengths: Better key distribution, scalability, authentication, non-repudiation.
* Weaknesses: Works slower, mathematically intensive tasks.

#### Asymmetric Encryption Functions

• Asymmetric algorithms offer authentication and non-repudiation, depending on the algorithm used.

• Asymmetric systems offer more accessible and manageable key distribution than symmetric systems.

* Authentication
  + A message can only be decrypted with a public key if encrypted with the corresponding private key.
  + Bob, the only person with his private key, provides authentication.
* Confidentiality
  + Alice encrypts the message with the receiver's public key, ensuring confidentiality.
* Non-repudiation
  + If Alice encrypts the message with her private key, only her public key can decrypt it, ensuring non-repudiation.

## Cipher Systems Overview

• Used by individuals and governments for confidentiality.

• Combines can be formidable opponents.

• Causes frustration for cryptanalysts.

#### Block Cipher:

• Encrypts a block of input to a block of output.

• Typically, two blocks are of the same length.

• Block size in most symmetric key systems is 64.

• In AES, the block size is 128.

• Different modes for encrypting plaintext longer than a block.

#### Stream Cipher:

• Treats a message as a stream of bits.

• Performs mathematical functions on each bit individually.

• Uses keystream generators to produce ciphertext.

## Hashing Algorithms Overview

• Creates message digest for digitally signed messages.

• Protects user passwords.

• Can be used with symmetric key encryption for message authentication code (MAC).

### Hash Function and Integrity

• Helps detect forgeries.

• Computes message checksum.

• Combines checksum with cryptographic function for tamperproof result.

• Hash is a checksum designed to prevent forgery.

• Hash value is usually finite, larger than checksum values.

### Common Hashing Algorithms Overview

• MD5 message digest algorithm: Generates a 128-bit message digest from any input.

• Secure Hashing Algorithm (SHA) variants: Common variants found in commercial software.

• Secure Hash Algorithm (SHA-1): Produces a 160-bit hash from any message.

• SHA256: Widely used with a digest size of 256 bits.

• Hash message authentication code (HMAC): Hash function using a key to create the hash.