**Cyber Security**

****

**Risk = Probability x Severity**

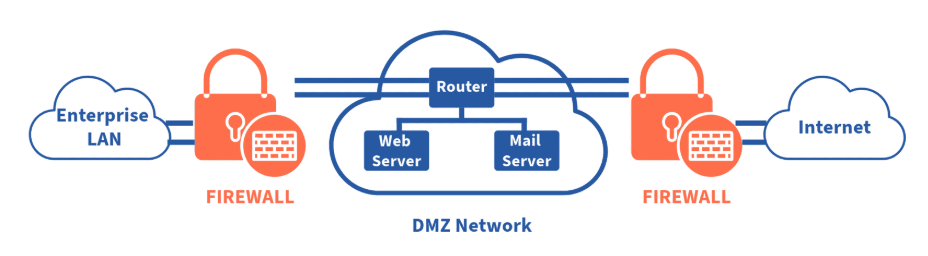
**Threats**

|  |  |
| --- | --- |
| **Cyber Threat** | Explanation |
| Malware | Malicious software designed to harm, exploit, or compromise a computer system. |
| **Social Engineering** | Manipulating people to give up confidential info or perform risky actions. |
| **Phishing** | Fraudulent messages pretending to be trusted sources to steal data. |
| **Spear Phishing** | A targeted phishing attack using personalized details to deceive the victim. |
| **SQL Injection** | Injecting malicious SQL into input fields to access or modify databases. |
| **DoS (Denial of Service)** | Overloading a system to make it unavailable to users. |
| **DDoS (Distributed DoS)** | A coordinated DoS attack from multiple sources to crash a target. |
| **Ransomware** | Encrypts data and demands payment to restore access. |
| **Zero-Day** | Exploits an unknown software flaw before it's patched. |
| **Trojan Horse** | Malware disguised as legitimate software to trick users. |
| **MITM (Man in the Middle)** | Intercepts and possibly alters communication between two parties. |
| **Brute Force Attack** | Tries many password combinations until the correct one is found. |

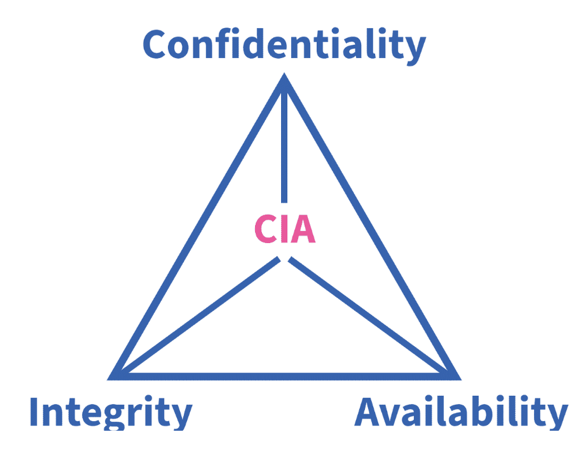
**Security Controls**

* Preventative Controls – Firewalls, Encryption, access controls
* Detective Controls – Intrusion Detection Systems (IDS), Security Info & Event Management (SIEM) & regular audits
* Corrective Controls – Incident Response plans, Patch management, Disaster recovery plans.

Demilitarised Zones for Networks



**Principles of CIA Triad model**

****

**Confidentiality:** Ensuring that information is not accessed by unauthorised individuals. (encryption, access controls, Authentication)

**Integrity:**Maintaining the accuracy and completeness of data. (Hash Functions, Check Sums, Version Control)

**Availability:** Ensuring that information is accessible to authorised users when needed, in a timely manner.

(Redundancy, Failure mechanisms, Backups)

AAA Model complements the CIA Model

* Authentication- verifies users prior to access
* Authorisation – Determines Access level/permissions
* Accounting- Tracking and logging user activities

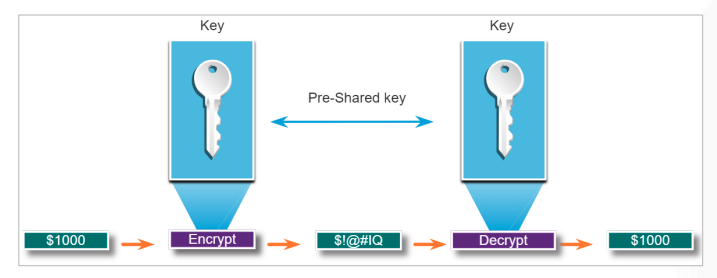
**Confidentiality**

* Access Controls: Restricting data access to authorised users
* Authentication Protocols: Verifying user identities
* Encryption: Scrambling data to protect it

**Types of Encryption:**

**Symmetric encryption**

* Symmetric algorithms use the same pre-shared key (secret key) to encrypt and decrypt data.
* Fast so are commonly used for bulk Data & VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
* When using these algorithms, the longer the key, the longer it will take for someone to discover the key.
* Most encryption keys are up to 256 bits. Use a longer key for more secure communications.
* Symmetric encryption algorithms are sometimes classified as a block cipher or a stream cipher.



**Asymmetric encryption:**

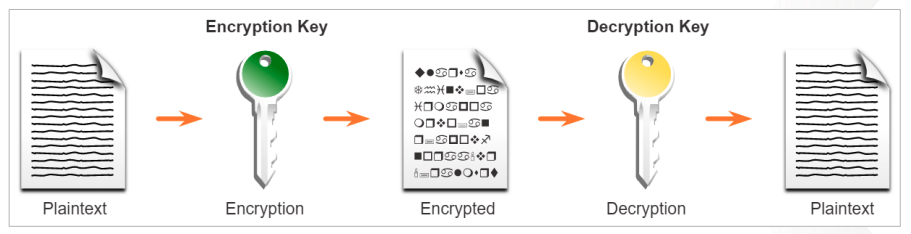
• Asymmetric algorithms, also called public-key algorithms, are designed in a way that the encryption and the decryption keys are different.

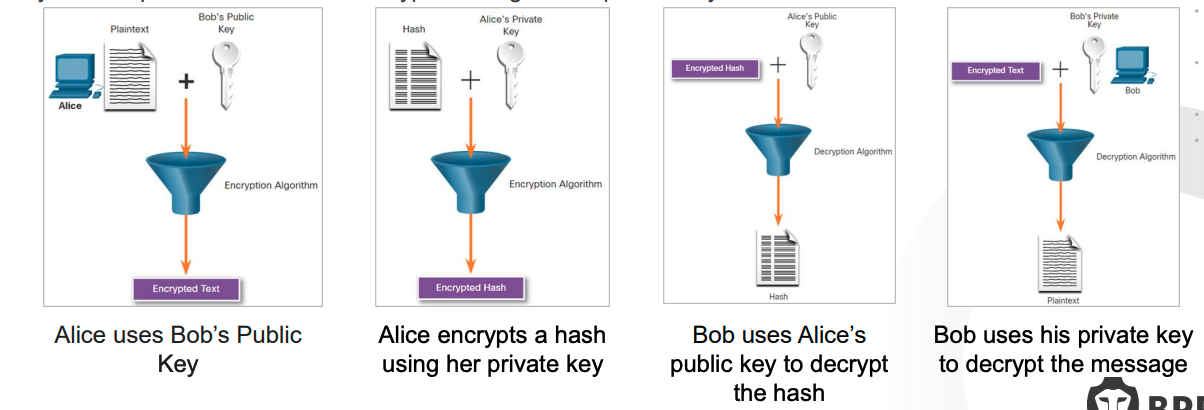
• Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for decryption.

• Asymmetric encryption can use key lengths up to 4,096 bits.

• Asymmetric algorithms are substantially slower than symmetric algorithms.

* Common For fast data transmissions such as HTTPS & Bank Data





**Hash Functions:**

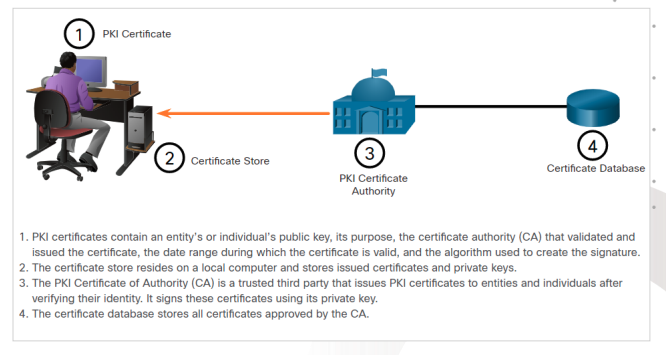
* A hash function takes input data and produces a fixed-size string (hash value).
* It’s one-way: you can’t reverse the hash to get the original data.
* Used in password storage, digital signatures and data integrity
* Common hash functions: \*\*SHA-256\*\*, \*\*SHA-1\*\*, \*\*MD5\*\*.
* Main properties:
  + Deterministic - same input → same hash
  + Fast to compute
  + Irreversible: hard to reverse-engineer the input
  + hard to find two inputs with the same hash

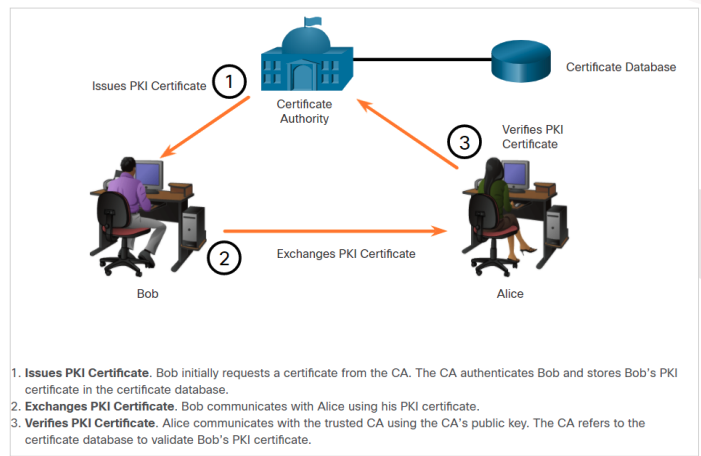
**The public key infrastructure**

• PKI is needed to support large-scale distribution and identification of public encryption keys.

• The PKI framework facilitates a highly scalable trust relationship.

• It consists of the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.





**Integrity**

**Hash Functions:**

* A hash function takes input data and produces a fixed-size string (hash value).
* It’s one-way: you can’t reverse the hash to get the original data.
* Used in password storage, digital signatures and data integrity
* Common hash functions: \*\*SHA-256\*\*, \*\*SHA-1\*\*, \*\*MD5\*\*.
* Main properties:
  + Deterministic - same input → same hash
  + Fast to compute
  + Irreversible: hard to reverse-engineer the input
  + hard to find two inputs with the same hash

**Checksums:**

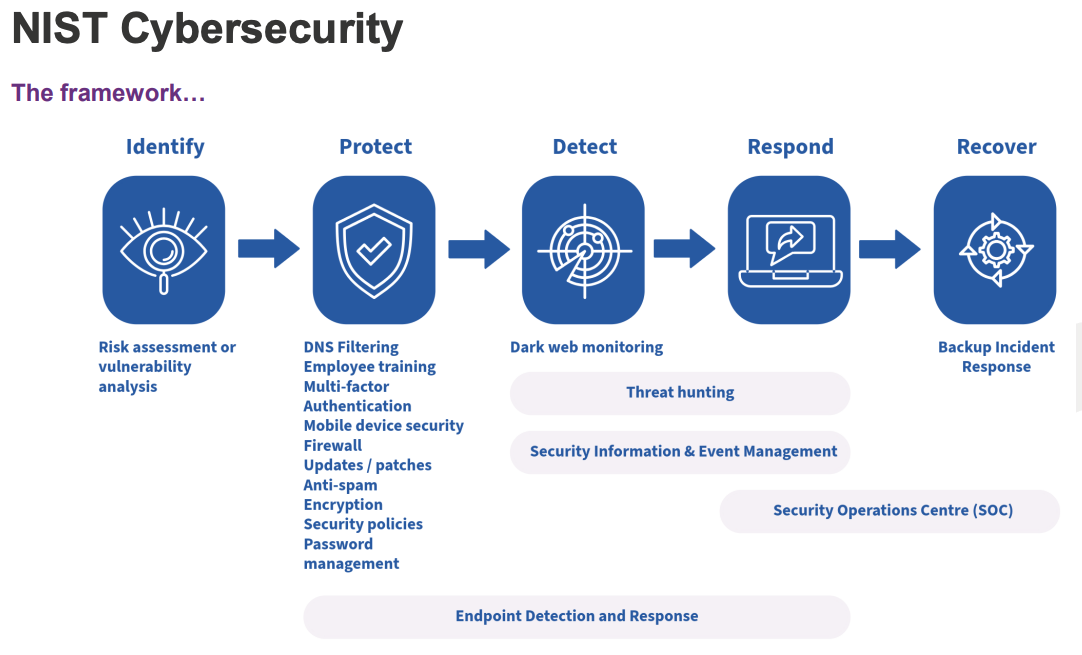
* Used to detect errorsin files or data transmission.
* Hash acts like a fingerprintof the data.
* Process:
* When data is sent or stored, a hash is calculated and stored or transmitted with it.
* Later, the hash is recomputed to check if the data has changed.
* Examples: CRC32 (simple checksum), MD5 (common in file verification)

**Availability**

* **Data Backups & Replications**
  + **Backups** - copies of data saved regularly so it can be restored if lost.
  + **Replication**-keeping **real-time or near-real-time copies** of data in different locations or systems.
* **Failover Solutions** 
  + automatically switching to a backup system or server if the main one fails, minimizing downtime.
* **Clustering-**
  + A group of servers that work together. If one server fails, another takes over.
* **Plan for Failure**
  + A disaster recovery plan helps teams respond quickly to problems, reducing recovery time.
* **Geographic Redundancy.**
  + Data and systems are duplicated in **different physical locations** so that a local disaster (like fire or flood) won’t stop service.
* **Network Load Balancing**
  + Distributes incoming traffic across multiple servers to **prevent overload** and keep the system responsive.

**NIST Cybersecurity**

The NIST Cybersecurity Framework is a comprehensive set of guidelines and best practices for organisations to manage and mitigate cybersecurity risks.

****