**PROSIT – 4**

**KEYWORDS** A

* SELinux - Security-Enhanced Linux (SELinux) is a security architecture for Linux® systems that allows administrators to have more control over who can access the system.
* Bitlocker - BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices.
* Windows environment - The Windows environment is the onscreen work area provided by Windows, analogous to a physical desktop, and the operating system's core extension points.
* Linux servers - A Linux server is a server built on the Linux open-source operating system. It offers businesses a low-cost option for delivering content, apps and services to their clients. Since Linux is open-source, users also benefit from a strong community of resources and advocates.
* WSUS - Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates.
* Cloud Security - Cloud security refers to the cybersecurity policies, best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments.
* Encrypted - convert (information or data) into a code, especially to prevent unauthorized access.
* *Access Management* - Businesses use access management solutions to authenticate, authorize, and audit access to applications and IT systems. Often delivered as a component of an identity and access management (IAM) solution, access management solutions help strengthen security and reduce risk by tightly controlling access to on-premises and cloud-based applications, services, and IT infrastructure.
* *Monitoring policies* - Policy monitoring is a process by which stakeholders follow and assess policies to ensure they are developed, endorsed, enacted, and implemented as intended.
* Ransomware - a type of malicious software designed to block access to a computer system until a sum of money is paid.
* DDoS - A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
* Phishing - the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
* Advanced Security – the Software feature which enables Customer to identify security vulnerabilities through customizable and automated semantic code analysis.

**CONTEXT** A

Lucas reinforce the company security by setting up environments, managements access and policies ensuring its updated to known threats and vulnerabilities, also implements employee training to enhance awareness and support secure practices.

**PROBLEM STATEMENT** A

How can TechNova enhance security across diverse systems and cloud environments while mitigating human vulnerabilities and evolving cyber threats?

**ACTION PLAN** A

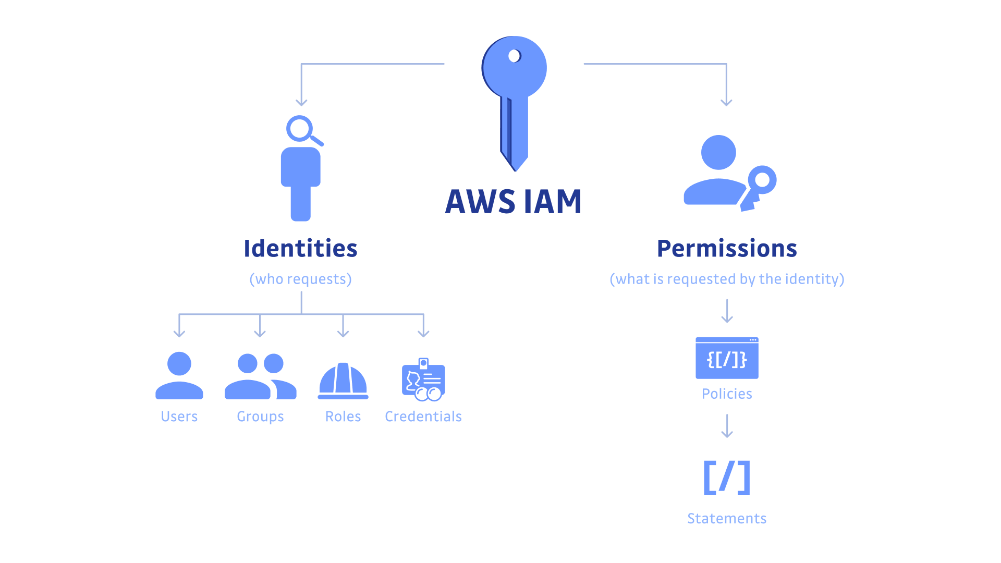
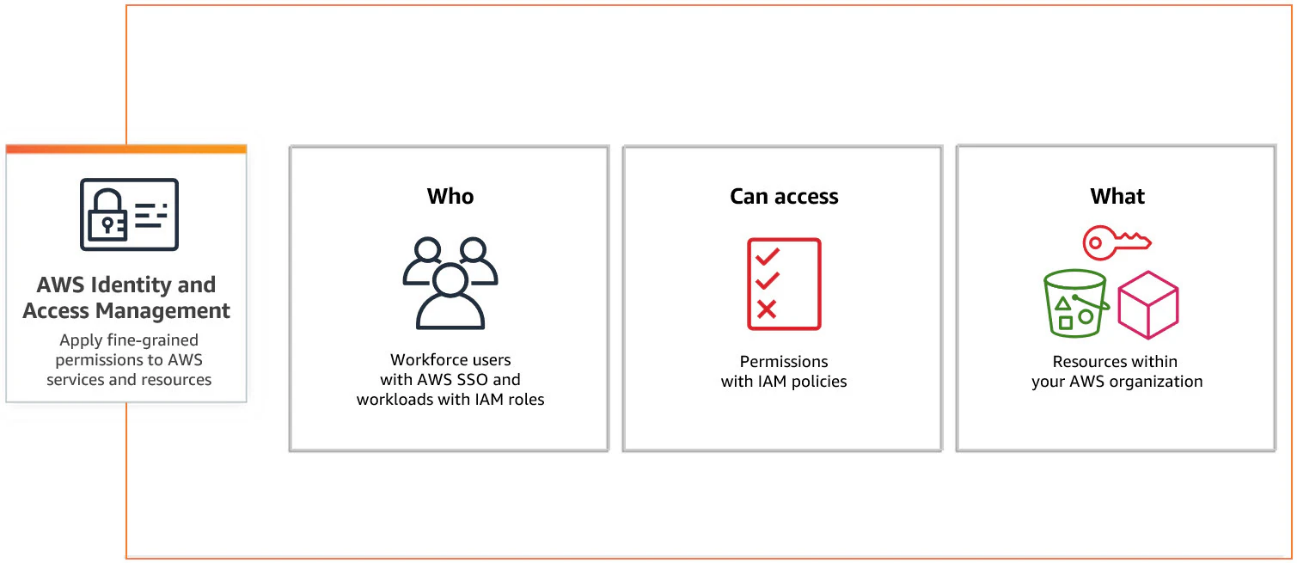
1. Look at resources on security measures
2. Study the most common attacks and learn mitigation
3. How to secure OSes (Linux, Windows)
4. Cloud and network security
5. **Access management and control (IAM)**
6. **GPOs**
7. Authentication services and authorization models
8. **Encryption (types, methods Certificates signatures)**

**IAM** A

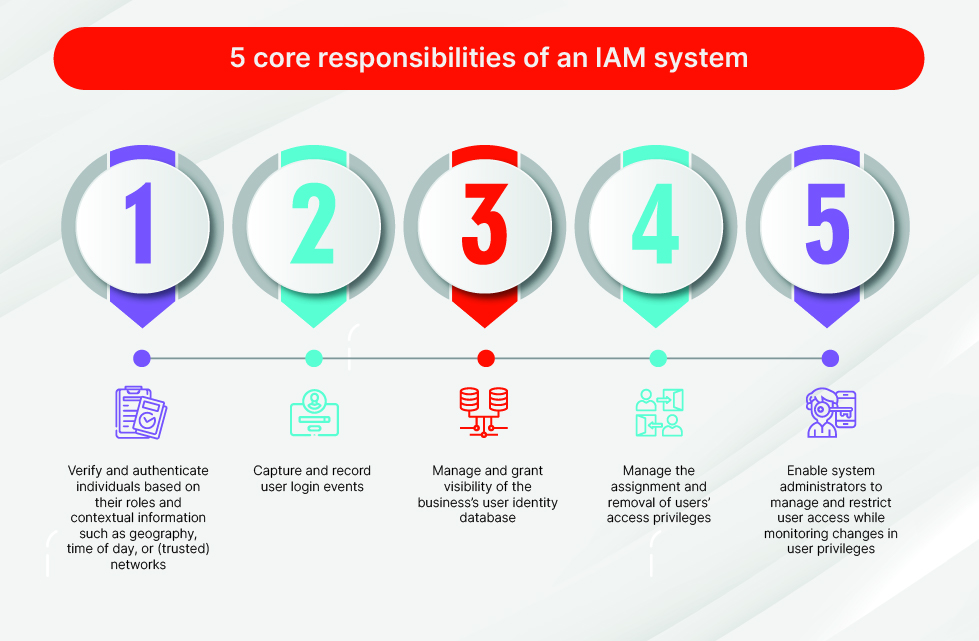
* Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities.
* With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations.
* Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management.
* These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.
* IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.

Components of IAM:

* how individuals are identified in a system (understand the difference between identity management and authentication);
* how roles are identified in a system and how they are assigned to individuals;
* adding, removing and updating individuals and their roles in a system;
* assigning levels of access to individuals or groups of individuals; and
* protecting the sensitive data within the system and securing the system itself.



Responsibilities of IAM:



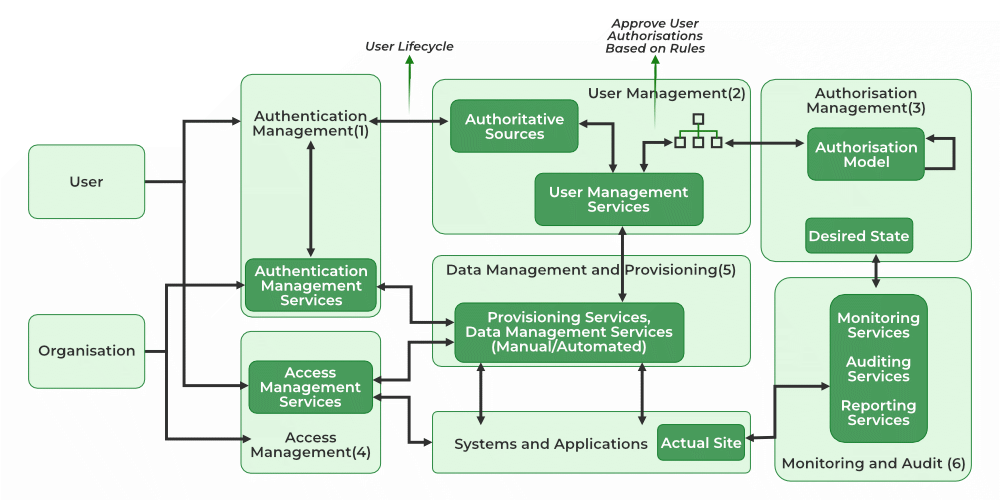
Benefits of IAM:

* Access privileges are granted according to policy, and all individuals and services are properly authenticated, authorized and audited.
* Companies that properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.
* Automating IAM systems allows businesses to operate more efficiently by decreasing the effort, time and money that would be required to manually manage access to their networks.
* In terms of security, the use of an IAM framework can make it easier to enforce policies around user authentication, validation and privileges, and address issues regarding privilege creep.
* IAM systems help companies better comply with government regulations by allowing them to show corporate information is not being misused. Companies can also demonstrate that any data needed for auditing can be made available on demand.

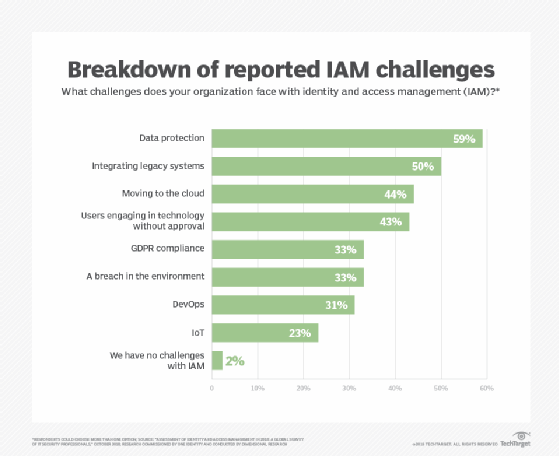
Types of digital authentication:

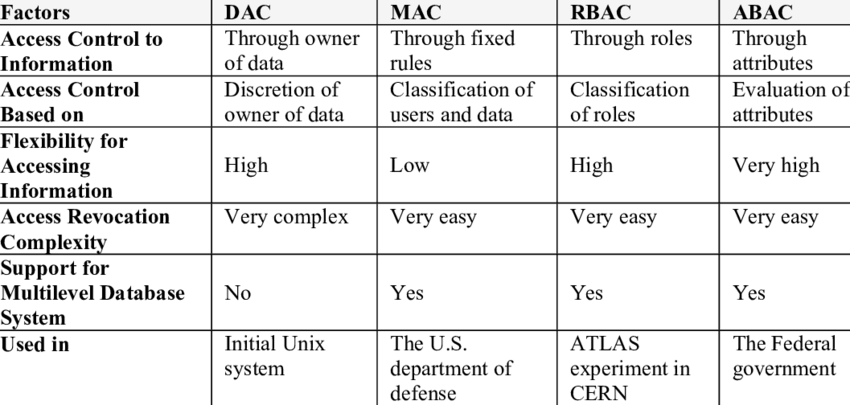
* Unique passwords
* Pre-shared key (PSK) -> less secure than individual passwords
* Behavioural authentication - When dealing with highly sensitive information and systems, organizations can use behavioural authentication to get far more granular and analyze keystroke dynamics or mouse-use characteristics.
* Biometrics
  + data security (accessing, using and storing biometric data);
  + transparency (implementing easy-to-understand disclosures);
  + optionality (providing customers a choice to opt in or out); and
  + biometric data privacy (understanding what constitutes private data and having rules around sharing with partners.

Framework of IAM



Challenges of IAM





**GPOs** A

What is Group Policy?

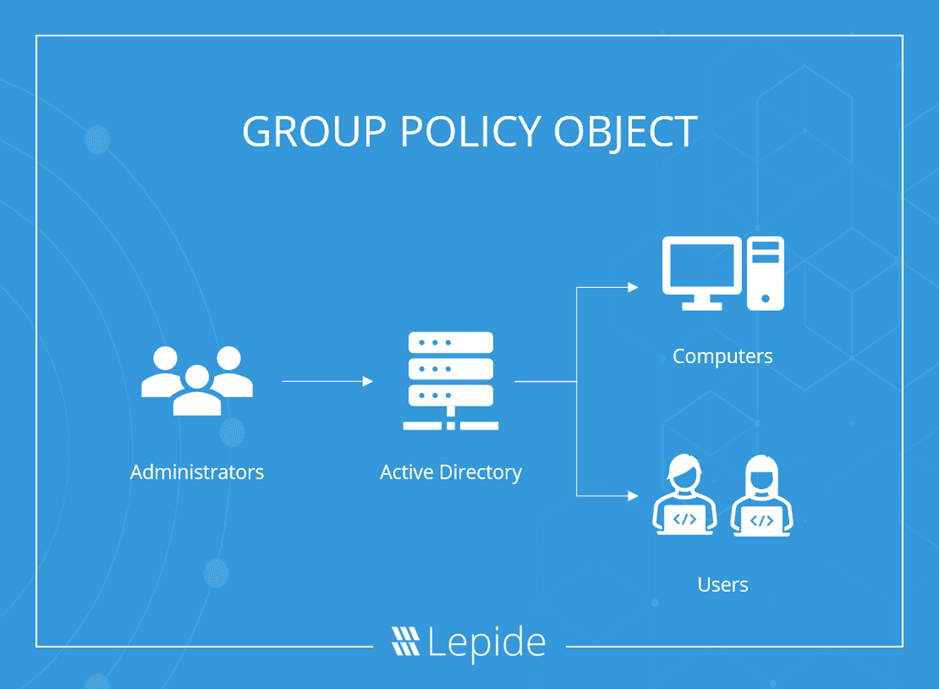
* Group Policy is a powerful feature in Microsoft Windows operating systems that allows administrators to manage and enforce system settings and configurations for a group of computers within an Active Directory environment.
* It serves as a centralized method for controlling various aspects of the operating system, applications, and user settings across a network.
* By defining policies in a hierarchical structure, administrators can ensure consistency and uniformity in the computing environment, simplifying the management of multiple systems.

✒️Note✒️

Group Policy is a fundamental tool for system administrators managing large-scale networks, providing a robust mechanism for maintaining control, security, and consistency across diverse computing environments.

What is GPO?

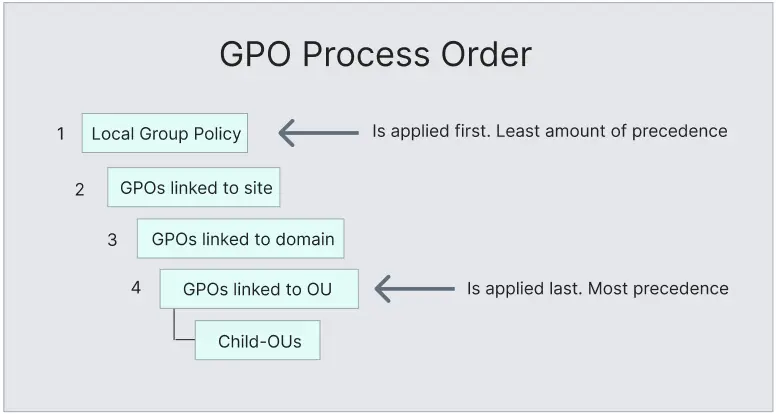
* A Group Policy Object (GPO) is a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor.
* GPOs can be associated with single or numerous Active Directory containers, including sites, domains, or organizational units (OUs).
* The MMC allows users to create GPOs that define registry-based policies, security options, software installation, etc.
* Active Directory applies GPOs in the same, logical order; local policies, site policies, domain policies and OU policies.



Examples of GPO:

* A Group Policy Object could be used to determine the home page that a user sees when they launch their internet browser after logging onto the domain.
* Administrators can use GPOs to define which network-connected printers appear on the list of available printers after a user in a specific Active Directory OU log onto the domain.
* Admins can also use GPOs to tweak several security protocols and practices, such as restricting internet connection options, programs, and even screen time.

How are GPO processed?

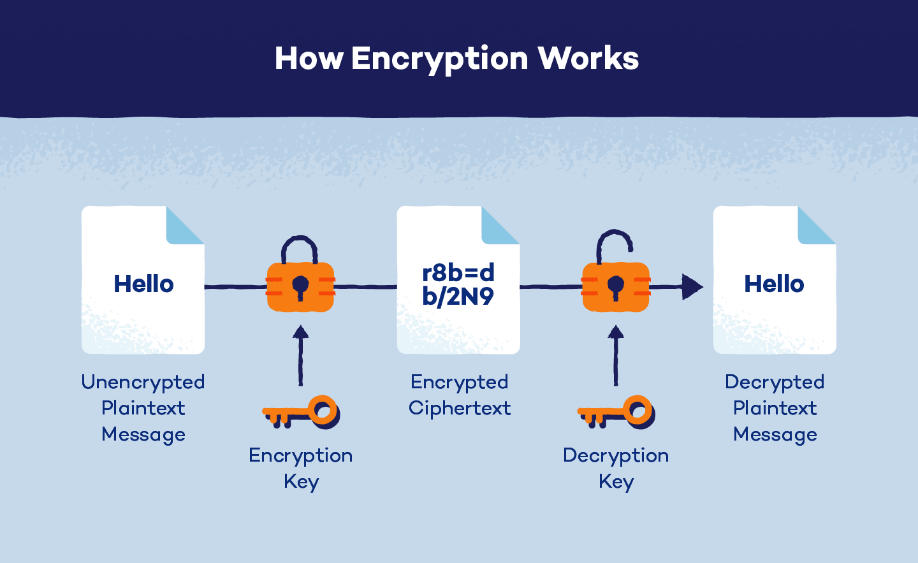


* The order that GPOs are processed is known as LSDOU, which stands for local, site, domain, and organizational unit.
* The local computer policy is the first to be processed, followed by the site level to domain AD policies, then finally into organization units.
* If there happen to be conflicting policies in LSDOU, the last applied policies win out.

**ENCRYPTION** A

* At its most basic level, encryption is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it.
* That process can range from very simple to very complex.

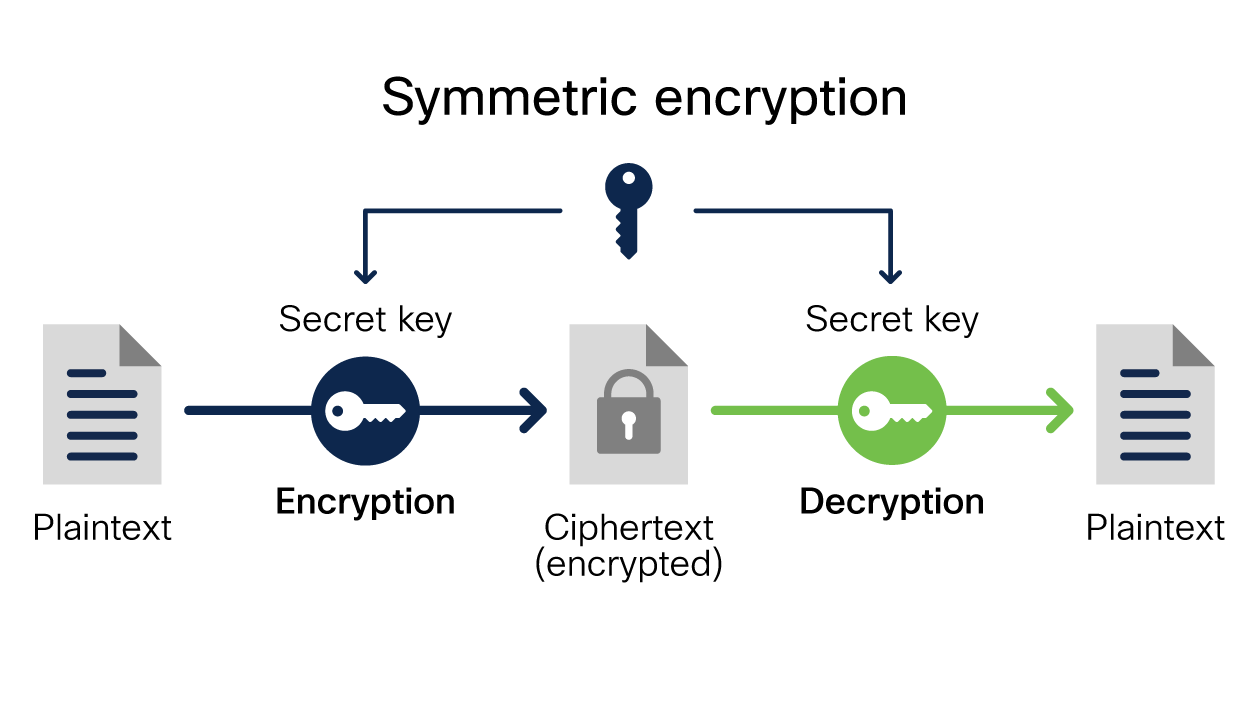
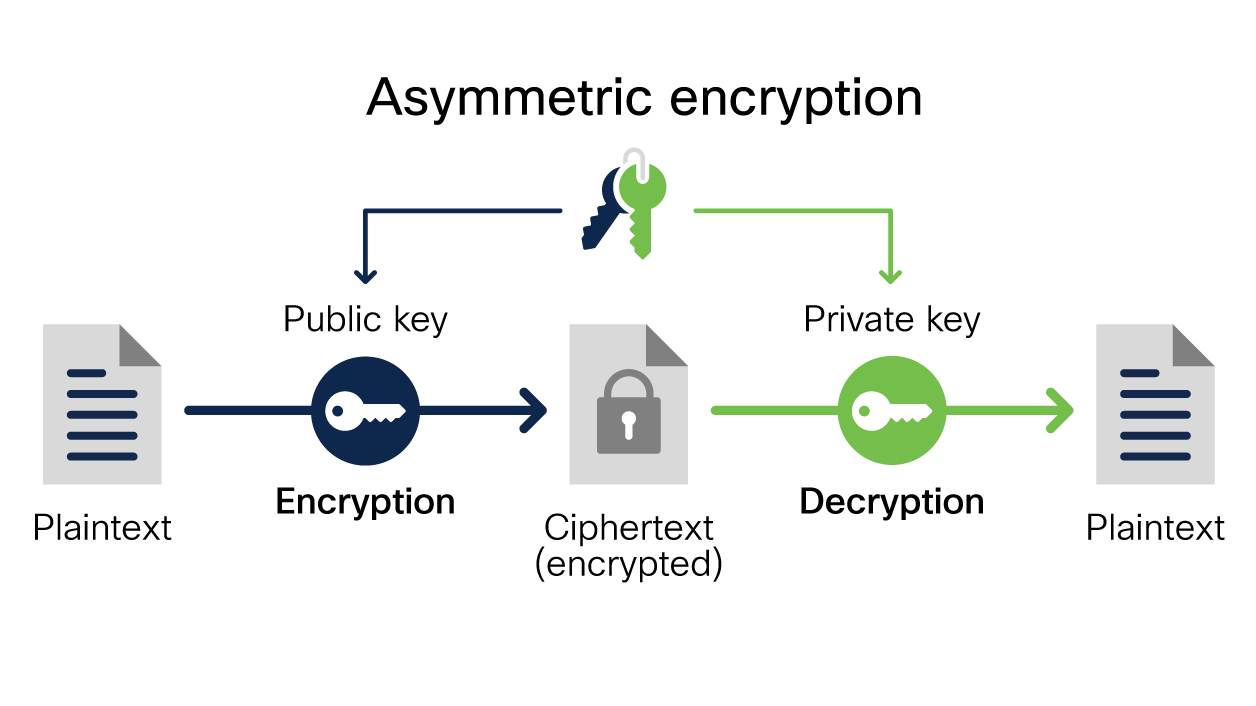
How encryption works?



* Encryption works by encoding “plaintext” into “ciphertext,” through the use of algorithms.
* To decode the data back to plaintext requires the use of a decryption key, a string of numbers or a password also created by an algorithm.
* Secure encryption methods have such a large number of cryptographic keys that an unauthorized person can neither guess which one is correct, nor use a computer to easily calculate the correct string of characters by trying every potential combination (brute force attack).

Types of encryptions

* **Symmetric encryption** uses the same key for encryption and decryption. Because it uses the same key, symmetric encryption can be more cost effective for the security it provides. It is important to invest more in securely storing data when using symmetric encryption.

* **Asymmetric encryption** uses two separate keys: a public key and a private key. Often a public key is used to encrypt the data while a private key is required to decrypt the data. The private key is only given to users with authorized access. As a result, asymmetric encryption can be more effective, but it is also more costly.

Types of data encryption

|  |  |
| --- | --- |
| Triple DES | * 3DES is a version of the original DES encryption algorithm that encrypts data three times. * It uses three 64-bit keys, so the key length is 192 bits. * It is a symmetric encryption, and the key is private. * Because it encrypts data in 64-bit segments, Triple DES is considered a block cipher. |
| Blowfish | * Blowfish is a symmetric block cipher. * It does variable-length key encryption. * It encrypts segments ranging from 32 to 448 bits. * It is an unpatented and unlicensed encryption technique. For this reason, it is free and available for public use. |
| RSA | * The RSA encryption key, named after creators Ron Rivest, Adi Shamir, and Leonard Adelman, is the standard encryption technique for important data security. * It is asymmetric cryptography, so there is one public key and one private key. * The RSA algorithm uses prime factorization. Simply put, this key requires the factorization of a product involving two large prime numbers. While it seems easy, figuring out these two numbers can be difficult. Even for large computers, it can be expensive and exhaustive to decrypt. While RSA can be very useful, it becomes increasingly inefficient at higher security levels. |
| AES | * AES is a symmetric block cipher that was originally named Rijndael. * This block cipher uses three separate keys: AES-128, AES-192, and AES-256. * These three keys are used to encrypt and decrypt information of 128 bits. Since its adoption, AES has been used to protect classified government information and sensitive data. |
| ECC | * Elliptic Curve Cryptography (ECC) is a very advanced approach. * Often based on a common public key algorithm, ECC combines elliptic curves and number theory to encrypt data. * These elliptic curves are within finite fields and are symmetrical over the x-axis of a graph. * Given these properties, cryptographers can provide robust security with much smaller and efficient keys. * For example, an RSA key of 15,360 bits would be equivalent to an ECC key of just 512 bits. |

Functions of encryption

* Confidentiality: keeps the contents of the data secret
* Integrity: verifies the origin of the message or data
* Authentication: validates that the content of the message or data has not been altered since it was sent
* Nonrepudiation: prevents the sender of the data or message from denying they were the origin

Advantages of encryption

* Protects data across devices
* Ensures data integrity
* Protects digital transformations - encryption plays a key role in protecting that data while it is in-transit to the cloud, once it is at rest on the server, and while it’s being processed by workloads.
* Helps meet compliance requirements

Disadvantages

* Ransomware - malicious actors can sometimes use it to hold data hostage. If an organization is breached and its data accessed, the actors can encrypt it and hold it ransom until the organization pays to have it released.
* Key management
* Quantum computing - quantum computing has the potential to break existing encryption. In the future, all organizations will have to adapt encryption techniques by using quantum encryption techniques.

Three stages during which data can be encrypted:

* Encryption at rest
* Encryption in transit
* Encryption in use

Difference between hashing and encryption

|  |  |
| --- | --- |
| **HASHING** | **ENCRYPTION** |
| Hashing is a one-way function to convert information to a shorter fixed value known as the key. | Encryption is a two-way function that transforms plaintext into ciphertext and then uses a key to decode the ciphertext into plaintext. |
| The main objective of hashing is to audit data: indexing and retrieving items from the database. | The main objective of encryption is to transmit data over networks securely. |
| Hashed data is of fixed length and does not grow parallel to the increase in information length. | Encrypted data is not of a fixed length. It grows in parallel with increased information length. |
| Example: MD5, SHA256 | Example: RSA, AES and DES |

Certificate-based encryption

* Certificate-based encryption is a system in which a certificate authority uses ID-based cryptography to produce a certificate.
* This system gives the users both implicit and explicit certification, the certificate can be used as a conventional certificate (for signatures, etc.), but also implicitly for the purpose of encryption.

Difference between encryption and signing

|  |  |
| --- | --- |
| **ENCRYPTION** | **SIGNING** |
| used for encoding sensitive information sent in an email or document. | used for verifying the identity of the source of the information sent over the Internet. |
| There are two encryption methods: asymmetric and symmetric. Asymmetric encryption uses public-private key infrastructure. | Signing uses the hashing algorithm to generate a hash digest that utilizes the public-private keys for sender authentication. |
| Here, the sender uses the public key to encrypt the data while forwarding it to the recipient who uses the private key to decrypt the same. | Here, the sender uses the private key while the public key is used by the receiver to verify the sender’s authenticity. |
| enforced by a digital security certificate such as SSL/TLS for sender data verification. | enforced by a digital signature which is stored in a code signing certificate for sender identity verification. |

Why should we use digital signatures?

* Digital signatures in the form of code signing certificates are used primarily for identifying and authenticating the individuals or publishers of the message or file.
* Digital signatures can also help you to safeguard your data from serious threats and vulnerabilities too.
* Often encryption and digital signing are used together to protect the data or file from getting compromised while authenticating the sender at the same time. This is because of the need to meet the legal security standards set by GDPR, FIPS, HIPAA, CA/B, and others.
* The use of digital code signing certificates and encryption together helps keep the integrity, confidentiality, and authenticity of sensitive data.