Unit-11 Computer Security

Prashant Gautam

M.Sc. CSIT

Content

- Introduction;
- Security Threat and Security Attack;
- Malicious Software;
- Security Services;
- Security Mechanisms (Cryptography, Digital Signature, Firewall, Users Identification and Authentication, Intrusion Detection Systems);
- Security Awareness; Security Policy

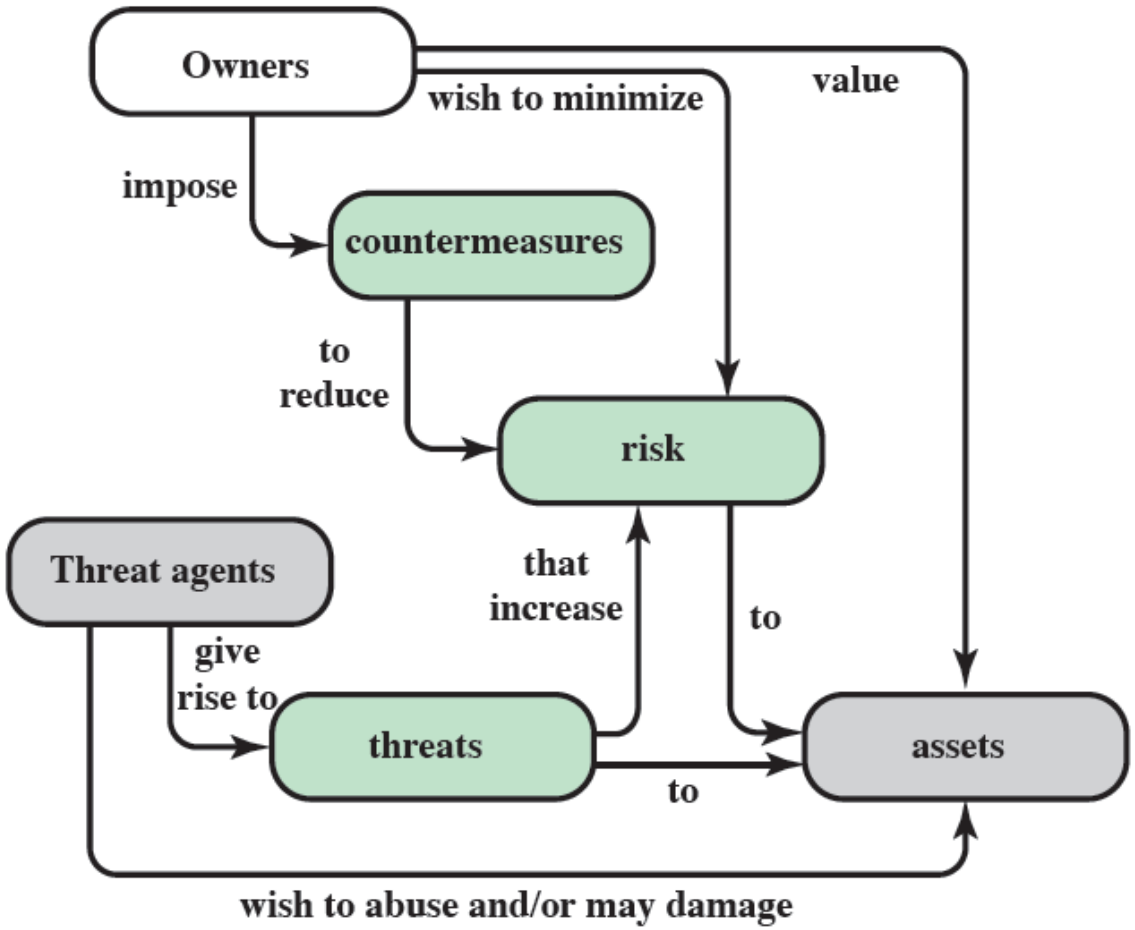
Computer Security

- Computer security is the practice of protecting computer systems, networks, and data from unauthorized access, theft, damage, or other malicious activities.
- It involves the use of various security measures such as passwords, encryption, firewalls, antivirus software, and intrusion detection systems to prevent unauthorized access, identify and respond to security incidents, and ensure the confidentiality, integrity, and availability of computer systems and data.

Three key objectives (the CIA triad)

- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **Integrity**
  - **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner
- **Availability**: assure that systems works promptly and service is not denied to authorized users

Terminologies



Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

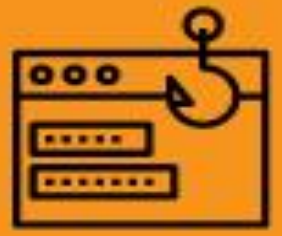
Security Threat/Attack

- A cybersecurity threat is a **malicious** and **deliberate attack** by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

Types of Cybersecurity Threats

Malware

Phishing



Spear Phishing

Man in the Middle Attack

Denial of Service Attack

SQL Injection

Zero-day Exploit

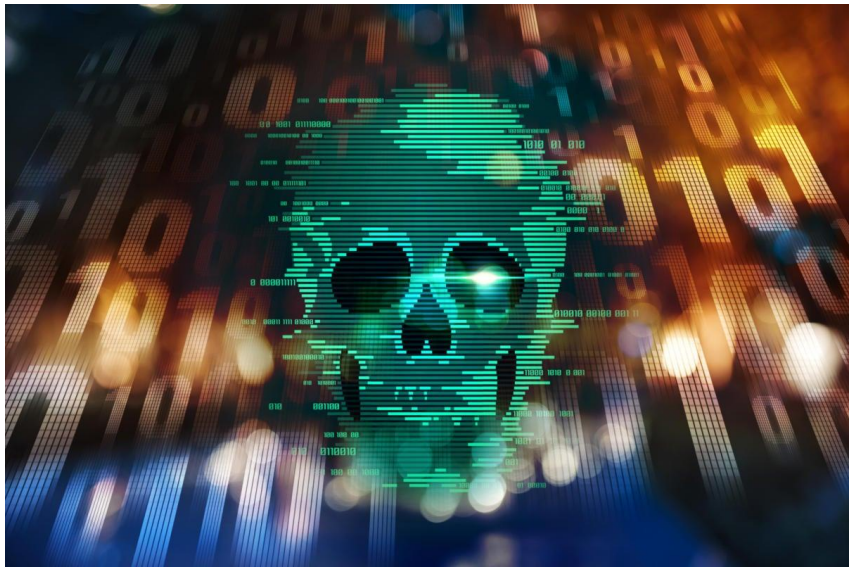
Advanced Persistent Threats

Ransomware

DNS Attack

1) Malware

- Malware attacks are the most common cyber security threats.
- Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email.
- Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.



Malicious Software/Malware

2) Phishing

- Cybercriminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials

3) Spear Phishing

- Spear phishing is a more sophisticated form of a phishing attack in which cybercriminals target only privileged users such as system administrators and C-suite executives.

4) Man in the Middle Attack

- Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication. Once the attacker interprets the communication, they may filter and steal sensitive data and return different responses to the user.

5) Denial of Service Attack

- Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.

6) SQL Injection

- A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.

7) Zero-day Exploit

- A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploit the vulnerability before a patch or solution is implemented.

8) Advanced Persistent Threats (APT)

- An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

9) Ransomware

- Ransomware is a type of malware attack in which the attacker locks or encrypts the victim’s data and threatens to publish or block access to data unless a ransom is paid. Learning more about ransomware threats can help companies prevent and cope with them better.

10) DNS Attack

- A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems (DNS Tunneling).

Security Awareness

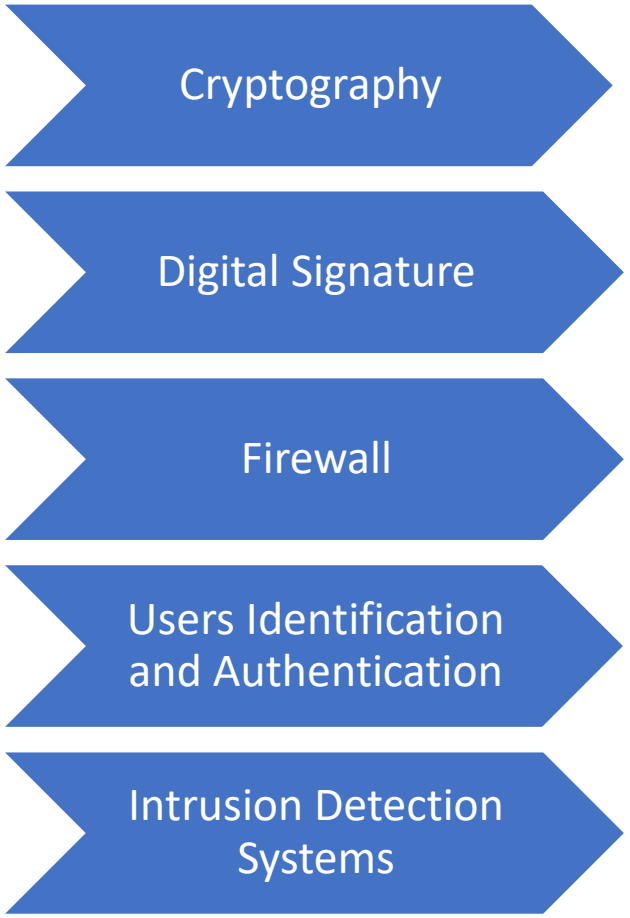
TOP TIPS

- Use significantly different passwords for each service you have
- Change passwords every 90 days for all services
- Ensure your passwords are a minimum of 8 characters, using lower-case letters, uppercase letters, numbers and special characters
- The password chosen must not include any usernames or easy to guess phrases e.g. "password"
- Having difficulty remembering lots of different passwords? Try a password manager
- Use multi-Factor authentication to give further security to your online accounts

Computer/Cyber Security awareness

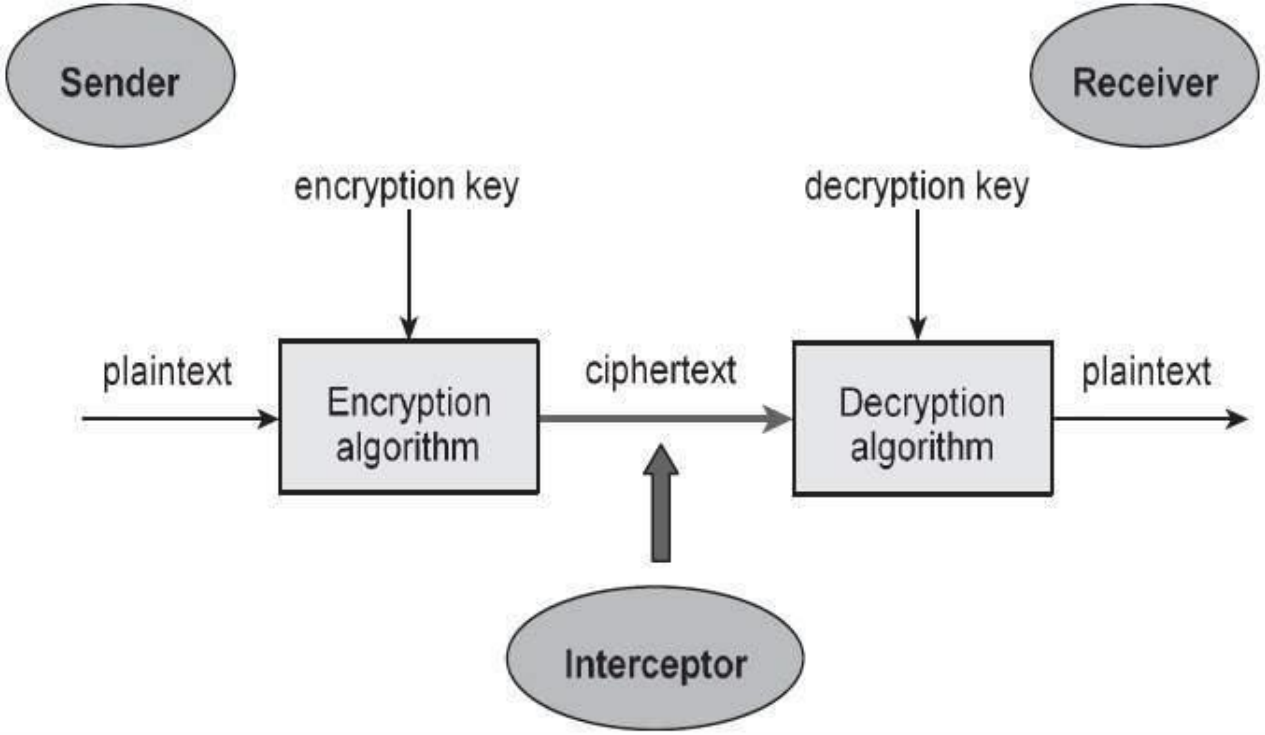
- Use strong passwords
- Keep software updated
- Don't click on suspicious links
- Use anti-virus software
- Secure your Wi-Fi network
- Be cautious when using public Wi-Fi
- Back up your data
- Be careful with personal information
- Monitor financial accounts
- Use two-factor authentication.

SECURITY MECHANISMS



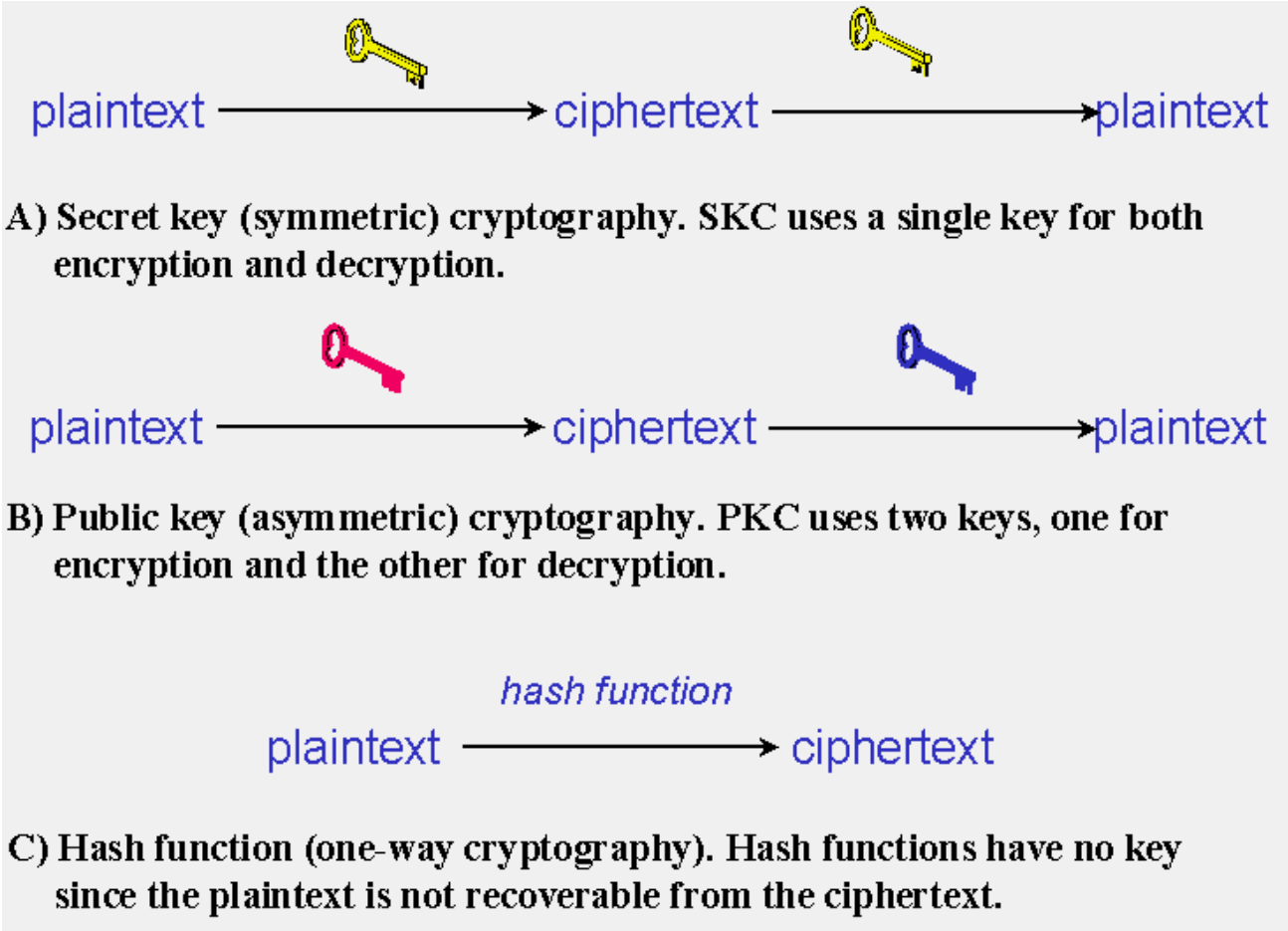
Cryptography

- Cryptography is the science of writing information in a “hidden” or “secret” form and is an ancient art.
- Cryptography is necessary when communicating data over any network, particularly the Internet.
- It protects the data in transit and also the data stored on the disk.

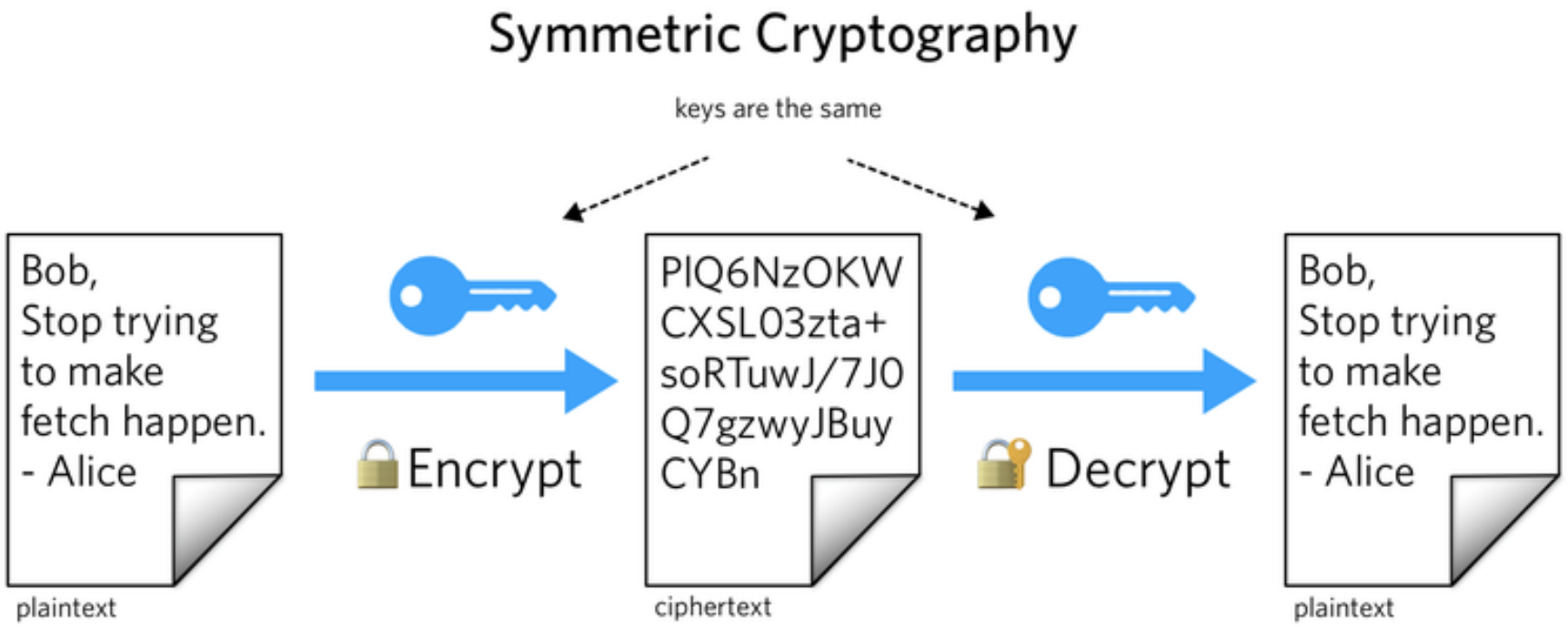


Types

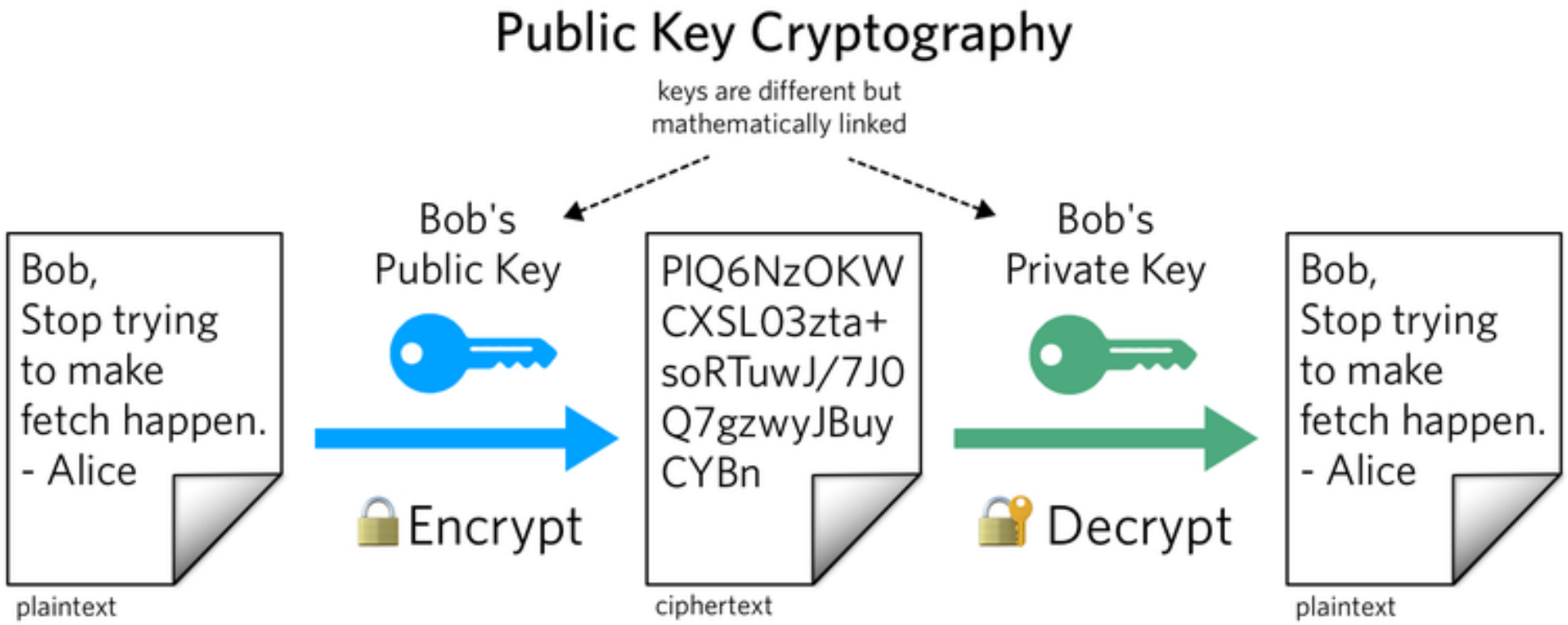
- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption,
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption,
- Hash Functions: Uses a mathematical transformation to irreversibly encrypt information.



Secret Key Cryptography (SKC)

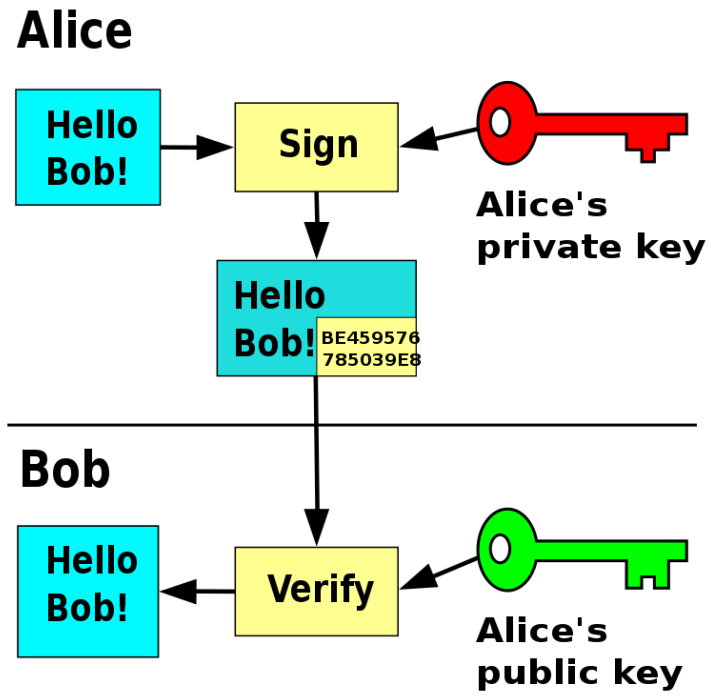


Public Key Cryptography (PKC)

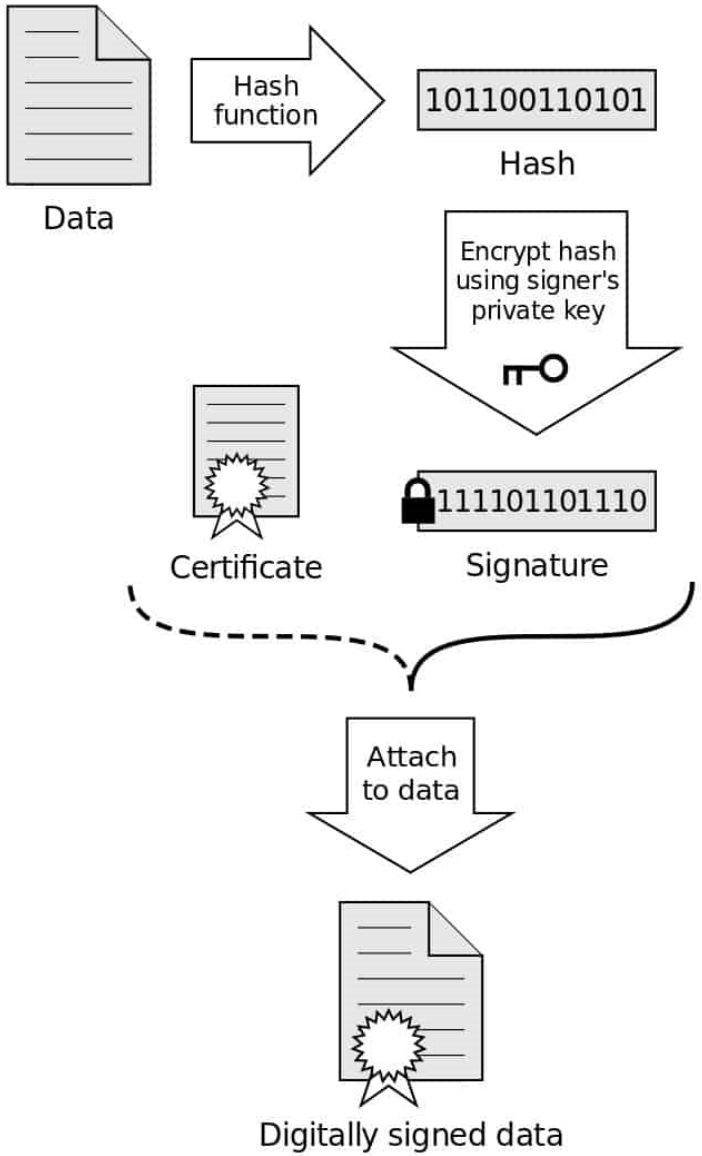


Digital Signature

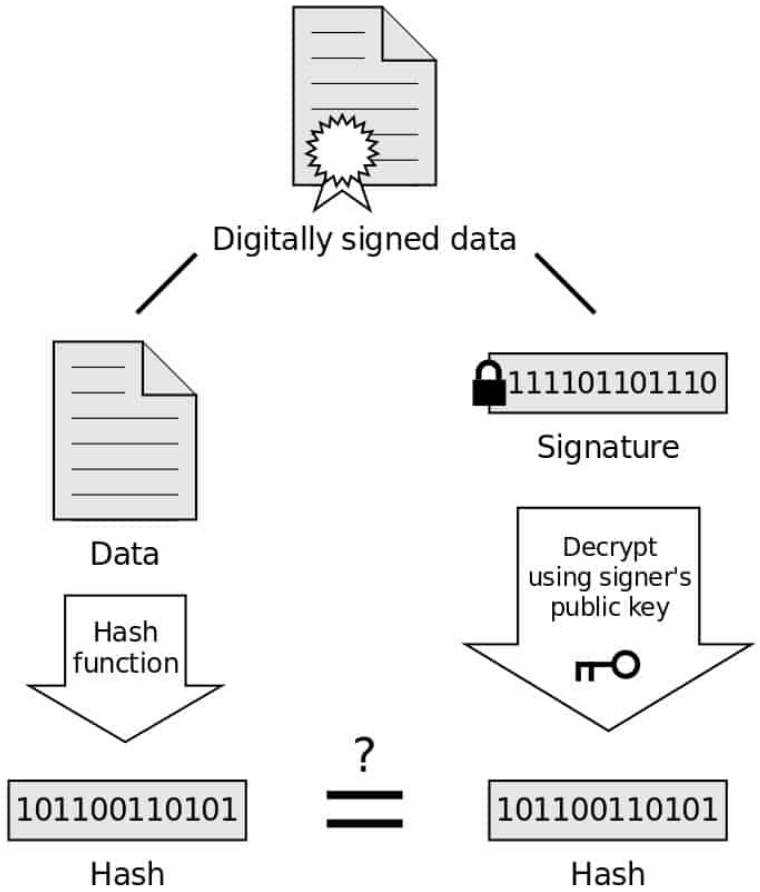
- A digital signature is **a mathematical technique used to validate the authenticity and integrity of a digital document, message or software**.



Signing

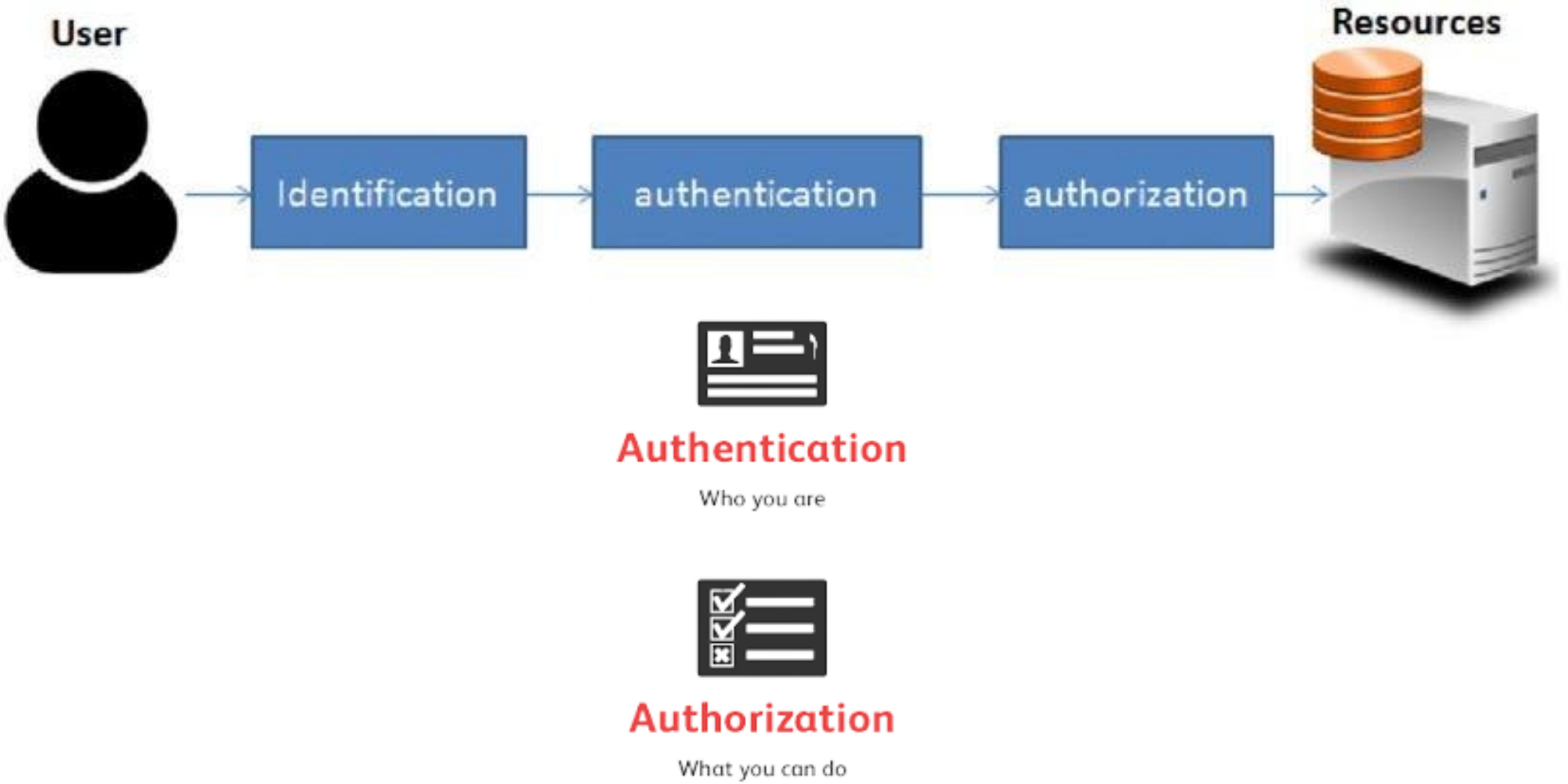


Verification



If the hashes are equal, the signature is valid.

Identification, Authentication and Authorization



1. Identification

- *Identification* is the ability to identify a user of a system uniquely or an application that is running in the system.
- This can be accomplished with a username, a process ID, or anything else that can uniquely identify a subject.
- Security systems use this identity when determining if a subject can access an object.

2. Authentication

- *Authentication* is the ability to prove that a user or application is genuinely who that person or what that application claims to be.
- For example, consider a user who logs on to a system by entering a user ID and password. The system uses the user ID to identify the user. The system authenticates the user at the time of login by checking that the supplied password is correct.

There are 3 main methods of authentication.

✓*Something you know (Knowledge factor)* - such as a password or PIN

✓*Something you have (Ownership factor)* - such as an identity card, smart card, or security token

✓*Something you are (Inherence factors)* - using biometrics

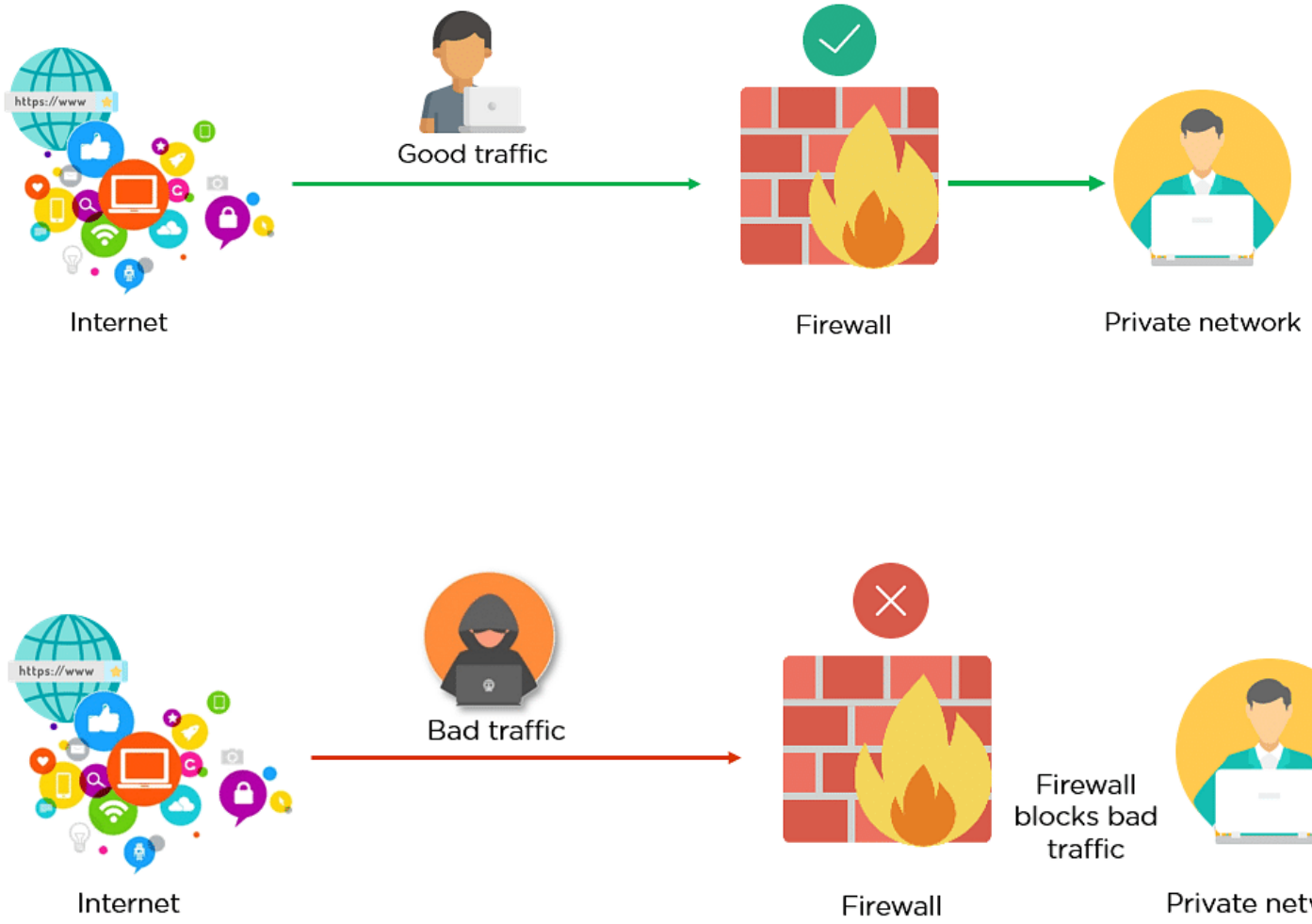
3. Authorization

Authorization is the allocation or delegation of permissions to a particular individual or type of user.

Authorization carries out the rest of an organization's identity and access management processes once the user has been authenticated. Users are granted authorizations according to their role at an organization.

Firewall

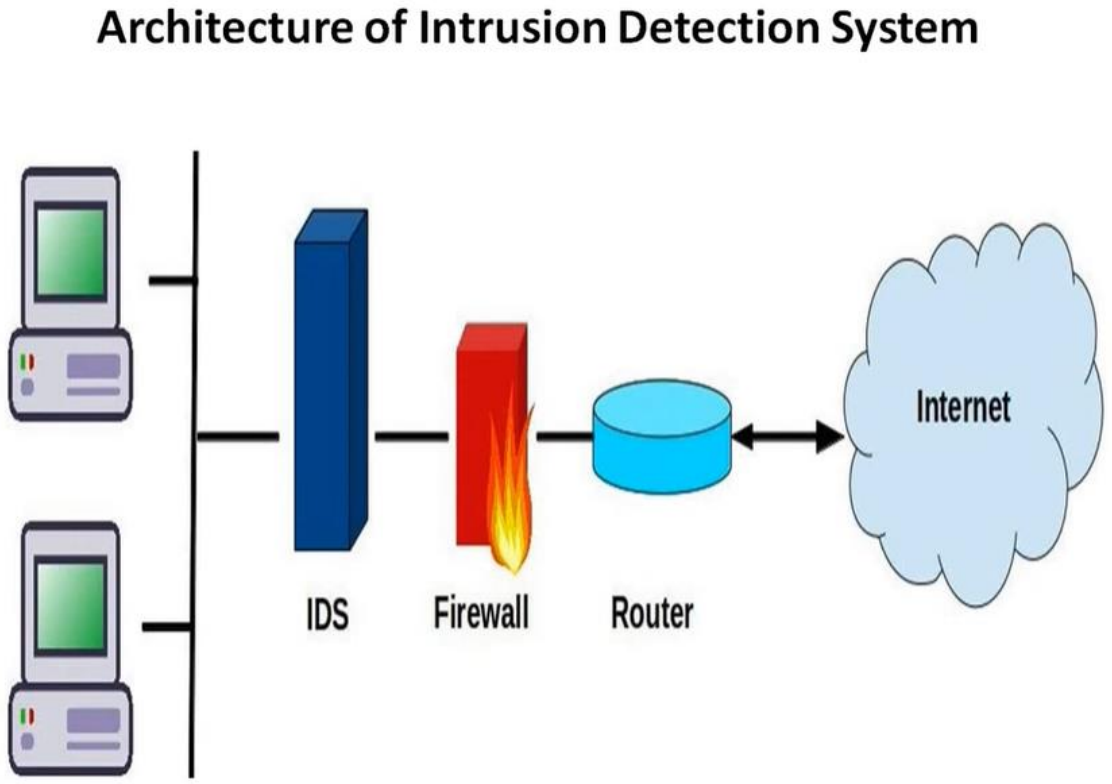
- A firewall is essential software or firmware in network security that is used to prevent unauthorized access to a network.
- It is used to inspect the incoming and outgoing traffic with the help of a set of rules to identify and block threats by implementing it in software or hardware form.
- Firewalls can be used in both personal and enterprise settings, and many devices come with one built-in, including Mac, Windows, and Linux computers.



Intrusion Detection System

What is Intrusion Detection?

- Monitoring and analyzing both user and system activities.
- Analyzing system configurations and vulnerabilities.
- Assessing system and file security
- Ability to recognize patterns of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violation



Intrusion Detection System

Why Need of Intrusion Detection System?

- To prevent unauthorized behaviors
- To detect attack and other security violation
- To detect and deal with attacks
- To document the existing threats
- Acts as a quality control for security design and administration
- To provide useful information about intrusion that is to take place, allowing improved diagnosis recovery and corrections.

Assignment

1. Explain different security mechanism in details.
2. Explain Firewall and its types.
3. Explain IDS and its significance in the security of computer Network.