

Computer Networks

Lecture 10

Network Security

By
Dr. Khaled ELMenshawy

Lecture

10

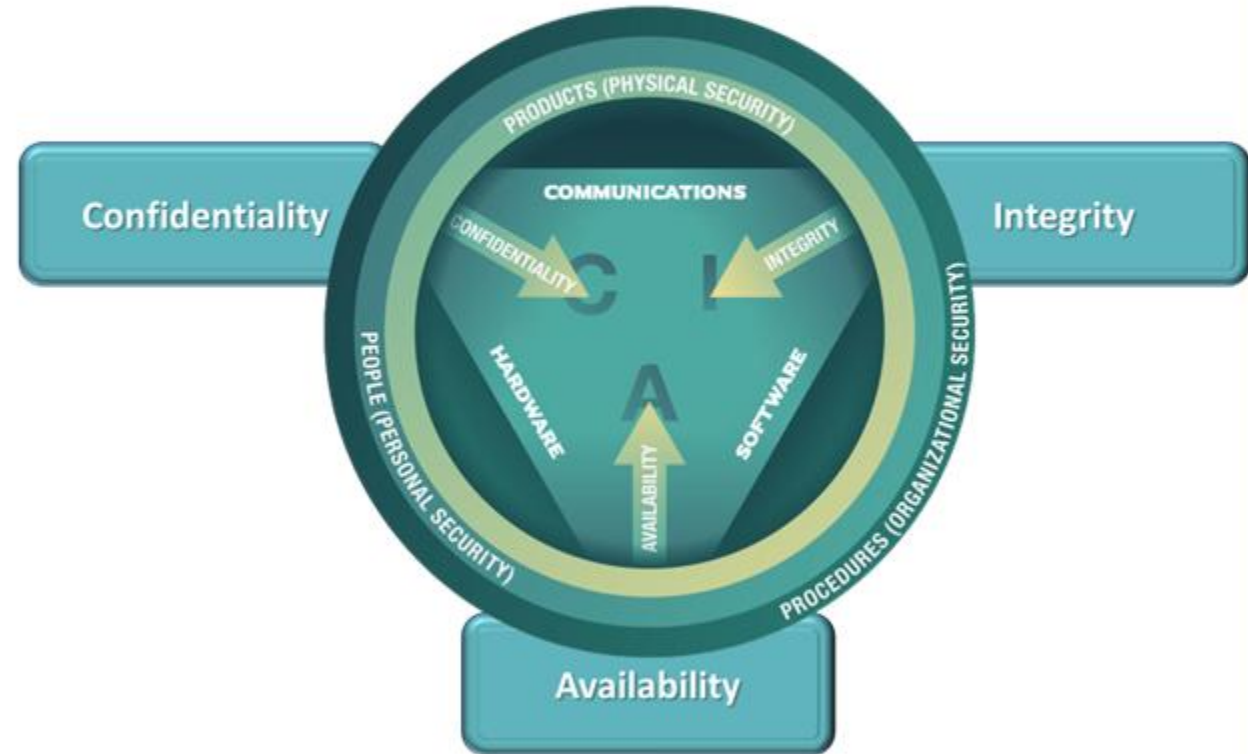
LEARNING OUTCOMES

- Understand the principle of Network security .
- Recognize the Types of Attacks
- Differentiate between symmetric and asymmetric Cryptography.
- Recognize different symmetric and asymmetric ciphers (DES, 3DES, AES, RSA, RC4).
- Recognize different common encryption methods (Digital certificates, PKI, SSL, TLS, Hash function, digital signature).
- Recognize different Authentication Protocols (PAP, SPAP, CHAP, TOTP, HMAC-OTP, Kerberos, EAP)
- Understand Wireless network security.
- Understand operation security (Firewall, IDS, IPS).
- Understand VPN and DMZ.
- Virtualization.

What is network security?

What is network security?

- It is a set of rules and configurations designed to protect the integrity, confidentiality and availability of computer networks and data using both software and hardware technologies.



What is network security?

Confidentiality:

The secured information is accessible only to authorized users and prevents the disclosure of information to unauthorized parties. *Revealing the data only to authorized users.*

Integrity:

Information must be remained accurate, consistent, and not subject to unauthorized modification.
changes need to be done only by authorized users and through authorized mechanisms.

Availability:

Information is always available for authorized users. *The computer system remains work without degradation of access, provide resources to authorized users when they need it.*

What is network security?

Assets	Confidentiality	Integrity	Availability
Hardware	-	-	Equipment or device is stolen or disabled, thus denying service.
Software	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task	Programs are deleted, denying access to users.
Data	An unauthorized read of data is performed.	Existing files are modified, or new files are fabricated.	Files are deleted, denying access to users.
Communication and Network	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.	Messages are destroyed or deleted. Communication lines or networks are unreachable.

Key Security Terminologies

Terminology	Definition
Access Control List (ACL)	A mechanism that implements access control for a system resource by listing the identities of the <u>system entities</u> that are permitted to access the resource.
Adversary (threat agent)	An entity that attacks, or is a threat to, a system.
Asset (resources)	Something of value to a person, business or organization.
Attack	An assault on system security that derives from an intelligent threat.
Authentication	The process of confirming the correctness of the claimed identity.
Authorization	The approval or permission for someone or something to do something.
Countermeasure	An action, device, procedure, or technique that prevents or reduces a threat
Hacker	Someone who violates computer security for malicious reasons

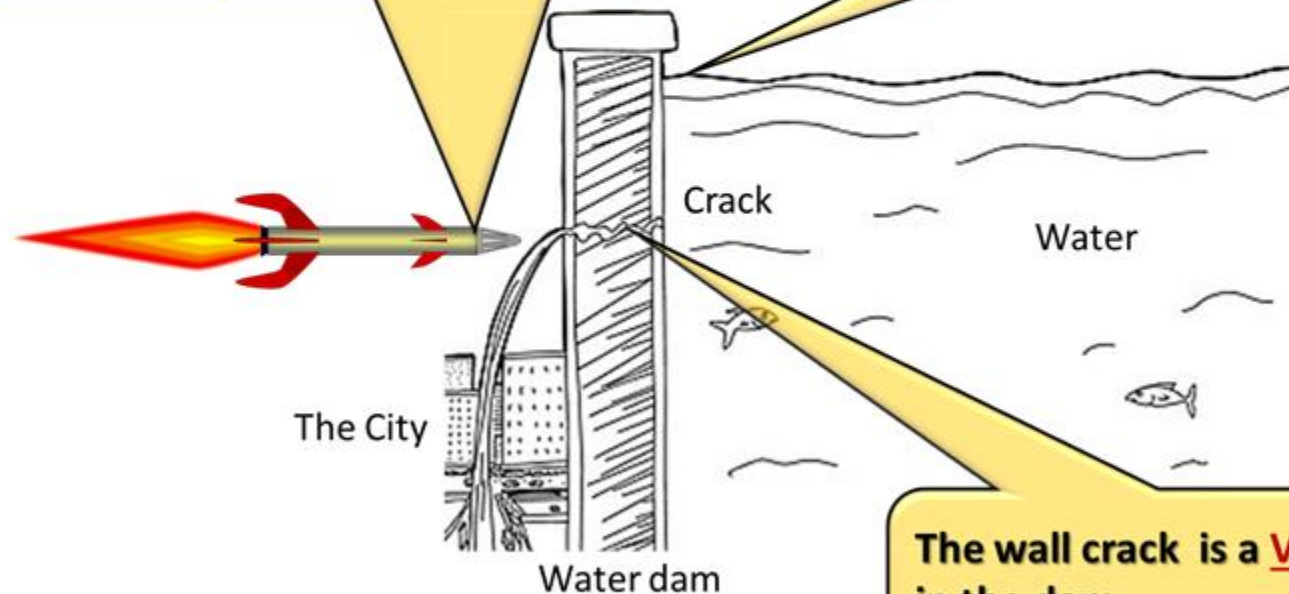
Key Security Terminologies

Terminology	Definition
Risk	The likelihood of exposure, critical asset or sensitive information loss as result of a cyber attack or breach within an organization.
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive assets.
Threat	A potential for violation of security by something that could cause harm to a system or organization.
Vulnerability	A weakness in a system's design, implementation, or operation and management could be exploited to violate the system's security policy.

What is network security?

Somebody **attack** the dam using the wall crack (Vulnerability)
Ex. (Computer) attacker sending malicious software to the open port to harm the system

Crossing the water behind the dam to the City is a **Threat**.
Ex. (Computer) System failures



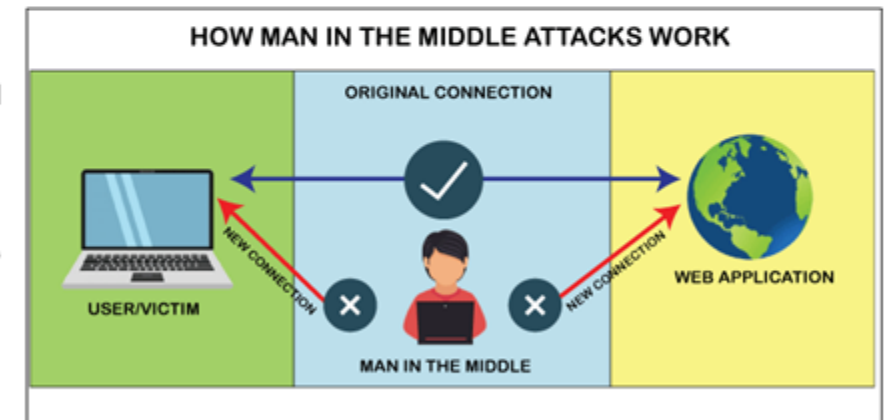
The wall crack is a **Vulnerability** in the dam.
Ex. (Computer) Open ports

Phishing:

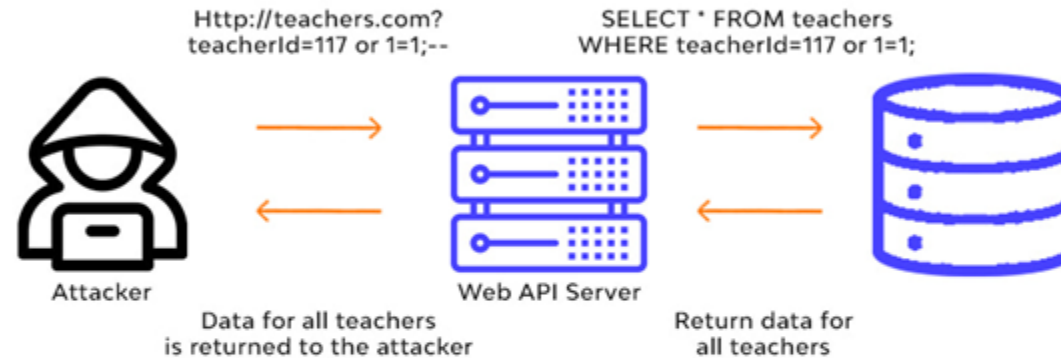
It is a criminal mechanism that use of email or websites for tricking users into giving personal information such as ID, Credit data, financial bank account credentials etc.

Man-in-the-middle attack:

The attacker intercepts communication between two individuals in order to steal data and gains access to the communication and changes part or all the data, The users remain unaware of the intrusion by the attacker.



SQL Injection

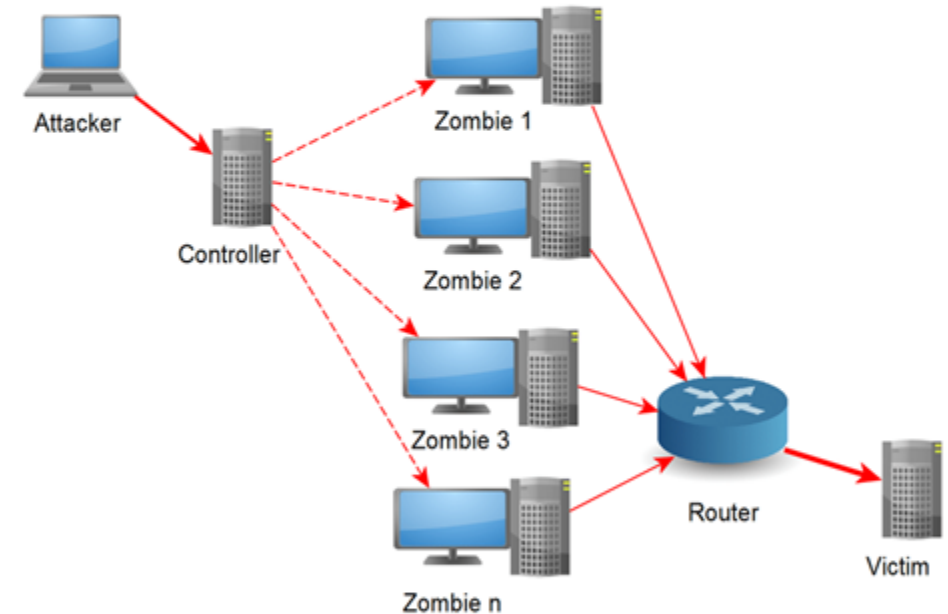
**SQL injection:**

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. The attackers exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Denial-of-service attack (DoS):

Attacker meant to shut down a machine or network, making it inaccessible to its intended users.

- **Buffer overflow attacks:** send more traffic to a network address than the programmers have built the system to handle.
- **ICMP flood :** sending spoofed packets that ping every computer on the targeted network.
- **SYN flood:** sends a request to connect to a server but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.



Brute Force:

This is an attack where the attacker tries guessing system access credentials like passwords by trying different character combinations until a correct combination is identified.

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password.

Brute Force Attacks Explained

In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.



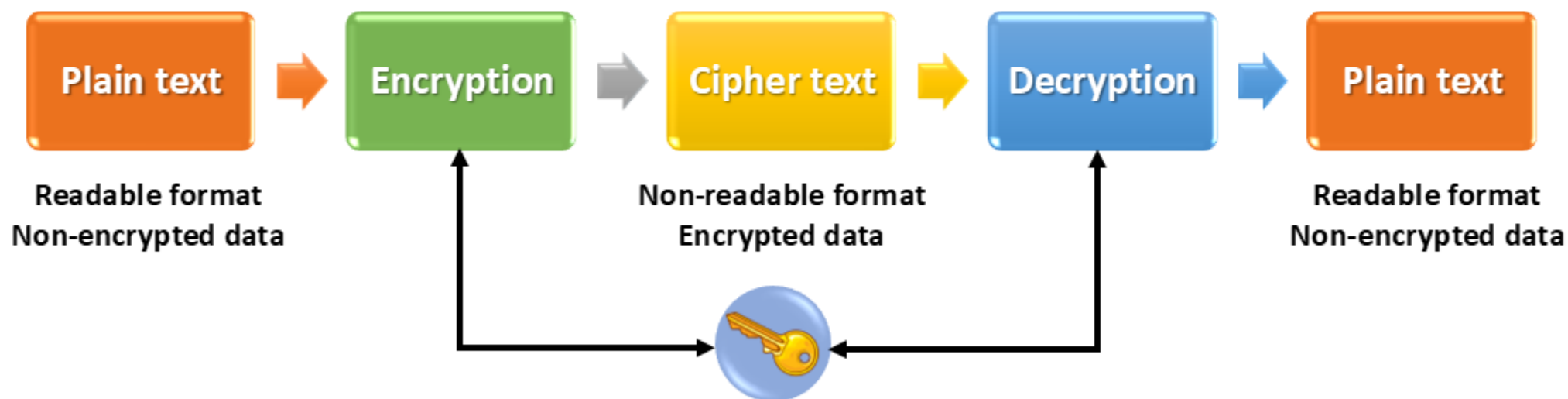
Malware:

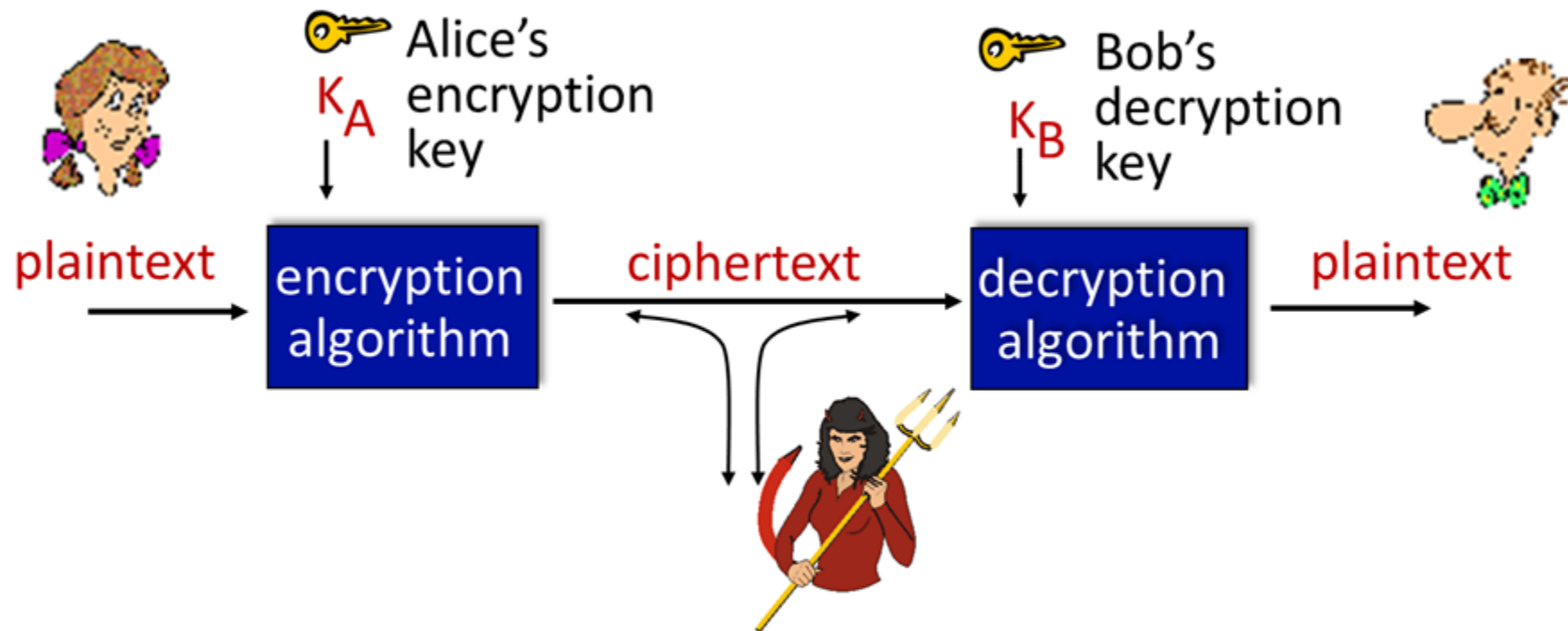
Malware is a computer program that performs malicious actions on another computer to disrupt or damage a user's computer.

- **Virus**, A self-replicating program that attaches itself to clean file.
- **Trojans**, A type of malware that is disguised as legitimate software.
- **Ransomware**, Malware which locks down a user's files and data.
- **Botnets**, Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.
- **Adware**, Advertising software which can be used to spread malware.

What is Cryptography?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.





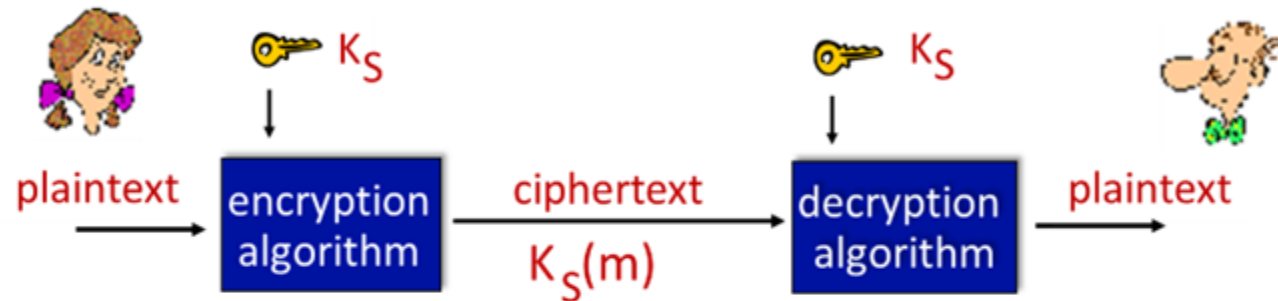
m: plaintext message

$K_A(m)$: ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Types of encryption

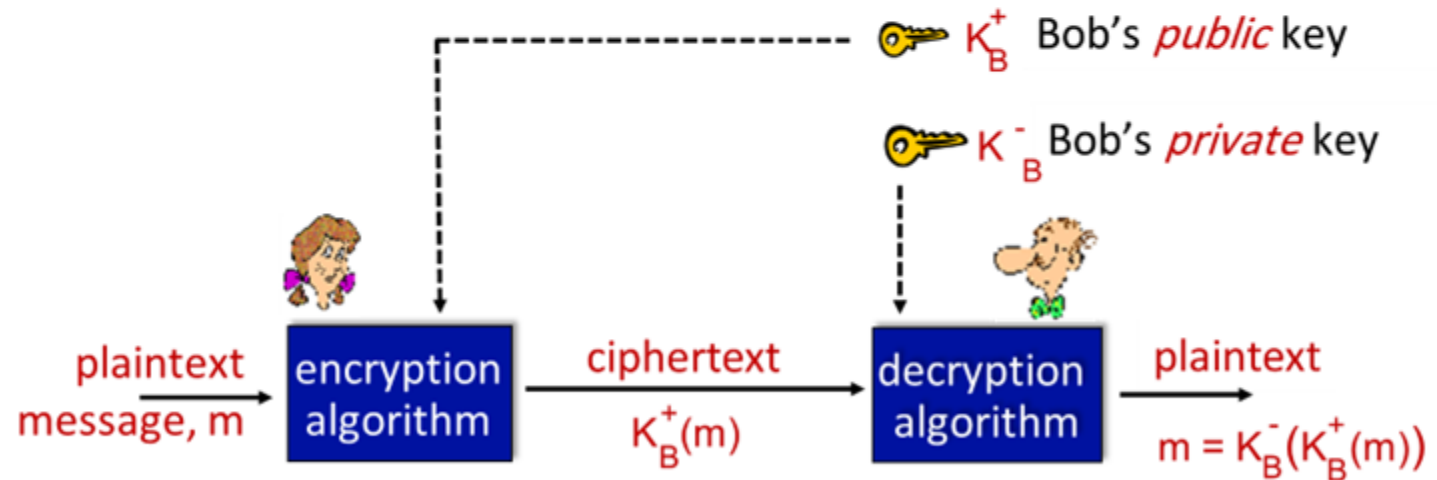
Symmetric



One single key for encryption and decryption,
such as DES and AES.

Asymmetric

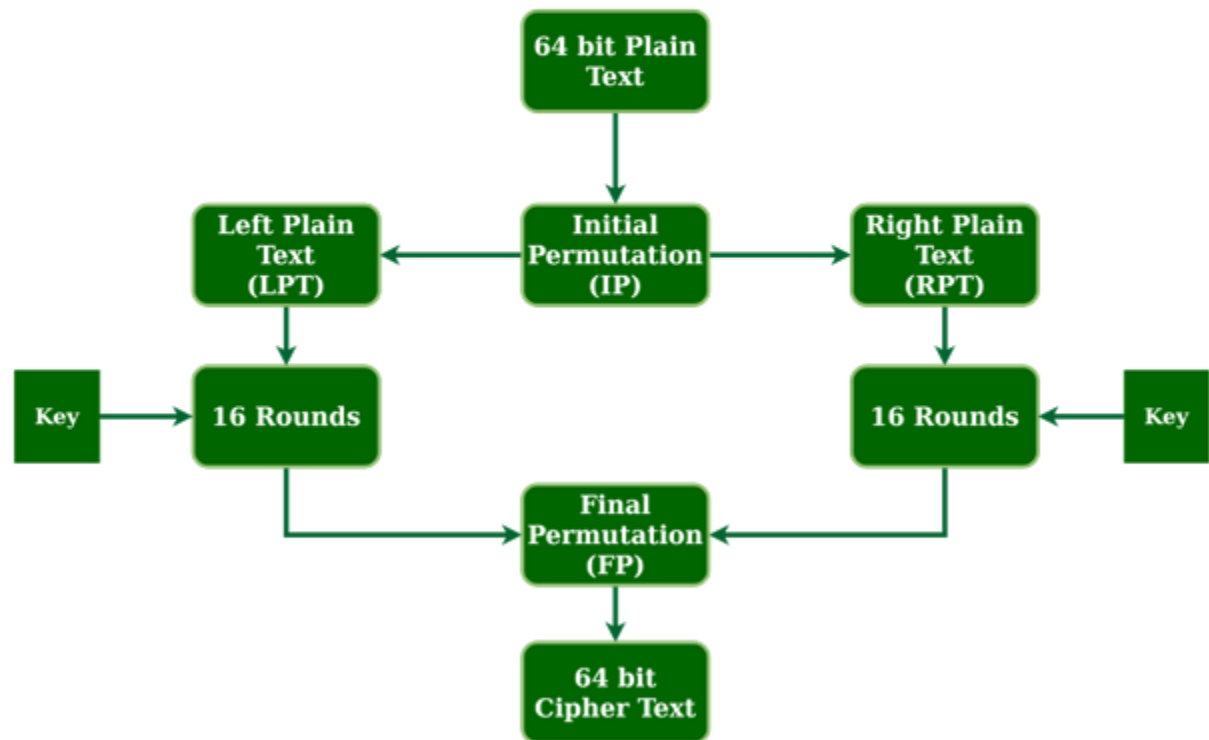
Two keys one for encryption
and the other for decryption,
such as Diffie-Hellman and RSA.



Symmetric	Asymmetric
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits.	The length of key used is 2048 or higher.

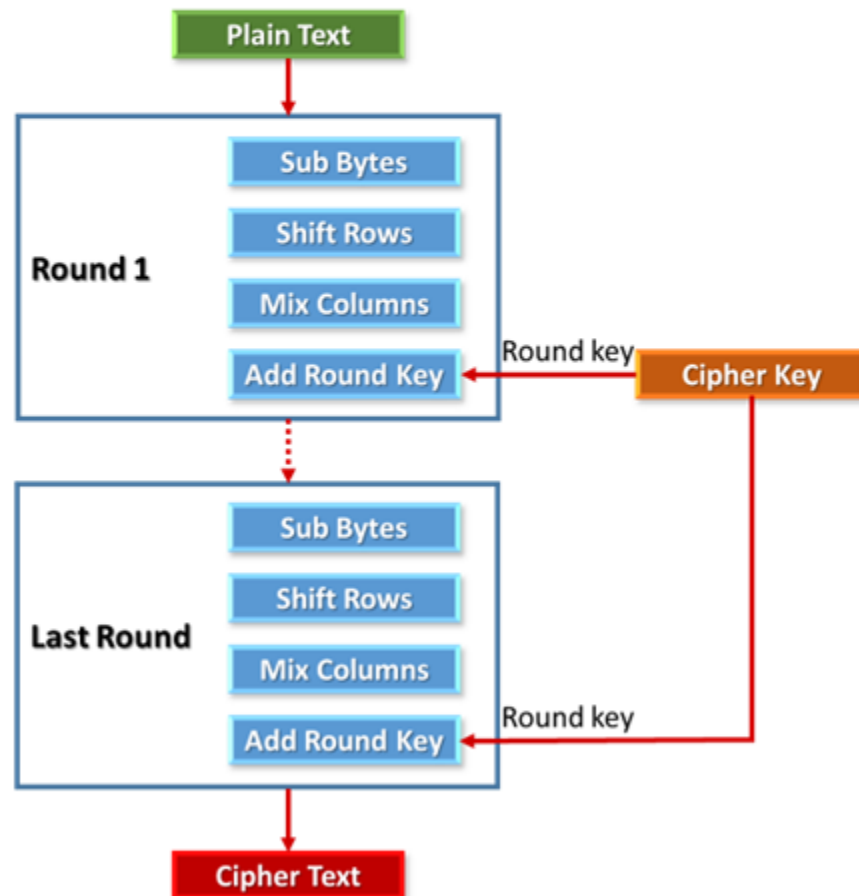
Data encryption standard (DES)

- **DES** is a 64-bit *block cipher* (because the key works only on 64 bits of data at a time).
- The key is 56 bits, with 8 bits used for error checking.
- Making DES more secure:
 - **3DES**: each block of data is encrypted 3 times with 3 different keys.
- DES encryption is obsolete today but 3DES will continue to be a reliable encryption algorithm at least through 2030.



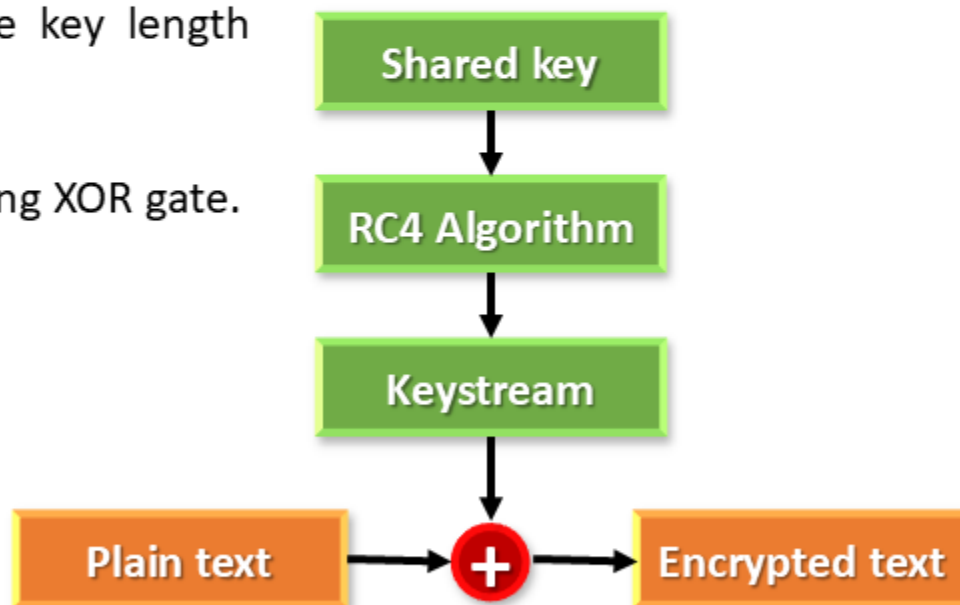
Advanced encryption standard (AES)

- **AES** is a 128-bit *block cipher* (because the key works only on 128 bits of data at a time).
- The key size can be 128/192/256 bits.
- The number of rounds depends on the key length as follows :
 - 128 bit key – 10 rounds
 - 192 bit key – 12 rounds
 - 256 bit key – 14 rounds
- **AES** is the most widely used encryption algorithm.
- Both AES and 3DES are unbreakable with current technology.



RC4 Cipher

- **RC4** is a *stream cipher*, which means that each digit or character is encrypted one at a time.
- **RC4** is used a shared key algorithm (symmetric cryptography), The key length varies from 40 to 2048 bits.
- Encryption is done by combining the keystream with the plain text using XOR gate.
- **RC4** became the basis for a number of protocols used to transfer information from one place to another. Such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) used in wireless communications.



Rivest, Shamir, and Adleman(RSA)

- Message: just a bit pattern which can be represented by an integer number e.g., $m = 10010001$. This message is represented by the decimal number 145.
- Thus, encrypting a message is equivalent to encrypting a number. which gives a new number (the ciphertext).
- Choose two large prime numbers p, q . (e.g., 1024 bits each).
- Compute $n = p * q$, $z = (p-1)*(q-1)$.
- Choose e (with $e < n$) that has no common factors with z (e, z are “relatively prime”).
- Choose d such that $ed \bmod z = 1$.
- **Public key** is (n, e) . **private key** is (n, d) . [$C = M^e \bmod n$, $M = C^d \bmod n$]

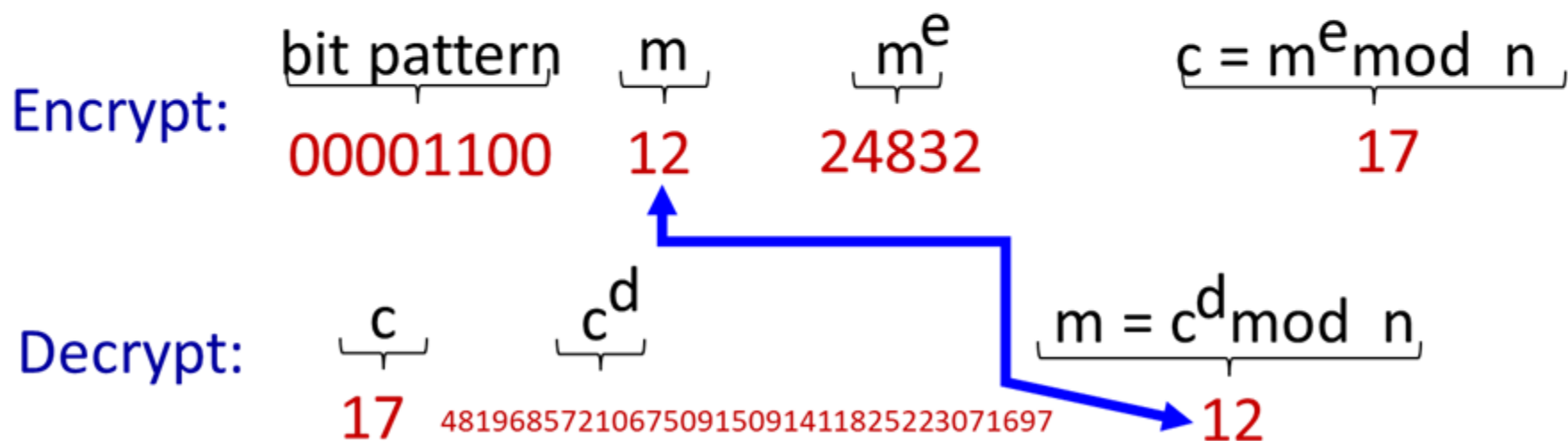
$\underbrace{(n, e)}_{K_B^+}$

$\underbrace{(n, d)}_{K_B^-}$

Chooses $p=5$, $q=7$. Then $n=35$, $z=24$.
 $e=5$ (so e , z relatively prime).
 $d=29$ (so $ed \bmod z = 1$).

Encrypting 8-bit messages.

RSA Example



Digital Certificates

- A *digital certificate* is a file or electronic password that proves the authenticity of a device, server, or user using the public key infrastructure (PKI).
- A *certificate authority (CA)* is the one responsible for issuing digital certificate, the CA may be a third-party organization such as VeriSign or internal to organization.
- *Revocation* of digital certificates happens when:
 - Certification is not used any more.
 - Details of certifications are changed.
 - The certificate owner's private key is compromised

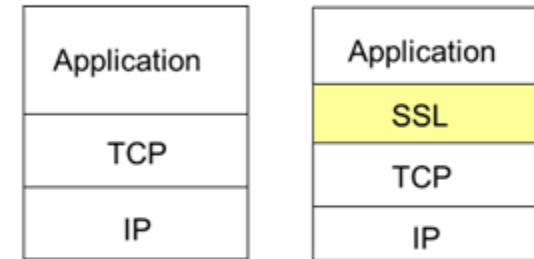


Public key infrastructure (PKI)

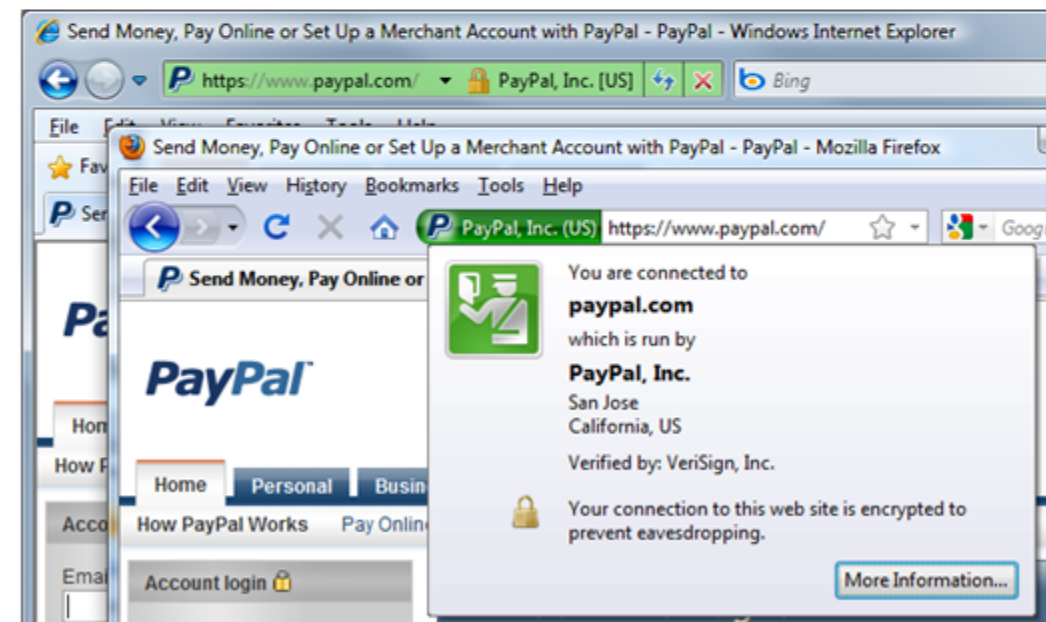
- PKI (or Public Key Infrastructure) is the framework of encryption that protects communications between the webserver and the clients.
- PKI has a common elements such as;
- **Digital Certificates**; it's a form of electronic identification for websites and organizations.
- **Certificate Authority (CA)**; popular certifying authorities include *VeriSign/Symantec, Kaspersky, Comodo, and Digicert.*
- **Registration Authority**; it is responsible for receiving certificate signing requests from applicants and forwards these requests to a Certificate Authority (CA).

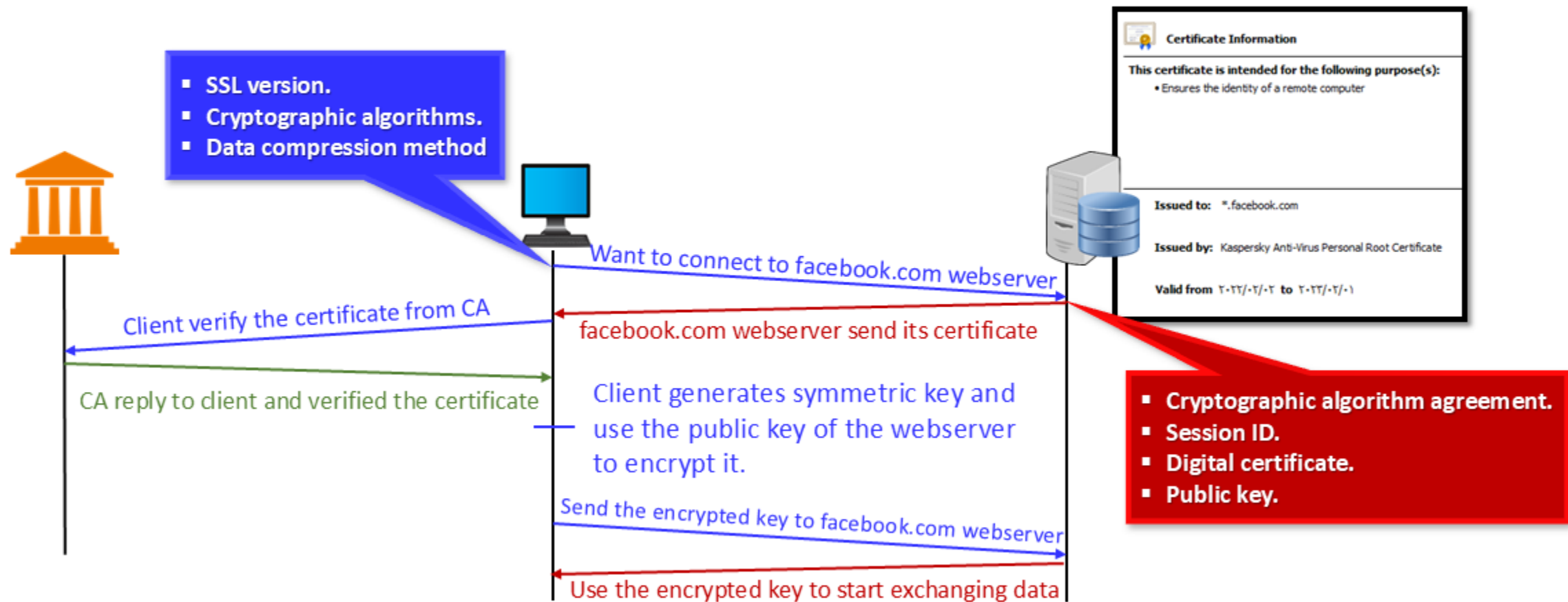
Transport Layer Security & Secure Socket Layer (TLS/SSL)

- SSL provides application programming interface (API) to applications.
- Used with **HTTPS** protocol (Secured version of HTTP).
- The TLS/SSL encryption is created with a **SSL certificate**. Certificates are issued by a certification company and contains information and instructions to transmit information between a web server and a user using a public key and a private key.



Normal application Application with SSL



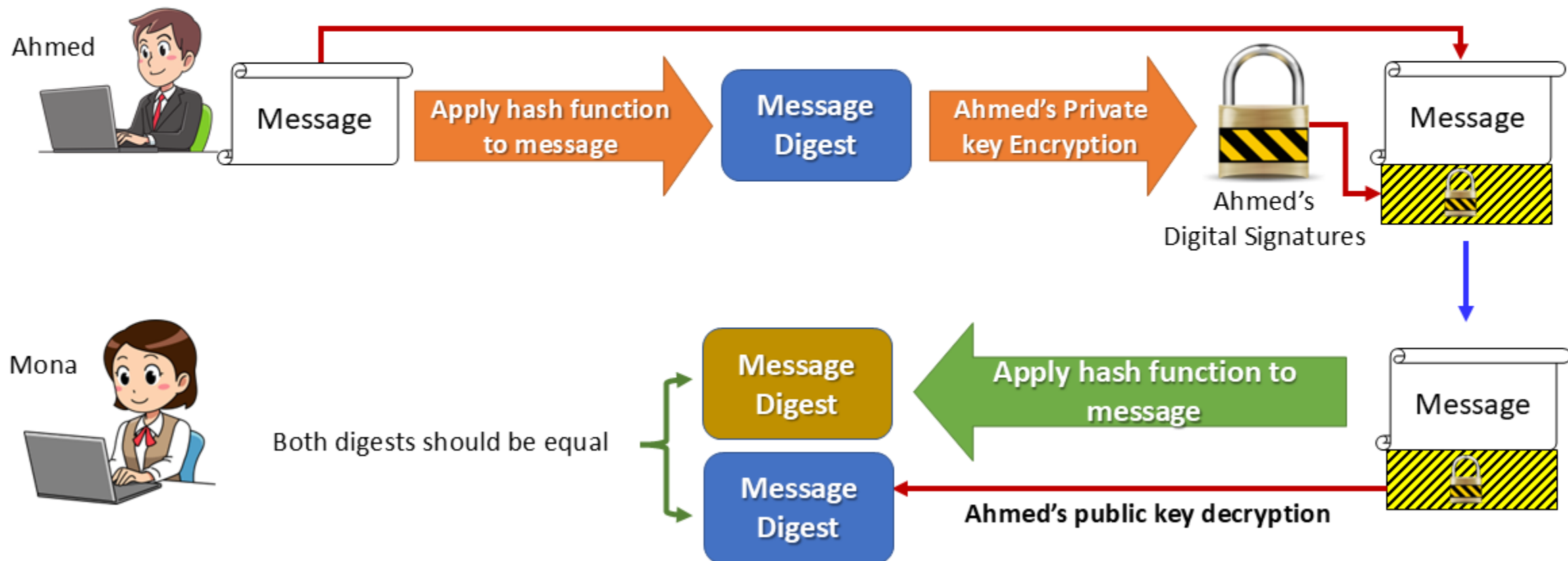
Transport Layer Security & Secure Socket Layer (TLS/SSL)

Hash Function

- Hash function takes a *string of variable length* and encodes as a *fixed-length hash value* called message digest. It does that via complex mathematical operations and it is *one-way function property*.
- *Collision Resistant property*; impossible to find two different inputs that produce the same output.
- A hash value is a like a fingerprint used to ensure the message's integrity.
- There are several different classes of hash functions. The most commonly used are:
 - **Message Digest Algorithm (MD5)**; it produces a 128-bit hash value.
 - **Secure Hash Algorithm (SHA)**; comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3 offer up to 512-bit hash value .
 - **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)**; provides 128-320-bit hash value .

Digital Signatures

- Digital signatures provide more security than other electronic signatures. It is analogous to hand-written signatures.
- SSL is asymmetric cryptography based on public-key infrastructure and it provides:
 - **Authentication**; prove the identity of the sender.
 - **Non-repudiation**; the sender can not deny sending the message.
 - **Integrity**; the message is not altered.

Digital Signatures

Authentication Protocols

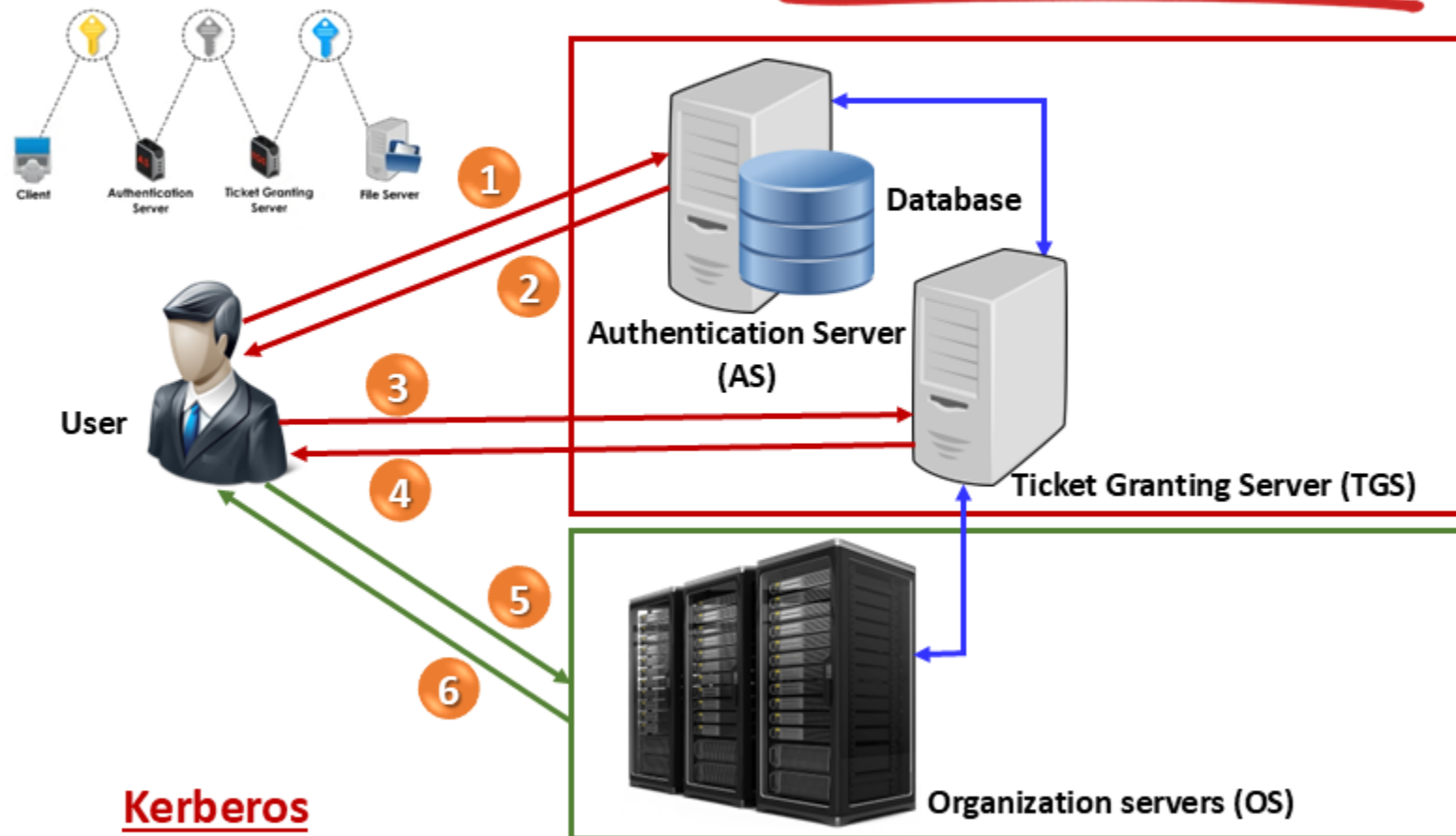
- An authentication protocol is defined as a computer system communication protocol which designed specifically to securely transfer authenticated data between two parties:
 - **Password Authentication Protocol (PAP)** is an authentication protocol that transmits data (passwords) in plain readable text as a single readable file.
 - **Shiva Password Authentication Protocol (SPAP)** is a proprietary form of **PAP** that offers more security than PAP. With SPAP, passwords are processed through a reversible encryption system.
 - **Challenge Handshake Authentication Protocol (CHAP)** is an industry standard communication protocol that uses the **MD5** Hashing scheme for authentication.
 - **Time-Based One-Time Password (TOTP)** is an authentication protocol that uses an algorithm to generate what is called a temporary passcode used for authenticating access to any system. This passcode is changed every 40 to 60 seconds.

Authentication Protocols

- **HMAC-Based One-Time Password** which is an authentication protocol similar to the TOTP that entails the generation of a one-time password used with only one authentication attempt.
- **Kerberos** is providing a centralized authentication servers and determines whether an individual is authorized for general entrance into a system, and whether they have access rights to particular resources belonging to the system, **Kerberos** supports a number of encryption types such as DES, AES, RC4, and Camellia.



Authentication Protocols



Kerberos

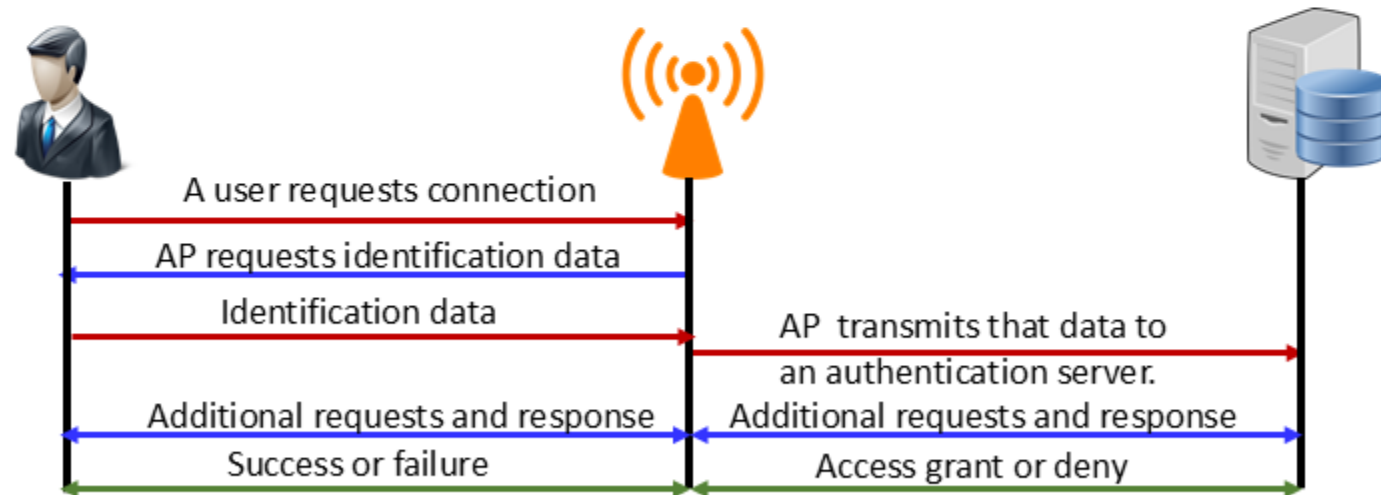
1	User login and requests for ticket-granting service, the request is encrypted using the user password.
2	Authentication Server decrypts the user request using the saved user password and verifies user's access right using database and then gives the user ticket-granting-ticket (TGT) encrypted with a secret key.
3	User send (TGT) to Ticket Granting Server which decrypts TGT using the secret key from AS.
4	TGS sends the user a token encrypted with another secret key shared with (OS).
5	The user sends the token to the (OS) which decrypt it with the secret key that shard with TGS.
6	OS grants access to the user.

Authentication Protocols

- **Internet Protocol Security (IPSec)** encryption is one part of the protocol suite that allows the information to be securely transmitted and received across a network often used in setting up *virtual private networks (VPNs)*. IPSec uses authentication (verification of identity and/or origin) and encryption (scrambling a message so that it has to be decoded to be understood) to send data across a network via:
 - **Authentication headers (AH)**; which ensure the integrity and verify the origin (source) of the data (verifying user identity).
 - **Encapsulating Security Payload (ESP)**; which works to ensure data confidentiality (protecting the data).

Authentication Protocols

- **Extensible Authentication Protocol (EAP)** is a protocol for wireless networks that expands the authentication methods between the supplicant (the Wi-Fi workstation) and the authentication server (Microsoft IAS or other). There are several authentication types of EAP include EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, and EAP-FAST.



- Wireless security providing safety, ensuring privacy, and allowing only authorized and authenticated access to networks.
- Wireless security encryption is mainly divided into four main types:

	WEP	WPA	WPA2	WPA3
Year	1999	2003	2004	2018
Encryption method	RC4	Temporal key integrity protocol (TKIP) + RC4	CCMP +AES	AES
Key size	40-bit	128-bit	128-bit	128-bit WAP3 personal 192-bit WAP3 Enterprise
Cipher type	Stream cipher	Stream cipher	Block cipher	Block cipher

- Firewalls are protective software/hardware barriers that defend computers and networks against malicious content and unauthorized access.
- Firewalls perform two basic security functions for a network:
- **Packet filtering**; the firewall operates at the packet level:
 - **Port filtering**; allow or deny packet based on port number.
 - **MAC filtering**; allow or deny packet based on MAC address.
 - **IP filtering**; allow or deny packet based on IP address (specific IP or range of IP addresses).
 - **Content filtering**; allow or deny packet based on content information of the packet.
 - **Dynamic filtering**; allow or deny packet based on the network policy after examine the whole packet.
- **Application proxy**; the firewall operates at application level rather than the packet level. It is able to recognize and block the malware attempts because it can examine the entire application being used.

Intrusion detection and prevention systems

Intrusion Detection System (IDS)

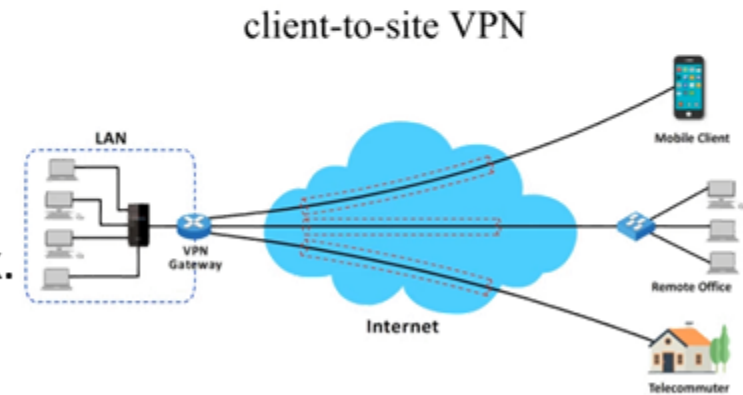
- An intrusion detection system (IDS) is a data security system that continually monitors network traffic and identifies patterns or traffic that seem unusual.
- Intrusion detection systems are classified based on how they implement intrusion detection:
 - **NIDS**; Network IDS, detection is placed at various important locations within the network.
 - **HIDS** - Host IDS, detection is placed at each device on the network.
- Methods of Intrusion Detection:
 - **Signature**; IDS monitors the information moving about in the system for known patterns or attributes.
 - **Anomaly**; IDS compares established norms with current values. If anything doesn't match, an alert is generated.
 - **Passive** ; IDS simply monitors, notices, and notifies. It doesn't take any corrective action when an issue occurs.
 - **Reactive** ; IDS behaves like the passive method. But it takes a corrective action when an issue occurs.

Intrusion detection and prevention systems

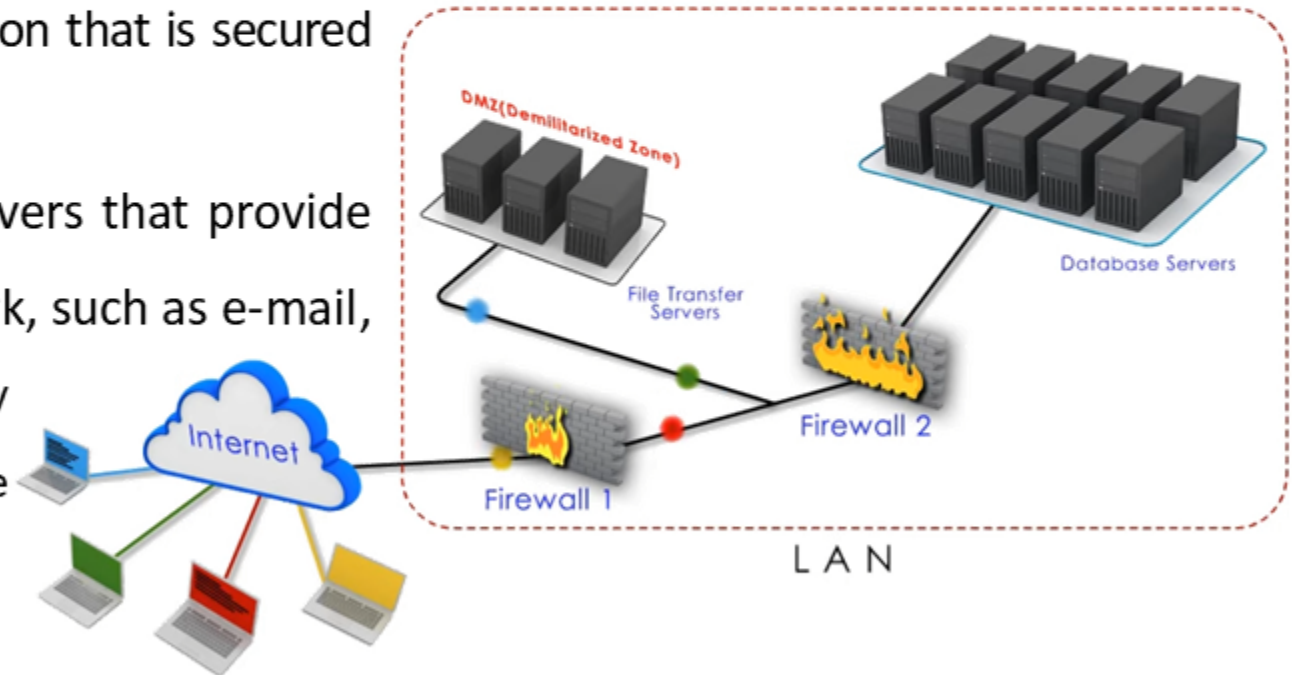
Intrusion Prevention System (IPS)

- An IPS helps identify malicious activity attempting to infiltrate the network and blocking it before it has the chance to damage the system.
- Intrusion prevention systems come in four primary types:
 - **Network-based**: Protect your computer network.
 - **Wireless**: Protect wireless networks only.
 - **Network behavior**: Examine network traffic.
 - **Host-based**: Come as installed software to protect a single computer
- IPS prevention Activities are:
 - Blocking all traffic suspected of having a malicious objects.
 - Dropping malicious packets, or pieces of data, trying to be delivered to a system.
 - Eliminating network access for suspicious senders or websites.

- A virtual private network (VPN) is a network that is completely isolated from the rest of the Internet. It provides people, businesses, governments, and military organizations to remotely use network resources securely.
- VPN use tunneling protocols such as Point-To-Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Layer (SSL), and IPsec.
- VPNs have two types:
 - **Site-to-Site VPN**; allows two or more networks to be joined together.
 - **Client-to-Site VPN**; allows a user with a computer to access a private network.

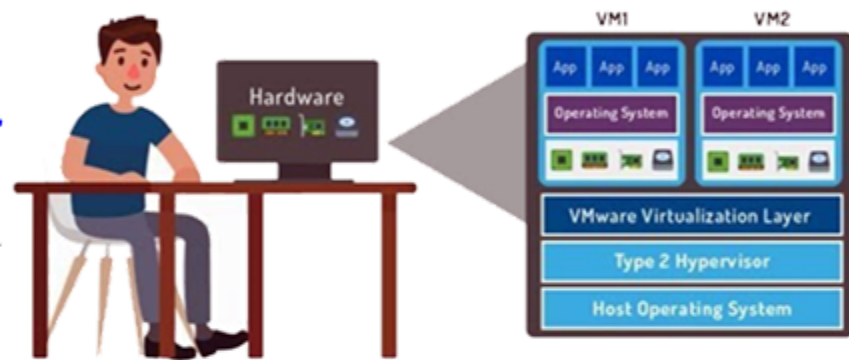


- A DMZ is a sub-network of an organization's network.
- It allows access to an un-trusted zone, such as the internet, but cannot reach back to the internal network system.
- An intranet is the internal network of an organization that is secured behind one or more firewalls.
- DMZ contains the most vulnerable to attack servers that provide services to users outside of the local area network, such as e-mail, Web and Domain Name System (DNS) servers, they are 'quarantined' inside a DMZ, from where they have limited access to the private network.



What is Virtualization?

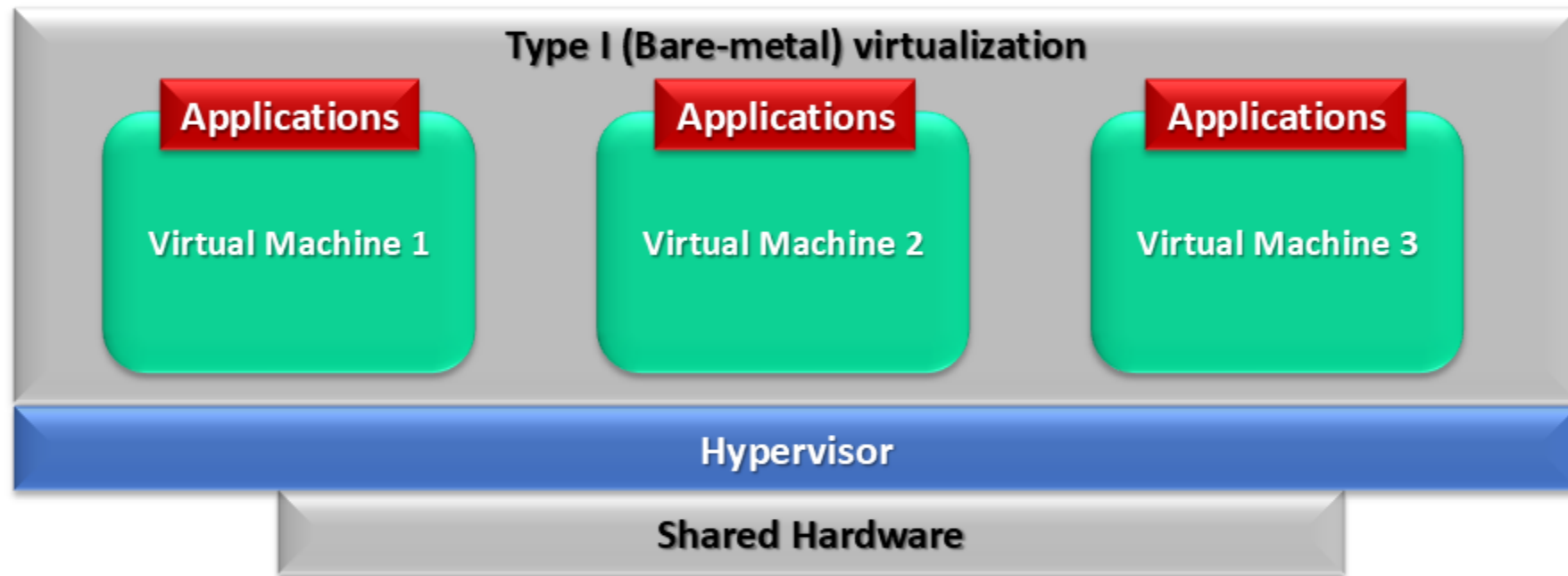
Virtualization; is the *simulation of the software and/or hardware* upon which other software runs. This simulated environment is called virtual machine (VM).



Running *multiple operating systems on the same hardware at the same time* and *Each VM can run its own operating systems and applications* as if it were in a physical machine.

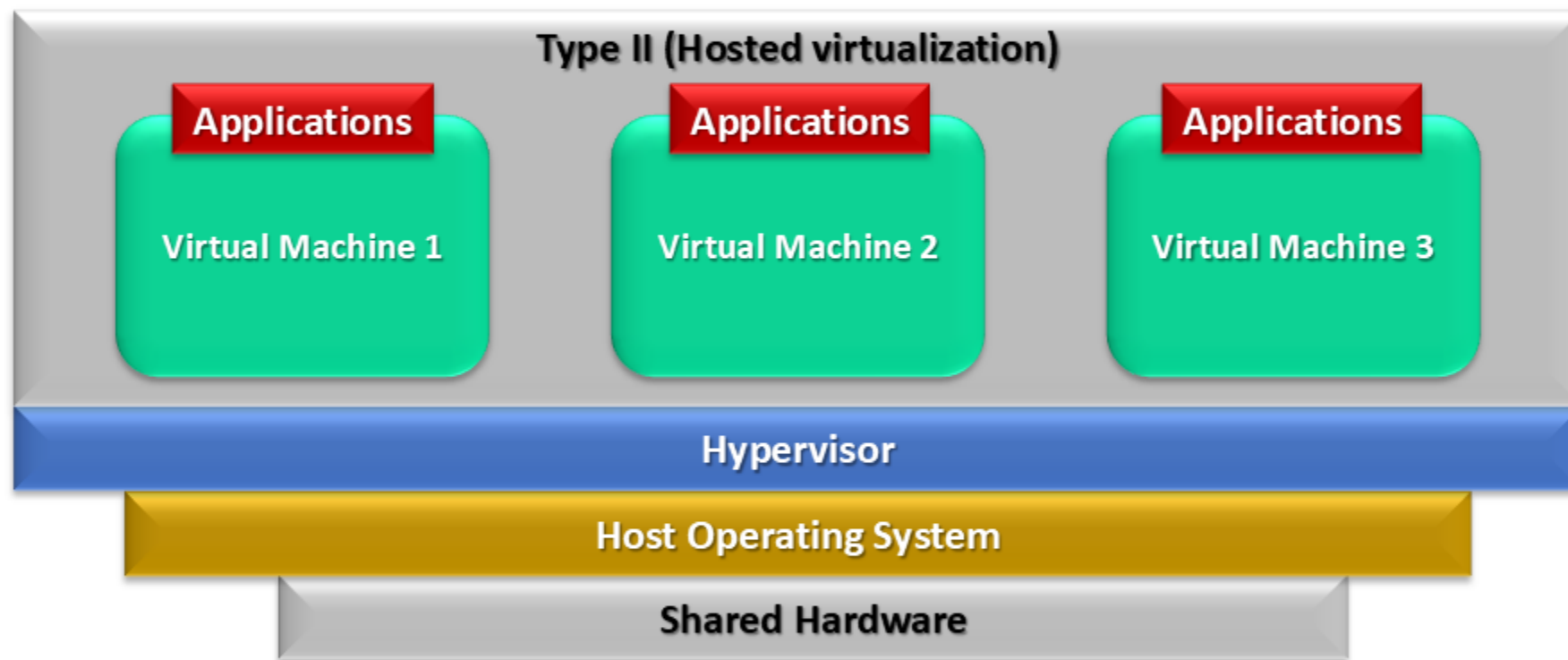
A piece of software called a **hypervisor** is installed to which *manages the distribution of the physical servers' resources* such as the processor, memory, and hard disk space among the virtual machines

Type I Hypervisor



Also known as a ***Bare-Metal*** or a *native hypervisor*, *runs directly on the host hardware and functions similarly to an operating system*. ***Examples of*** type 1 hypervisors include Microsoft Hyper-V, Citrix's XenServer and VMware ESXi and vSphere.

Type II Hypervisor



A *Hosted Architecture* which *operates within a standard operating system* such as Windows, Mac, or Linux. *Examples of* type 2 hypervisors include VirtualBox and VMware

There are some vulnerabilities that come to virtualization:

➤ *Virtual machine escape*; is breaking out one of isolated virtual machines and *interacting directly with the underlying hypervisor*, then attacker could *migrate themselves out and into another virtual machine* being hosted on the same physical server.

To mitigate VM escape:

- Keep virtual machine software patched.
- Install only the resource-sharing features that you really need.
- Keep software installations to a minimum because each program brings its own vulnerabilities.

- Privilege elevation; is occurring when a user is able to *grant themselves the ability to run functions as a higher-level user* such as the root or the administrator.

To mitigate Privilege elevation: Regularly patching and updating software, operating systems, and firmware.

- Live migration of virtual machines; is when a *virtual machine needs to move from one physical host to another*. If an attacker can place themselves between these two physical machines, they can implement a form of an *adversary-in-the-middle (AiTM)* attack where they can *capture the data being sent between two physical servers*.

To mitigate AiTM: use strong and unique passwords, enable MFA, and Use conditional access policies.

➤ **Resource reuse**; is a concept in computing where system resources, like memory, storage, or processing power can be reused for different tasks or processes. A resource reuse vulnerability occurs when *a system resource such as memory is not properly cleared or reset before being assigned to another task*. This can potentially *allow sensitive information from the previous task to be exposed to the new task*.

