# Unit 1

## Reading 1

### When was known as the founder of the Internet?

Key: Larry Roberts

### When has the Internet become an interconnection of millions of networks and why?

* In the 1990s. Since its inception as a tool for sharing Defense Department information
* I think because the internet brought connectivity to virtually all computers that could reach a phone line or an Internet - connected local area network(LAN)

## Reading 2

### What is Security?

**security** is “the quality or state of being secure to be free from danger.”.

### What is information security?

**Information security**, to protect the confidentiality, integrity and availability ofinformation assets

### What layers of security should a successful organization have in place to protect its operations?

* A successful organization should have the following multiple layers of security in place to protect its operations: **Physical security, personnel security, Operations security, Communications security, Network Security, Information Secutity.**
* Three Characteristic of information need project ingrate: confidentiality (tinh bao mat), integrity (tinh toan ven), availability (tinh co san)

### What does C.I.A stand for? What is it? What does C.I.A triangle mean in Vietnamese? Is the C.I.A. triangle model suitable for information security now?

* C.I.A Triangle: Confidentiality Integrity Availability : Tam giac bao mat
* The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle
* No.

### Compare 6 loai tan cong bi dong

* A passive attack: is one where the hacker/adversary only monitor the commonication chanel. A passive attacker only threatens confidentiality of data
* Active attack: is one where the adversary attempts to delete, add or alter the transmission on the channel an active threatens confidentiality, authentication and integrity.
* A direct attack is a hacker using a personal computer to break a system. An indirect attacker compromising a system and using it to attacker originate from a compromised system or resourced that is malfuntion or working under the control of a threat
* Intentional and unintentional attack (co chu dich>< vo tinh) : a hacker attempting to break into an information system is an intentional attack. Alight Strike that cause a fire a building is an unintentional attack

### Which areas does information security include?

Information security includes the systems and hardware that use, store, and transmit that information, the broad areas of information security management, computer and data security, and network security.

## Reading 3

### How many critical characteristics does information have? What are they?

Information has 7 critical characteristics: confidentiality, accuracy, authenticity, utility, possession, integrity and availability

## Reading 4

### What is an information system?

an **information system (IS)** is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization.

### What is the software? Which software do you know?

* Software is a collection of statements or instructions, written in one or more different programming languages in a specified order and comprises applications, operating systems, and assorted command utilities.
* Some software: Facebook, Telegram, Zing MP3

### What is the hardware? List some hardware components you know

* Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system.
* List some hardware components: CPU, Ram, Network Card, Hard Drive

### How many component of Information System? What are they?

There are 6 component of Information System, include: Hardware, Software, People, Network, Procedures, Data

# Unit 2

## Reading 1

### What is Intellectual property?

* Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person’s intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source
* Intellectual property can be trade secrets, copyrights, trademarks, and patents (hoc them)

### What is the most common IP breach?

The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**

### What is one of the most common methods of virus transmission?

One of the most common methods of virus transmission is via e-mail attachment files.

### What is the virus (worm, trojan, backdoor or trapdoor, polymorphic threats, Virus and Worm Hoaxes, Espionage or Trespass)? How do you work?

* **Virus:**
* A computer virusconsists of segments of code that perform malicious actions, using the all own replication machinery to propagate the attack beyond the initial target.
* How to work: The code attaches itself to an existing program and takes control of that program’s access to the targeted computer. The virus-controlled target program then carries out the virus’s plan by replicating itself into additional targeted systems.
* **Worm:**
* Named for the Tapeworm in John Brunner’s novel *The Shockwave Rider*, a worm is a malicious program that replicates itself constantly, without requiring another program environment. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
* How to work: The complex behavior of worms can be initiated with or without the user downloading or executing the file.
* **Trojan horse:** Trojan horses are software programs that hide their true nature and reveal their designed behavior only when activated
* **Back door or Trap door:** A virus or worm can have a payload that installs a back door or trap doorcomponent in a system, which allows the attacker to access the system at will with special privileges
* ***Polymorphic Threats:*** One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A polymorphic threatis one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures
* ***Virus and Worm Hoaxes:*** As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don’t exist.
* **Espionage or trespass** is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass

### Compare intelligence and industrial espionage

Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, **competitive intelligence**. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting **industrial espionage**

### Compare Virus and Worm:

* virusconsists of segments of code that perform malicious actions. Worm is a malicious program that replicates it.
* The primary difference between a virus and a worm is that must be triggered by the activation of their host; whereas worms are stand alone malicious programs that can self replicate and progagate independtly as soon as they have breached the system.

### Who are hackers? Which skill levels are divided among hackers?

* **Hackers** are “people who use and create computer software to gain access to information illegally.”
* There are generally two skill levels among hackers.

### Compare Elite hacker and novice or unskilled hacker

* Elite hacker: The first is the **expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in the second category, the novice or **unskilled hacker**.
* The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system
* Novice or unskill hacker: who originates nothing but simply steals code, techniques and attack methods from others

## Reading 2

### Which one is the biggest threat to an organization? Why?

* One of the greatest threats to an organization’s information security is the organization’s own employees
* Because employees use data in everyday activities to conduct the organization’s business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data—even, suggests, relative to threats from outsiders.

### Why do employees’s mistakes represent a serious threat to the confidentiality, integrity, and availability of data?

This is because employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

### What is a theft? Which type of theft in the information security do you know?

* The threat of theft—the illegal taking of another’s property, which can be physical, electronic, or intellectual—is a constant(dong 11 trang 43)
* There are two type of theft in the information security: physical theft, electronic theft

## Reading 3

### What is an attack?

* An **attack** is an act that takes advantage of a vulnerability to compromise a controlled system

### What is a vulnerability?

* A **vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective

### What does the **malicious code** attack include? What is spyware and adware?

* The **malicious code** attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
* **spyware** is “any technology that aids in gathering information about a person or organization without their knowledgeand it is placed on a computer to secretly gather information about the user and report it”
* **adware**—is “any software program intended for marketing purposes such as that used to deliver and display advertising banners or popups to the user’s screen or tracking the user’s online usage or purchasing activity.”

### What attack in the information security do you know?

SQL Injection, Weak Audit, Database protocol vulnerabilities, Weak authentication, excessive privileges

### List some attacks in the information security you know

Malicious Code, Hoaxes, Back Doors, Password crack, Brute Force, Dictionary, Denial –of –Service(DoS) and Distributed, DdoS, Spoofing, Spam, Mail Bombing, Man- in- the –Middle, Sniffers, Social Engineering, Phising, Pharming, Timing Attack

### What is password crack (hoaxes, brute force, dictionary, DdoS)?

* A more devious attack on computer systems is the transmission of a virus hoax *with a real virus attached*.
* Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks (to be covered shortly)
* The application of computing and network resources to try every possible password combination is called a **brute force attack (password attack)**
* The application of computing and network resources to try every possible password combination is called a **brute force attack**
* A **distributed denial-of-service (DDoS)** is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

## Reading 4

### What is the spoofing (man –in –the –middle, spam, mail bombing, social engineering, pharming, timing attack)?

* **Spoofing** is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host
* In the well-known **man-in-the-middle** or **TCP hijacking attack**, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network
* **Spam** is unsolicited commercial e-mail.
* Another form of e-mail attack that is also a DoS is called a **mail bomb**, in which an attacker routes large quantities of e-mail to the target
* A **sniffer** is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information.(
* social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. (**Phishing -** an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. A variant is ***spear phishing***, a label that applies to any highly targeted phishing attack. Doc them)
* Pharmingis “the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate site for the purpose of obtaining private information.
* A timing attackexplores the contents of a Web browser’s cache and stores a malicious cookie on the client’s system.

### What are Sniffers? What are they used for? Why are they dangerous?

* A **sniffer** is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information.
* Sniffers can be used both for legitimate network management functions and for stealing information.
* because they are virtually impossible to detect and can be inserted almost anywhere.

# Unit 3

## Reading 1

### What is a firewall in computing?

* In [computing,](https://en.wikipedia.org/wiki/Computing) a **firewall** is a [network security s](https://en.wikipedia.org/wiki/Network_security)ystem that [monitors](https://en.wikipedia.org/wiki/Network_monitoring) and controls incoming and outgoing [network traffic](https://en.wikipedia.org/wiki/Network_traffic) based on predetermined security rules.

### How can firewalls be categorized?

* Firewalls can be categorized by processing mode, development era, or structure

### What is a firewall? What are its benefits?

* A **firewall** in an information security program is similar to a building’s firewall in that it prevents specific types of information from moving between the outside world, known as the **untrusted network** (for example, the Internet), and the inside world, known as the **trusted network**.

### How many types of firewall do you know? What are they?

There are three type of firewall, include: packet filters, stateful filters, application layer

## Reading 2

### list some firewalls classified by structures?

Some firewalls are classified by structures:

* Commercial-Grade Firewall Appliances.
* Commercial-Grade Firewall Systems.
* Small Office/Home Office (SOHO) Firewall Appliances.
* Residential-Grade Firewall Software.
* Software Versus Hardware: The SOHO Firewall Debate

## Reading 3

### What is the SOCKs, the SOCKs System?

* The Socks: is the protocol for handling TCP traffic via a proxy server
* SOCKs System: is a proprietary circuit – level proxy that place specical SOCK client side agents on each work station

### Different “Screen Host Firewall” and “Dual Home Host Firewall”

* Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy.
* the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration. One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With two NICs, all traffic *must* physically go through the firewall to move between the internal and external networks. Implementation of this architecture often makes use of NAT

### What does the word “architecture” mean?

* Architecture is the art and science of designing and managing the construction of buildings and other structures. Architecture has many artistic qualities but must also satisfy practical considerations.

### How many common architectural implementations?

* there are four common architectural implementations: Packet-filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls.

## Reading 4

### What does the phrase “firewall processing mode”

* Firewall processing mode: is a packet filtering mode that examines the header information of a data packet, usually based on a combination of:
* IP source and destination address
* Direction (inbound or outbound)
* Protocol (for firewalls capable of examining the IP protocol layer)
* Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests (for firewalls capable of examining the TCP/UPD layer

### What firewall processing modes do you know? Give some information to support your anwsers?

* Introduction’s paragraph: There are five major processing-mode categories: packet-filtering firewalls, application gateways, circuit gateways, MAC layer firewalls and hybrid firewalls.
* Packet-filtering firewall examines the header information of data packets that come into a network. (Page 79 - Second paragraph)
* Application gateway is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router. (Page 85 - First paragraph)
* Circuit gateway firewall operates at the transport layer and prevents direct connections between one network and another. (Page 76 - First paragraph)
* MAC layer firewalls are designed to operate at the media access control sublayer of the data link layer (Layer 2) of the OSI network model. (Page 86 - MAC’s paragraph)
* Hybrid firewall includes the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. (Page 86 - Hybrid’s paragraph)

# Unit 4

## Reading 1

### What is an intrusion detection system(IDS)?

* An **intrusion detection system** (**IDS**)) is a device or [software application](https://en.wikipedia.org/wiki/Software_application) that monitors a [network](https://en.wikipedia.org/wiki/Computer_network) or systems for malicious activity or policy violations.

### What is IPS? What can it do?

* A current extension of IDS technology is the **intrusion prevention system (IPS)**, which can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response

### What do you about IDPS? What is IDPS used for?

* **intrusion detection and prevention system (IDPS):** combined term intrusion detection and prevention system is is generally used to describe current anti-intrusion technologies.
* IDPS used for:
* According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS:

To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the syste

* To detect attacks and other security violations that are not prevented by other security measures
* To detect and deal with the preambles to attacks (commonly experienced as network probes and other “doorknob rattling” activities)
* To document the existing threat to an organization
* To act as quality control for security design and administration, especially in large and complex enterprises
* To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors

## Reading 2

### What is NIDS’s function?

* Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network

### What is the difference between on-line NIDS and off-line NIDS?

* When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and offline NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real time. It analyses the [Ethernet packets](https://en.wikipedia.org/wiki/Ethernet_frame) and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

### What is HIDS? What is HIDS’s function?

* A **host-based intrusion detection system** (**HIDS**) is an [intrusion detection system](https://en.wikipedia.org/wiki/Intrusion_detection_system) that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system (NIDS) operates.
* One can think of a HIDS as an [agent](https://en.wikipedia.org/wiki/Software_agent) that monitors whether anything or anyone, whether internal or external, has circumvented the system's [security policy.](https://en.wikipedia.org/wiki/Security_policy)

## Reading 3

### What is a signature –based IDPS (statistical anomaly-based IDPS, Stateful Protocol Analysis IDPS )

* A signature-based IDPS(sometimes called a **knowledge-based IDPS** or a **misusedetection IDPS**) examines network traffic in search of patterns that match known **signatures**—that is, preconfigured, predetermined attack patterns. Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures.
* The statistical anomaly-based IDPS (stat IDPS) or **behavior-based IDPS** collects statistical summaries by observing traffic that is known to be normal.
* Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations

### What are the weaknesses of the signature-based approach?

* A potential problem with the signature-based approach is that new attack strategies must continually be added into the IDPS’s database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed. Another weakness of the signature based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame.

### What is the solution to the weaknesses of the signature-based approach?

* The only way a signature-based IDPS can resolve this vulnerability is to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

### What are the disadvantages of the statistical anomly-based approach?

* Unfortunately, these systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline.
* Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives

### What is the benefit of the statistical anomly-based approach?

* The advantage of the statistical anomaly-based approach is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type.

## Reading 4

### What are honeypots, honeynet, padded cell?

* Honeypots are decoy systems designed to lure potential attackers away from critical systems.
* When a collection of honeypots connects several honeypot systems on a subnet, it may be called a honeynet.
* A padded cell is a honeypot that has been protected so that that it cannot be easily compromised—in other words, a hardened honeypot.

### What are honeypots designed for?

* Divert an attacker from critical systems
* Collect information about the attacker’s activity
* Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond

### What are The advantages and disadvantages of using the honeypot or padded cell?

* Advantage:
* Attackers can be diverted to targets that they cannot damage.
* Administrators have time to decide how to respond to an attacker
* Attackers’ actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections.
* Honeypots may be effective at catching insiders who are snooping around a network.
* Disadvantage:
* The legal implications of using such devices are not well understood. - Honeypots and padded cells have not yet been shown to be generally useful security technologies.
* An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization’s systems. - Administrators and security managers need a high level of expertise to use these systems

### Diffenece “ enticement” and “entrapment”

* Enticement is the act of attracting attention to a system by placing tantalizing information in key locations.
* Entrapment is the act of luring an individual into committing a crime to get a conviction. Enticement is legal and ethical, whereas entrapment is not.

### What is Labrea?

LaBrea is a “sticky” honeypot and IDPS and works by taking up the unused IP address space within a network.

# Unit 5

## Reading 1

### What is cryptography? What is it used for?

* Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication

### What is encryption? What is decryption? What is the key?

* The process of making the information unreadable is called encryption or enciphering. The result of encryption is a ciphertext or cryptogram.
* Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so-called cipher is used.
* The key is known only to those who are authorized to read the information

### How is a cryptographic algorithm works?

* How a cryptographic algorithm works, is controlled by a secret key, sometimes called password or passphrase (on crypto machines, the key is the setting of the machine).
* Without knowing the key, it should be impossible to reverse the encryption process, or the time to attempt to reverse the process should required take so much time that the information would become useless.

### What is cryptanalysis?

Cryptanalysis or crypto-analysis is the study and analysis of existing ciphers or encryption algorithms, (or Cryptanalysis is the process of obtaining the original message (called the **plaintext**) from an encrypted message (called the **ciphertext**) without knowing the algorithms and keys used to perform the encryption) in order to assess their quality, to find weaknesses or to find a way to reverse the encryption process without having the key.

### How many goals does cryptography have? What are they?

Cryptography have four goals, include: ***Confidentiality, Data integrity, Data integrity, Non-repudiation***

### How many types of attack in a cryptanalytic attack?what are they?

there are two types of attack: The ciphertext-only attack, where the cryptanalyst or attacker has access only to the ciphertext, and the known-plaintext attack, where the cryptanalyst has access to both ciphertext and its corresponding plaintext or assumed plaintext, to retrieve the corresponding key

## Reading 2

### Who are Whitefield Daffier and Martin Hellman? What did they invent? What are their algorithms based on? What is one of the most significant contribution of public-key cryptography?

* Whitefield Diffie and Martin Hellman introduced the idea of public-key cryptography of which algorithms are based on the computational complexity problem.
* The Diffie–Hellman algorithms are based on the discrete logarithm problem.
* One of the most significant contribution provided by public-key cryptography is the digital signature.

## Reading 3

### What do the letter *A,M,C,K* denote?

* *A* denotes a finite set called the *alphabet of definition*
* *M* denotes a set called the *message space.* An element of *M* is called a *plaintext message* or simply *a plaintex*
* C denotes a set called the *ciphertext space.* An element of *C* is called a *ciphertext*
* *K* denotes a set called the *key space.* An element of *K* is called a *key*.

### What is ?

* *Ee* is called an *encryption function* or an *encryption transformation*.
* *Dd* is called a *decryption function* or *decryption transformation*.

m stand for message; c ciphertext

### What does an encryption scheme consist of?

An *encryption scheme* consists of a set {*Ee : e K*} of encryption transformations and a corresponding set {*Dd : d K*} of decryption transformations with the property that for each e K there is a unique key *d* *K* such that *Dd = E2-1*; that is, *Dd  (Ee (m)) = m* for all *m* *M*. An encryption scheme is sometimes referred to as *a cipher*.

### What does one have to do construct an encryption scheme?

* To construct an encryption scheme requires one to select a message space *M*, a ciphertext space *C*, a key space *K*, a set of encryption transformations {*Ee : e K*} and a corresponding set of decryption transformations {*Dd : d K*}

## Reading 4

### How many parties do you think normally participate in a two -way communication? Who are they?

There are four parties:

* An *entity* or a *party* is someone or something which sends, receives, or manipulates information. Alice and Bob are entities An entity may be a person, a computer terminal, etc.
* A *sender* is an entity in a two-party communication which is the legitimate transmitter of information.
* A r*eceiver* is an entity in a two-party communication which is the intended recipient of information.
* An *adversary* is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver

### What is channel, a physicallay secure channel or secure channel, a unsecured channel, a secured channel?

* A *channel* is a means of conveying information from one entity to another.
* A *physically secure channel* or *secure channel* is one which is not physically accessible to the adversary.
* An *unsecured channel* is one from which parties other than those for which the information is intended can reorder, delete, insert, or read.
* A *secured channel* is one from which an adversary does not have the ability to reorder, delete, insert, or read.

### What is information security service, breaking , a passive adversary, an active adversary?

* *Information security service* is a method to provide some specific aspects of security
* *Breaking* an information security service (which often involves more than simply encryption) implies defeating the objective of the intended service.
* A *passive adversary* is an adversary who is capable only of reading information from an unsecured channel.
* An *active adversary* is an adversary who may also transmit, alter, or delete information on an unsecured channel.

# Unit 6

## Reading 1

### What are hash function? What are hash algorithms? What is message digest?

* **Hash functions** are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content
* . **Hash algorithms** are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value.
* The **message digest** is a fingerprint of the author’s message that is compared with the recipient’s locally calculated hash of the same message.

### What hash functions do you know?

SHA-1, SHA -384, MD4, SHA -256

### Why are hash functions widely used in e-commerce?

hash functions confirm message identity and integrity, both of which are critical functions in e-commerce

### How many main properties does an ideal cryptographic hash function have? What are they?

The ideal cryptographic hash function has four main properties:

* It is easy to compute the hash value for any given message
* It is infeasible to generate a message that has a given hash
* It is infeasible to modify a message without changing the hash
* It is infeasible to find two different messages with the same hash.

### What is time-memory tradeoff attack? What method can prevent this attack?

* A recent attack method called rainbow cracking has generated concern about the strength of the processes used for password hashing. This type of attack is more properly classified as a **time–memory tradeoff attack**.
* you must first protect the file of hashed passwords and implement strict limits to the number of attempts allowed per login session. You can also use an approach called password hash salting. Salting is the process of providing a non-secret, random piece of data to the hashing function when the hash is first calculated

## Reading 2

### What is called symmetric encryption?

Encryption methodologies that require the same **secret key** to encipher and decipher the message are using what is called **private key encryption** or **symmetric encryption**.

### What is the primary challenge of symmetric key encryption?

The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band (meaning through a channel or band other than the one carrying the ciphertext) to avoid interception.

### What do you know about symmetric encryption?

* Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers
* One of the challenges is that both the sender and the recipient must have the secret key. Also, if either copy of the key falls into the wrong hands, messages can be decrypted by others and the sender and intended receiver may not know the message was intercepted. The primary challenge of symmetric key encryption is getting the key to the receiver, a process that must be conducted out of band (meaning through a channel or band other than the one carrying the ciphertext) to avoid interception

## Reading 3

### What is asymetric encryption? What do you know about it?

* **asymmetric encryption** uses two different but related keys, and either key can be used to encrypt or decrypt the message.
* Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification. This technique has its highest value when one key is used as a private key

### What is a mathematical trapdoor?

A mathematical **trapdoor** is a “secret mechanism that enables you to easily accomplish the reverse function in a one-way function.”.

### What can users do and what can’t they do with a trapdoor?

With a trapdoor, you can use a key to encrypt or decrypt the ciphertext, but not both, thus requiring two keys. The public key becomes the true key, and the private key is derived from the public key using the trapdoor.

## Reading 4

### What is PKI? What is used for?

**Public-key Infrastructure (PKI)** is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.

### What components are intergrated for a typical solution PKI to protect the tranmission and reception of secure information?

A typical PKI solution protects the transmission and reception of secure information by integrating the following components: A *certificate authority (CA),* A *registration authority (RA), Certificate directories, Management protocols, Policies and procedures.*

## Reading 5

### What is a cyberattack?

A cyberattack is any type of offensive maneuver that targets [computer information systems,](https://en.wikipedia.org/wiki/Computer_information_systems) [infrastructures,](https://en.wikipedia.org/wiki/Infrastructure) [computer networks,](https://en.wikipedia.org/wiki/Computer_network) or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.

### What types of attacks cryptography do you know? State your understanding about it.

* In general, attacks on cryptosystems fall into four general categories: man-in-themiddle, correlation, dictionary, and timing.
* A **man-in-the-middle attack** attempts to intercept a public key or even to insert a known key structure in place of the requested public key. Establishing public keys with digital signatures can prevent the traditional man in-the-middle attack, as the attacker cannot duplicate the signatures.
* **Correlation attacks** are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext generated by the cryptosystem. Differential and linear cryptanalysis, which are advanced methods of code breaking that are beyond the scope of this text, have been used to mount successful attacks on block cipher encryptions such as DES. The only defense against this attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of key changes.
* In a **dictionary attack**, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target in an attempt to locate a match between the target ciphertext and the list of encrypted words
* In a **timing attack**, the attacker eavesdrops on the victim’s session and uses statistical analysis of patterns and inter-keystroke timings to discern sensitive session information. Having broken an encryption, the attacker may launch a **replay attack**, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source
* Defending Against Attacks

# List tu viet tat

MODT: message of the day

APPA: Defence’ce Advanced Research Project Agency

MULTICS: Information and Computing Service

GE: General Electric

CNSS: Committtee on National Security System

IS: Information system

IP: intellectual property

DOS: Denial –of –Service

DSoS: Denial –of –Service and Distributed

SAM: Security Account Manager (trinh quan ly bao mat)

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

DEC: Digital Equipment Corporation

FWTK: Firewall Toolkit

FTP: File Transfer Protocol

DNS: Domain Name System

HTTP: Hypertext Transfer Protocol

NDFW: next generation firewall

WAF: Application Firewall

IPS: intrusion prevention system

SOHO: Small Office/Home Office

ISP: Internet service provider

DSL: digital subcriber lines

NIC: Network Interface Card

NAT: Network Address Translation

SOCKs server: Socket Secure Server

FDDI: Fiber Distributed Data Interface

IP: Internet Protocol

MAC: messgae authentication code

OSI: Open System Interconnect

RPC: Remote Procedure Calls

HIDS: A host –base intrustion detection system

NIDS: Network intrusion detection system

IDS: intrusion detection system

IDPS: intrusion detection and prevention system

SIEM: Security information and event management

SPA: Stateful Protocol Analysis

ARP: Address Resolution Protocol(Giao thuc phan giai dia chi)

SHS: Secure Hash Standard

NIST: Nationa; Institute of Standards and technology

DES: Data Encryption Standard

AES: Advanced Encryption Standard

PKI: Public –Key Infrastructure