INTERNET OF THINGS (IOT)

Asst. Prof. DR. MUHANED TH. M. AL-HASHIMI

Tikrit University

Collage Of Computer And Mathematical Science

2024 - 2025

BASICS OF NETWORK SECURITY

LECTURE 2

2204 - 2025

18 Of February

Outline

This lecture will talk about:

- Introduction to Security
- Network Confidentiality
- Cryptography
- Message Integrity and Authenticity
- Key Management
- Internet Security
- Firewall

Introduction to Security

- The range of **operations** dependent on **computers**, **computer networks**, and the **Internet** is **vast**. Healthcare, banking, governance, security, military, research, power, agriculture, and other fields are nowadays largely dependent on **networked systems**.
- The huge implications of the **failure** of one of these domains due to computer-based **security** lapses هفوه ,زلةare **undeniable** لايمكن انكارها. This necessitates يستلزم the need for various security protocols for computer networks and computer-based systems.
- Typically, **security in networks focuses on preventing** unauthorized or forced access to a user's or organization's system or systems.
- The **concept of security applies** even to computers or systems that are **not connected** to a network or the Internet.
- The **main aspects of securing** a **system are** security الامان, privacy الخصوصية, and authenticity المصداقية.
- The **security operations in computers** encapsulate تتضمن the **protection of** hardware, software, data, and identity.

Introduction to Security

- The various forms of **network attacks are classified into two broad categories**:

1. General cyber threats:
   Attacks such as authentication violations انتهاكات المصادقة, non-repudiation عدم الإنكار, Trojan horses, viruses, fraud الاحتيال, sabotage التخريب, denial of service رفض الخدمة, and even natural disasters الكوارث الطبيعية are categorized as general cyber threats.

2. Threats to web databases:
   Attacks such as access control violations انتهاكات التحكم في الوصول, **integrity** violations انتهاكات النزاهة, السلامة, **confidentiality** violations انتهاكات السرية, **privacy** violations انتهاكات الخصوصية, **authenticity** violations انتهاكات الموثوقية, and **identity** thefts are categorized as threats to web databases.

Introduction to Security

- ✓ Most of the commonly available **security tools** are **antiviruses**, **anti-malware**, **anti-spyware**, and **firewalls**.
- ✓ These are mostly **software-based tools** and used by individuals or for personal computing systems.
- ✓ However, costlier options such as **hardware-based systems** and **hardware-software hybrid systems** such as access control mechanisms, hardware firewalls, and proxy servers are the most opted-for security measures for large organizations.
- ✓ These **tools** are designed to protect a user from a range of attacks.

Introduction to Security

- Some **basic practices** on the computer or over networks can easily ward off تصد, تمنع most security threats.

✓ **Examples** of these **practices** include the following.

(i) **Choosing passwords wisely** so that it is a mixture of alphabets (preferably, both uppercase and lowercase characters), numbers, and special characters; passwords need to be changed periodically.

(ii) **Avoid sharing passwords** or credentials, or storing/recording them in an obvious واضحة,ظاهرة manner such as on a piece of paper, or your desktop.

(iii) **Keeping systems up to date** and patched on time.

(iv) **Using anti-virus**, **anti-spyware**, and **firewalls** tend to reduce the scope of threats.

(v) **Avoid downloading of suspicious attachments** and clicking on **random links** or **pages**.

Security

- **Security** in **networks** and **computer** systems work toward the following **three goals**:

1. Confidentiality السرية
2. Integrity السلامة, النزاهة
3. Availability التوافر

- This is often referred to as the CIA triad.

Security

1. Confidentiality: السرية , الخصوصية

Confidentiality pertains تتعلق to the **protection** of stored and transmitted information over the network in such a ***manner*** that the **information itself is concealed** مخفية and **protected from unauthorized access**.

- ✓ **Attacks** such as **snooping** التجسس and **traffic analysis** تحليل حركة المرور pose تشكل a direct threat to the confidentiality of information.

- ✓ A **breach** خرق of **confidentiality can occur** if the nature of the information, the **information** itself, or the **address** of the **sender** or **receiver** is **revealed** كشف to an **unauthorized third party**.

Security

2. Integrity سلامة

- ✓ The loss of **integrity** of any **stored** or **transmitted** information may arise due to both intended or unintended actions أفعال مقصودة أو غير مقصودة.
- ✓ Whenever **changes are made to any information** in a system or network by unauthorized entities, a breach of the system or network **integrity is presumed** يُفترض حدوث.
- ✓ **Attacks** such as repudiation رفض,نفي , replays, modification, and masquerading التنكر may pose severe threats to the integrity of information.
- ✓ It is interesting to note that **changes in information** due to **power outages** or other **natural causes** may also be considered a **breach of information integrity**.

Security

3. Availability

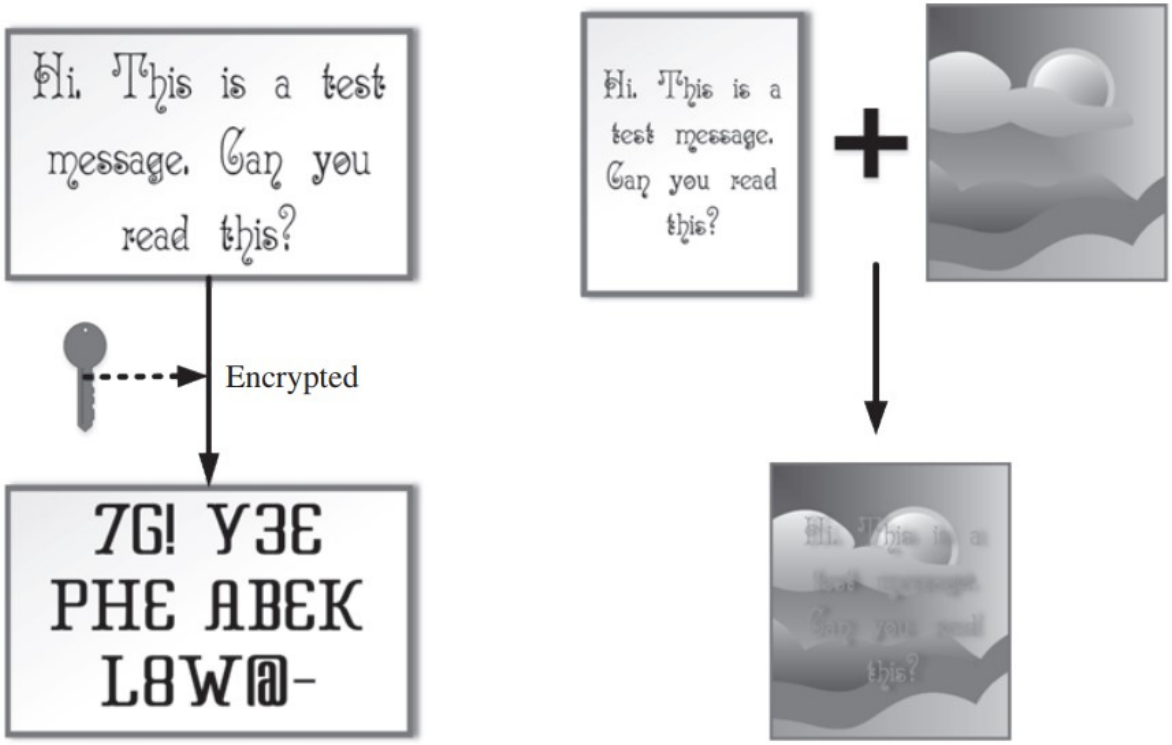
- ✓ the **unavailability** of any **information** to **authorized entities** over a network implies يعني infringement انتهاك of availability, which is one of the three members of the CIA triad.
- ✓ **Attacks** such as denial of service رفض الخدمة or distributed denial of service رفض الخدمة الموزعة directly affect the availability of information.
- ✓ These **attacks** may completely block attempts to access information or any part of it over the network by flooding the network with unscrupulous traffic. إغراق الشبكة بحركة مرور غير آمنة They may result in temporary or permanent loss of information from the network or the system.

Network Confidentiality

- Modern-day computer systems rely on تعتمد على various mechanisms to address the need of **confidentiality of information** being transmitted over the network.
- **If these confidentiality measures** are not present, as soon as the information leaves the relative safety الأمان النسبي of a user's computer and diffuses انتشارها over the network, it can be accessed by anyone with the right tools and skill-set.
- Such a scenario would make modern-day operations such as online transactions المعاملات عبر الإنترنت, e-commerce, banking, e-mails, conversations, shared online storage, and a host of other such applications useless عديمة الفائدة.

Network Confidentiality

- **Methods** and **schemes** such as cryptography and steganography **help** in achieving confidentiality over the network.



Data confidentiality schemes

Network Confidentiality

- Cryptography التشفير

  focuses on **encrypting the information** to be transmitted, making the contents unreadable without the proper decryption credentials.

- Steganography اخفاء المعلومات

  focuses on **hiding the information** in plain sight. عن أعين الجميع

Network Confidentiality

- The table below compares the **main differences between steganography and cryptography**. While **cryptography** focuses on encrypting the information to be transmitted, making the contents unreadable without the proper decryption credentials, **steganography** focuses on hiding the information in plain sight.

An overview of the differences between cryptography and steganography

Parameters	Cryptography	Steganography
What	Method of hiding information, making it readable only by the sender and the receiver.	Method of concealing information within a non-secret medium or content.
When	Used when the message being transmitted has a high chance of being intercepted and probed.	Used when the transmitted message has a very low chance of being intercepted and probed.
Why	Used in order to obscure the transmitted content so that intercepting parties may be able to capture the message but cannot read it.	Used in order to hide the very existence of the transmitted message so that no party has any idea about the presence of the message.
Where	Messages rendered unusable by encrypting its contents, which may be text, images, sounds, or videos.	Messages hidden within lowest bit of noisy images, sound files, files in computer databases, and others.
How	Key-based encryption, hashing.	Cover synthesis, cover selection.

Network Confidentiality

- These measures of incorporating and enhancing network **confidentiality** keep out unwanted eavesdroppers المتطفلين from intercepting اعتراض any information transmitted over a network.
- However, various attacks—**trojans**, **viruses**, **worms**, and others—have been engineered to overcome these confidentiality measures and access information being transmitted over the network.
- Many non-profits, as well as commercial organizations every day, keep track of newer confidentiality-compromising attack signatures worldwide and release preventive measures تطلق تدابير وقائية such as security patches تصحيحات الامان or updates to various systems.

Cryptography

- **Cryptography**, which roughly stands for **hidden writing** in Greek, is an ancient قديم science of passing secret information by **hiding its contents or making the contents obscure** غامض to the normal eye.

- **Modern-day cryptography** is found in almost all forms of networked communication and transactions.

- The **mathematically** intensive كبير and processing-heavy كثيف cryptographic **algorithms** that form the base of information encryption over networks are theoretically breakable نظريا قابلة للكسر but without any possible means وسائل or within a possible time frame ضمن اطار زمني محدد.

Cryptography

- Consider encrypted messages being transmitted between persons A and C.
- Person B (an adversary خصم) is trying to capture and get hold of the information passing between A and C.
- **Even if B gets hold of the encrypted information**, decoding it would take him **months**, if not **years**, by which time either the message would have **lost its significance**, or the encryption **key** would have **changed**, making his **attempts** to extract information futile and a **useless** venture.

Cryptography

- Cryptography is divided into **two** types:
  1) Symmetric key. المفتاح المتماثل
  2) asymmetric key. المفتاح غير المتماثل

- **Cryptography serves** the following **five** purposes in modern-day networked systems:
  1) confidentiality.
  2) authentication.
  3) integrity.
  4) nonrepudiation.
  5) key exchange.

Cryptography

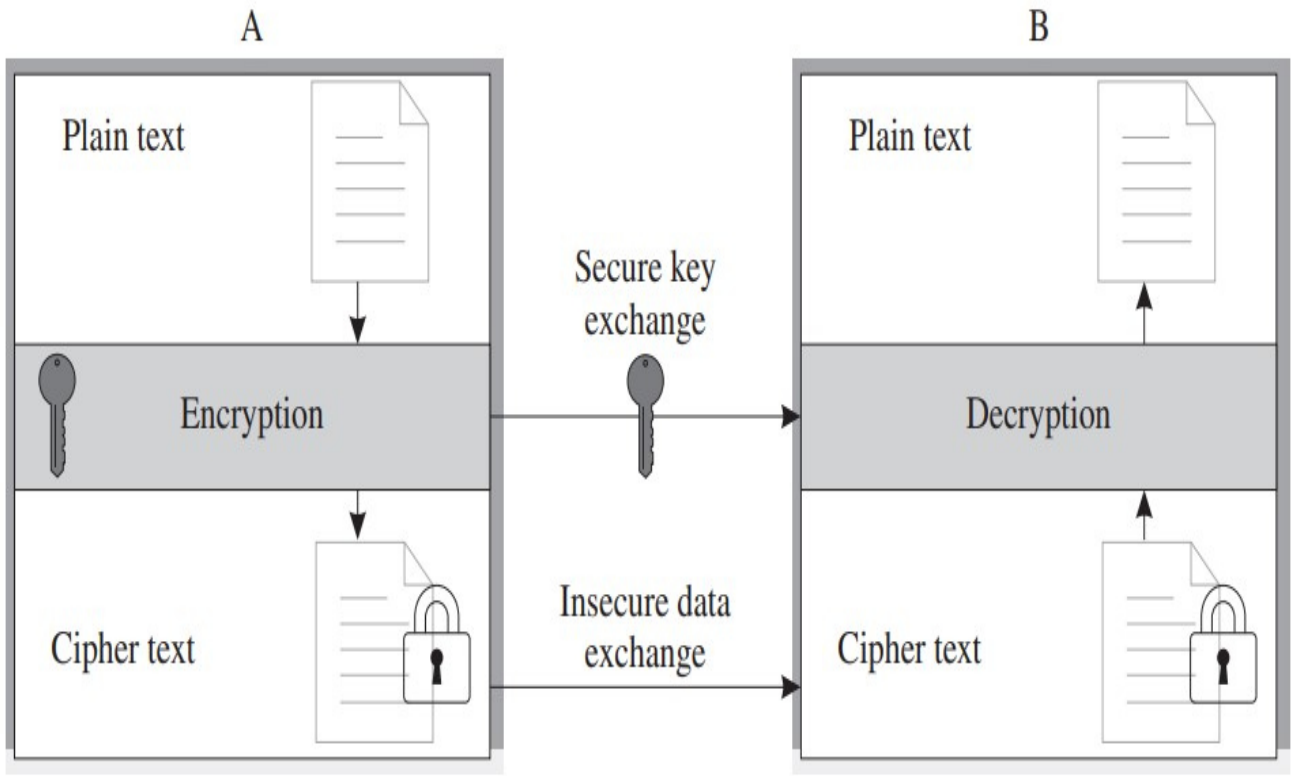
- Typically, in **cryptography**, the message to be transmitted is **referred to** as **plaintext** (P), which is **encrypted** (E) using a **key** (k) to generate a **ciphertext** (C).
- This **ciphertext** is transmitted over the network. Upon receiving the ciphertext, a **receiver** uses his key (k) to decrypt (D) the ciphertext message back to plaintext.
- The **encryption process** is denoted as C = Ek(P), whereas the **decryption** is denoted as P = Dk(C).

Symmetric key cryptography

- Symmetric key cryptography is also referred to as **secret key cryptography** التشفير بالمفتاح السري .
- This cryptographic technique **uses a single key** for both **encryption** and **decryption**.
- It finds **primary usage** يتم استخدامه بشكل أساسي in ensuring privacy and confidentiality of information في ضمان خصوصية وسرية المعلومات.

Symmetric key cryptography

- Symmetric key cryptography is also referred to as **secret key cryptography**.
- This cryptographic technique **uses a single key** for both **encryption** and **decryption**.
- It finds primary usage in ensuring privacy and confidentiality of information.



Symmetric key cryptography

- The **simplest example** of a symmetric key cryptosystem is a substitution additive cipher التشفير الإضافي الاستبدالي , where the message to be encoded (P) is modified تعديل الرسالة المراد تشفيرها by increasing the position of the alphabet by a fixed number key (k) to obtain the ciphertext (C = Ek(P)).

- The **receiver** must use the same key (k) to **decrypt** the **ciphertext** message into **plaintext**.

Symmetric key cryptography

- The table below shows the process of encrypting and decrypting a message (SECRET) using a modulo-five substitution additive cipher.

Plaintext	Corresponding alphabet number	Encryption (Key = 5)	Ciphertext	Decryption (Key = 5)	Plaintext
S	19	19 + 5 = 24	X	24 – 5 = 19	S
E	5	5 + 5 = 10	J	10 – 5 = 5	E
C	3	3 + 5 = 8	H	8 – 5 = 3	C
R	18	18 + 5 = 23	W	23 – 5 = 18	R
E	5	5 + 5 = 10	J	10 – 5 = 5	E
T	20	20 + 5 = 25	Y	25 – 5 = 20	T

Message encryption and decryption using a modulo $k(k = 5)$ substitution cipher

Symmetric key cryptography

- **The main drawback** عقبة,عيب of this system of cryptography is that the **shared key** needs to be securely shared مشاركة بشكل امن between the **sender** and the **receiver**.

- If the key falls into the hands of an adversary, the confidentiality of the encrypted message can be easily compromised مساومة .

- Additionally, these ciphers are prone to decryption عرضة للفك using exhaustive key searches بحث شاملة عن المفاتيح or brute-force attacks هجمات القوة الغاشمة .

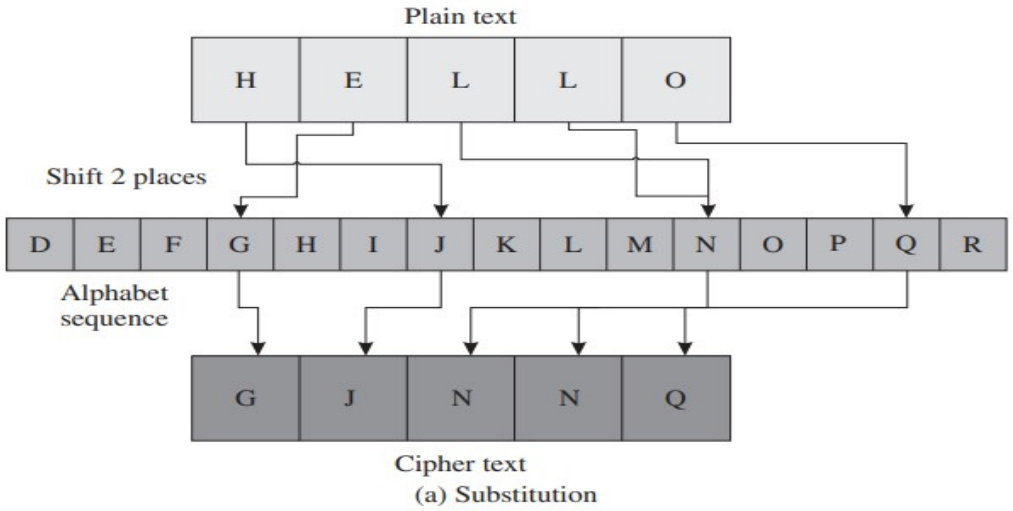
Symmetric key cryptography

- The example of a substitution cipher تشفير الاستبدال demonstrated الموضح in Table below is known as the **monoalphabetic** احادي الابجدية cipher. These ciphers have a **one-to-one mapping** between plaintext and substituted ciphertext, which makes them easy to crack كسر using brute-force attacks.

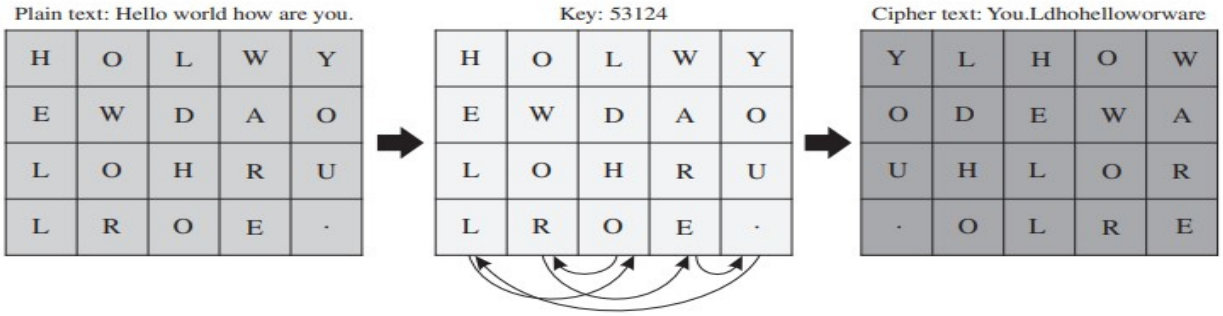
- To increase the complexity of the monoalphabetic system, **polyalphabetic** متعدد الابجدية ciphers can be used, such that the plaintext message has a **one-to-many** relation with the ciphertext.

- **Modern cryptosystems** use a variety of ciphers that fall under the category of **symmetric key ciphers** such as **substitution**, **transposition**, **block**, and **stream** ciphers.

Symmetric key cryptographic primitives اساسيات التشفير بالمفتاح المتماثل



(a) Substitution



(b) Transposition

Symmetric key cryptography

- Modern cryptosystems use a **variety of ciphers** that fall under the category of symmetric key ciphers such as **substitution**, **transposition**, **block**, and **stream** ciphers.
- These symmetric key cryptographic algorithms are compared in Table next slide.
- **Data Encryption Standard (DES)** معيار تشفير البيانات is a popular modern-day **symmetric key cryptographic** scheme. DES falls under the category of block ciphers.

A comparative overview of various cipher types

Parameter	Substitution cipher	Transposition cipher	Block cipher	Stream cipher
What	Method of encryption where plaintext is replaced by a fixed system based ciphertext. The fixed system may be single letters, letter pairs, or a combination of more than two letters.	Method of encryption where bits and chunks of plaintext are transposed or shifted from its original position to generate ciphertext.	Method of encryption using a deterministic algorithm that works on blocks or a fixed length of bits using symmetric key based transposition. Substitutions and permutations are iteratively applied to blocks, allowing this method to be highly effective in providing message security.	Method of encryption where plaintext is combined with a stream of pseudo-random cipher digit. Here, each plaintext digit is encrypted with its corresponding cipher stream digit.
Advantages	Simple to formulate and use. Substitution creates confusion.	Transposition creates diffusion. Highly effective when used with other schemes such as substitution or fractionation.	Highly suitable for providing confidentiality and authenticity of messages.	Highly robust, simple and speedy during hardware implementation.
Disadvantages	Easy to guess and crack.	Regular transpositions can be easily decrypted by anagraming and genetic algorithms.	The use of invertible functions in block ciphers eventually reveals its pseudo-random nature.	Biases in choosing keystreams may allow revelation of its non-random nature.
Types	Homomorphic, polyalphabetic, polygraphic, mechanical, one-time pad.	Rail fence, route, columnar, Myszkowski.	DES, AES, Blowfish	Synchronous, self-synchronizing

Asymmetric key cryptography التشفير بالمفتاح غير المتماثل

- Asymmetric key cryptography is also referred to as **public key cryptography**.
- This cryptographic technique uses two separate keys for encrypting and decrypting messages.
- The secret key is **personal to each user** and is referred to as the **private key**.
- The other key is known as the **public key** as it is known to all and in the public domain.
- The encryption and decryption of messages using this scheme require **both keys**.

Asymmetric key cryptography التشفير بالمفتاح غير المتماثل

- The essence جوهر of asymmetric key cryptosystems is the application of mathematical functions on numbers to generate new numbers.
  تطبيق الدوال الرياضية على الأرقام لتوليد أرقام جديدة.
- These **mathematical functions** are generally **one-way functions**, دوال أحادية الاتجاه where the **forward** function is **easy** to compute, but the **inverse** is very **complicated**, if not impossible.
- It is interesting to mention that both the **keys are unrelated to one another**, and the knowledge of one does not compromise or give away any hint about the other key.
- This scheme is in contrast to symmetric key cryptosystems, which mainly rely on substitution and permutation الاستبدال والتبديل of symbols for encrypting messages.

Asymmetric key cryptography التشفير بالمفتاح غير المتماثل

- From an operational point of view, unlike symmetric ciphers which directly use symbols يستخدم الرموز بشكل مباشر , in asymmetric key cryptography, the plaintext message has to be **encoded into integers** before encrypting them يتعين تشفير رسالة النص العادي إلى أعداد صحيحة قبل تشفيرها.

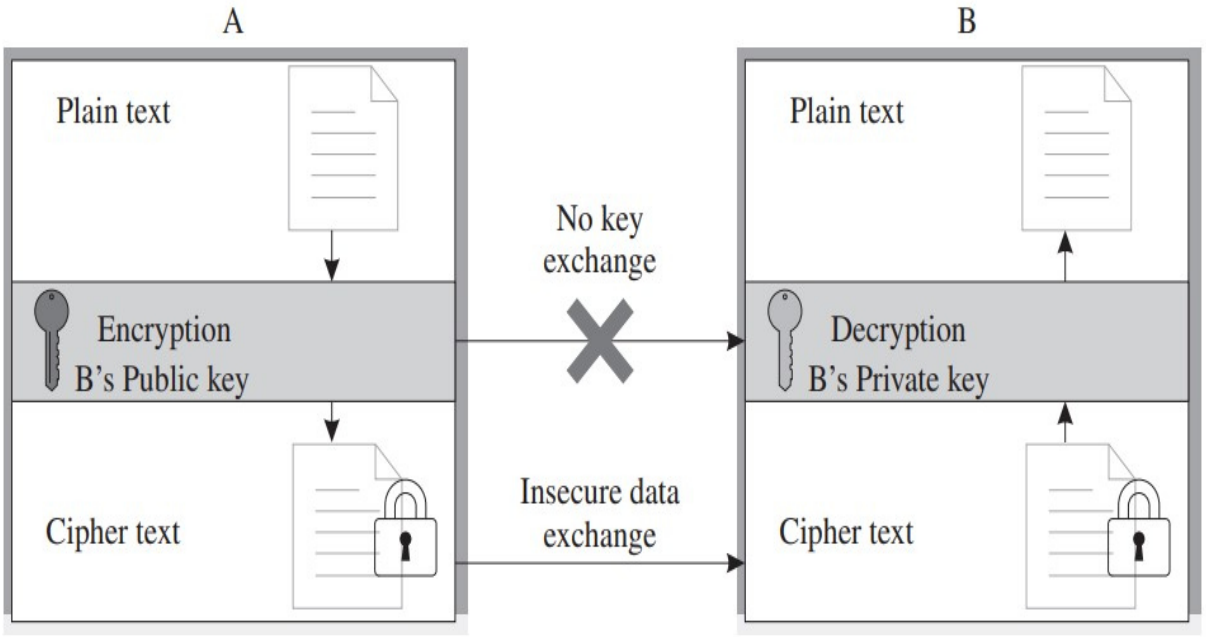
- Similarly, for the **reverse process** of decryption, the decrypted message is in the form of integers, which have to be mapped back to symbols to generate the plaintext message.

A comparative overview of symmetric and asymmetric key cryptography

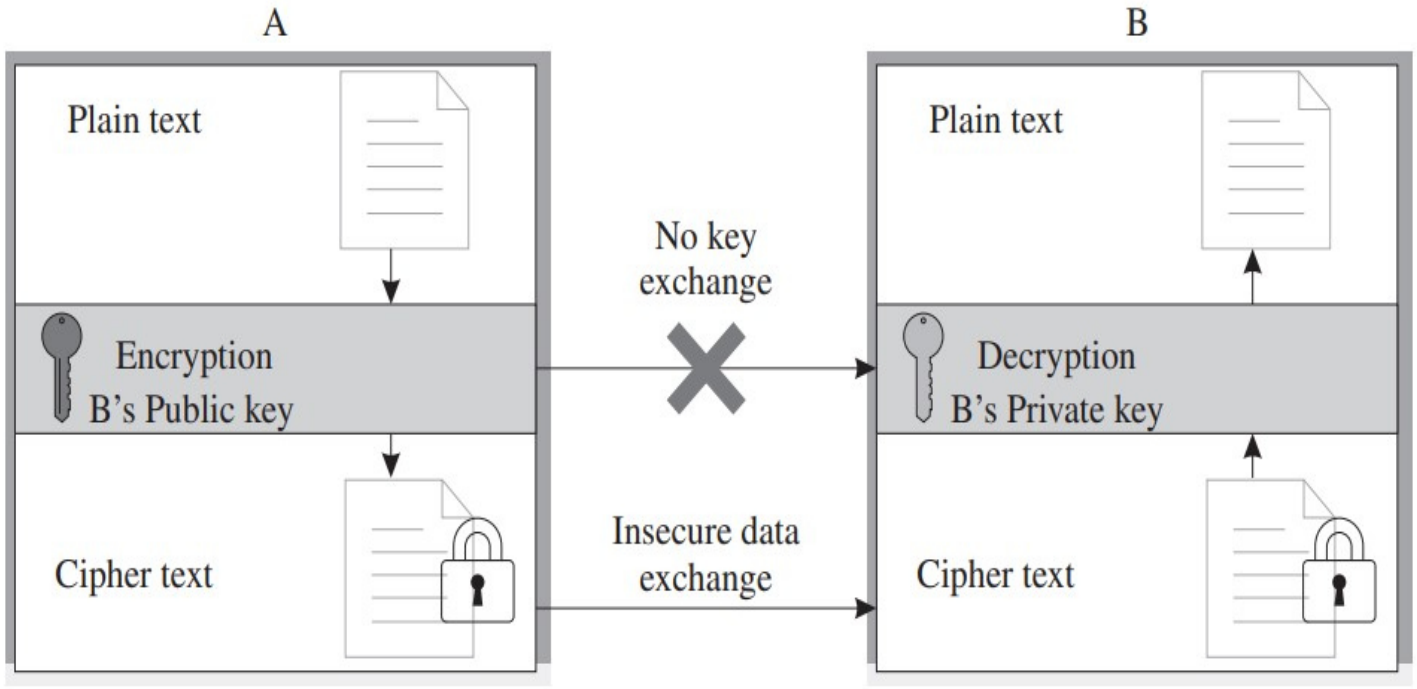
Parameter	Symmetric key	Asymmetric key
Encryption/ decryption keys	Uses same key for encryption and decryption; Also called secret key cryptography.	Uses different keys for encryption and decryption; Also called public key cryptography.
Number of keys	For n users, $n(n-1)/2$ key pairs are required.	For n users, $2n$ keys required.
Key generation	Randomly generated and simple.	Complex, generally large prime numbers are used.
Security of key	Keys need to be secured.	Key security not necessary.
Example	AES-126	RSA

An asymmetric key cryptographic mechanism

- For example, consider that A intends to send a message to B over a non-secure network channel. A encrypts the message using B's public key.
- This encrypted message can only be decrypted using B's private key.
- The encryption process at A can be denoted as **CB = EB(k1)(P)**.
- At B, the decryption process to extract the plaintext message from the ciphertext is denoted as **P = EB(k2)(CB)** such that **k1**, **k2** are respectively the **public** and **private** keys of B.
- **EB(k1)** is used only for **encryption**, whereas **EB(k2)** is used for **decryption** only.



An asymmetric key cryptographic mechanism



An asymmetric key cryptographic mechanism

- Contrary to popular belief, the symmetric key and asymmetric key schemes complement one another and are used in conjunction with one another in a vast number of applications.

- For example, the shared key in symmetric key schemes is generally transmitted to the receivers using asymmetric key schemes. **Rivest–Shamir–Alderman (RSA) algorithm** is a popular asymmetric key cryptographic scheme.

Message Integrity and Authenticity

- The types of information being transmitted over networks worldwide are huge.
- With the increase in acceptance of network-based solutions, the challenges in ensuring the **quality of service** and **safety** are increasing day by day.
- The massive **application** types give rise زادت to various issues regarding **quality** of **service**.
- The concept of confidentiality is not inherent متأصل,ملازم for all message types being transmitted over the networks.
- There are **operations** that focus more on the **integrity** of the transmitted message, rather than on its **confidentiality**.

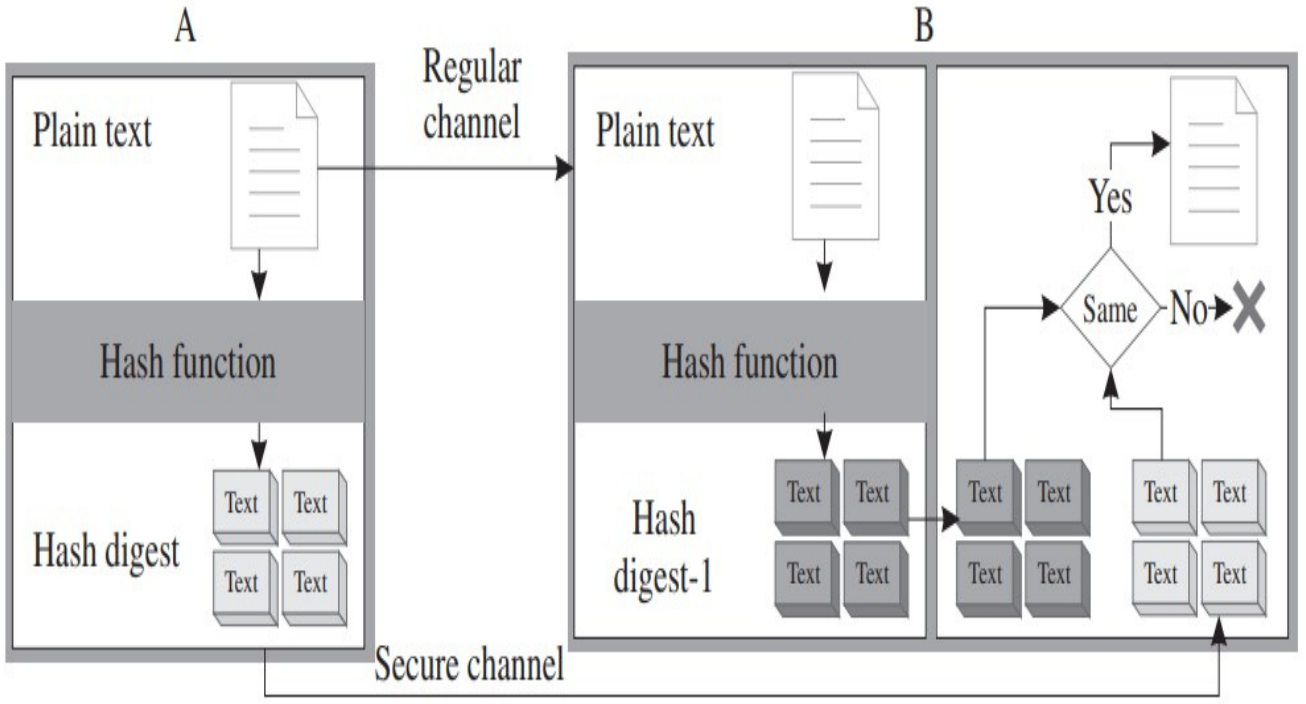
Message Integrity and Authenticity

- As a **simple example**, if we consider an **online banking system**, the account **login** and **powers of transaction** rely heavily on various **security** and **confidentiality** measures.

- However, in a blockchain-based banking system, the implications of message integrity far outweigh the impact of message confidentiality so much so that all transactions are transparent in a blockchain system, yet they are immune to tampering العبث and fraudulent manipulations التلاعب الاحتيالي.

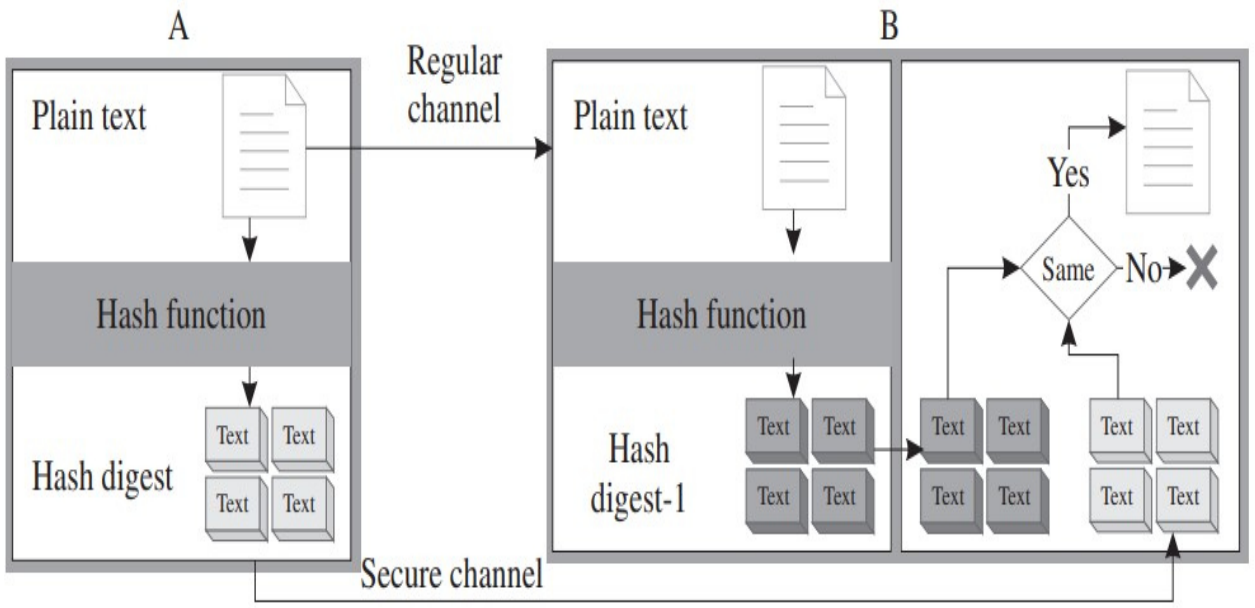
Message Integrity and Authenticity

- Newer models of the economy are being planned upon **blockchain-based systems**. The most **popular scheme** of ensuring message **integrity** over a network is **hashing**.
- Some of the more popular **hashing techniques** include algorithms such as SHA and MD5.
- A hash function applied on a message **creates a digital fingerprint** for that message, which is referred to as its **digest**.



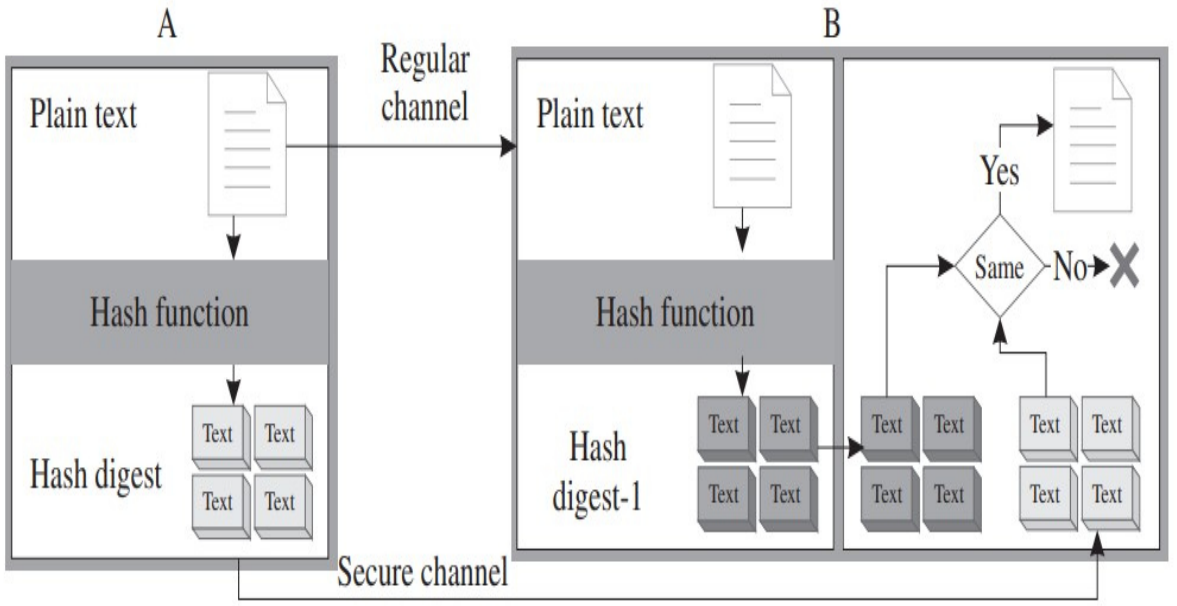
Message Integrity and Authenticity

- Before transmission of the message, a **message digest** is securely transmitted to a receiver.
- The message can be transmitted in any manner, and over any channel—both secure or insecure.
- The **receiver**, upon receiving this message generates its hash digest and **compares it** to the one **received earlier**.
- The message is considered tamper-free only if both of these digests match.



Message Integrity and Authenticity

- The authenticity of a message (whether the sender of the message is the same person as claimed by the message) is ensured by using a **pre-shared key** between the **sender** and the **receiver**.
- The pre-shared key is applied to the hashing function to generate a **message authentication code (MAC)**, which is transmitted along with the message.
- The **receiver**, upon **receiving** the message generates another **MAC** using the **pre-shared key**.
- If this newly generated MAC matches the one received over the network, the **authenticity** of the message is **ensured**.



Message Integrity and Authenticity

- The **main advantage** of this method is that

✓ there is **no need for a separate secure channel** for transmitting message digests,

✓ in addition to the feature of **both integrity and authenticity check** of the message.

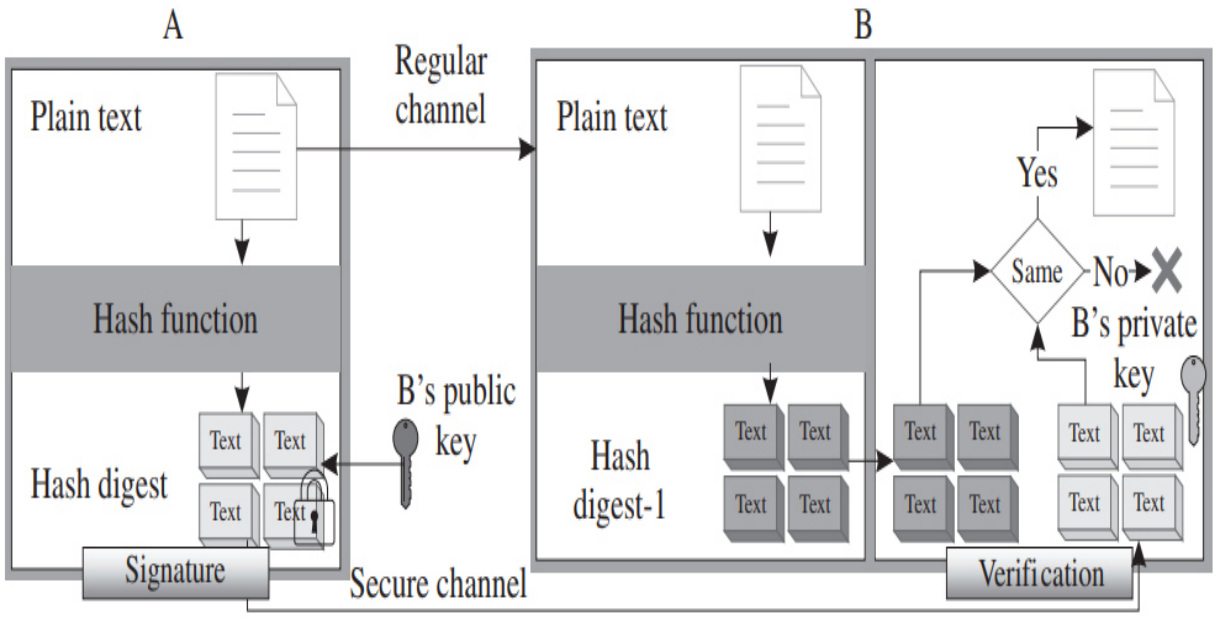
- However, **on the flip-side**, if the pre-shared key is compromised, this **authentication** method **fails**.

Digital signatures

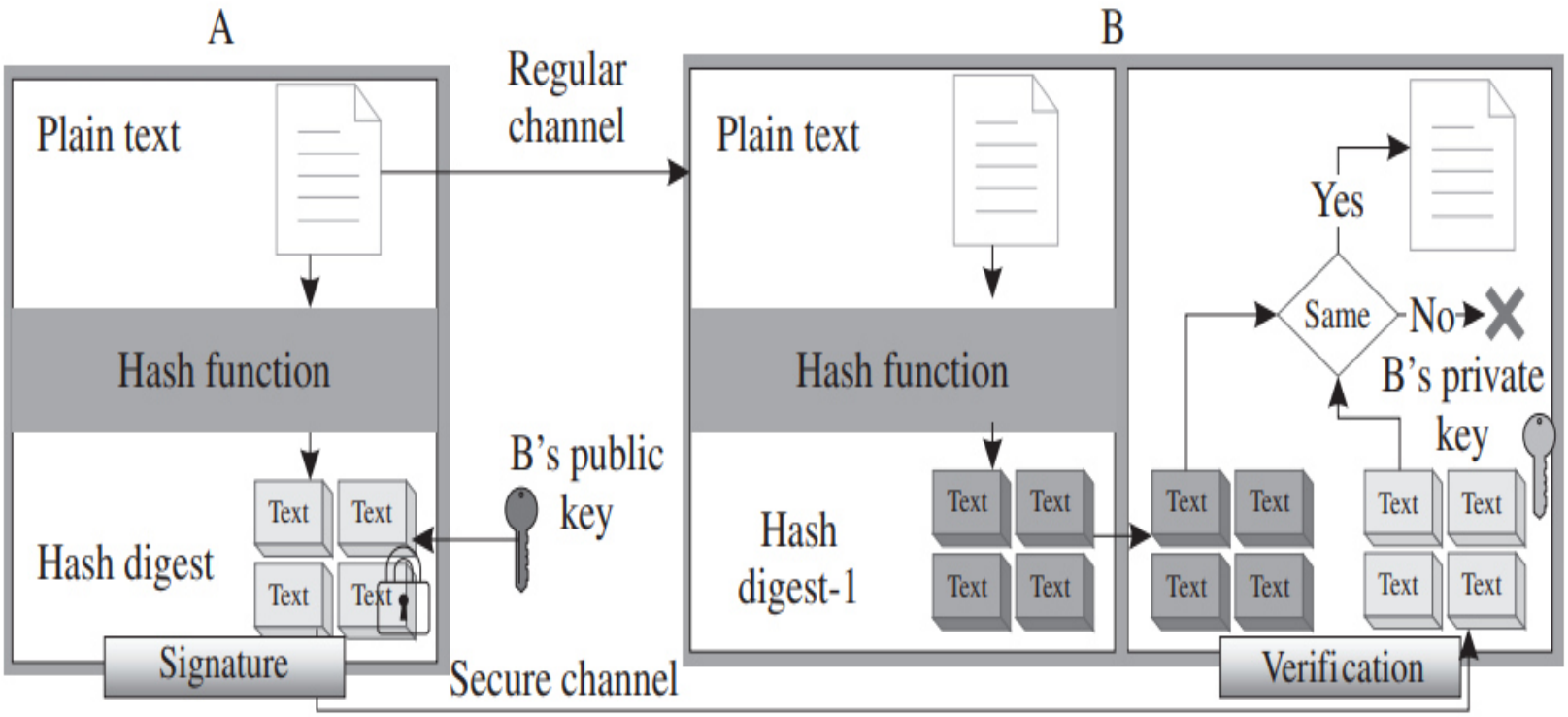
- A **digital signature** is functionally similar to paper-based signatures, which are primarily used to bind a person/user/signatory with the content of a message.
- In digital signatures, the binding is verifiable by the receiver of the message or even third parties, as it mainly authenticates the message.
- The **method of digitally signing** a message is akin to **public key cryptography**. Each signatory has a **public** and a **private** key.
- The **private key** is used for signing the message and is referred to as the **signing key**, whereas the **public key** is used for verifying the message and is known as the **verifier key**.
- **Digital signatures** ensure that a message complies with the features of **authenticity**, **integrity**, and **non-repudiation**.
- **RSA** is a commonly used **algorithm** for digital signatures.

A mechanism for digital signing of electronic documents

- Suppose, A is the signatory and B is a verifier at the two ends of a network. A converts the message to be sent to B into a hash digest by passing it through a hash function. The hash digest is then signed-on by A's private/signing key.
- This signature is transmitted with the data to B.
- Upon receiving this signed message, the verifier applies A's public key on the message to obtain the message hash digest.
- B independently hashes the data received with the signature. If the independently generated hash digest is similar to the one that has been obtained by using A's public key, the signature of A is verified by B.



A mechanism for digital signing of electronic documents



Digital signatures

- The **authentication feature of digital signatures** can be grouped into two broad categories:

  1) Entity authentication.
  2) message authentication.

✓ **Entity authentication** is often referred to as **peer entity authentication**. It is used for binding a person to a message. An entity authentication scheme assures the receiver of a message about the sender's participation in generating the message.

✓ In contrast, **message authentication**, which is also known as **message origin authentication**, is a means to ensure receivers of a message that the message has not been tampered with during its transmission from the sender.

Digital signatures

- **Digital signatures** are categorized into **four** classes:

1) Certified signatures.
2) Approval signatures.
3) Visible digital signatures.
4) Invisible digital signatures.

Key Management

- **Key management** is one of the most crucial aspects of modern-day cryptography and deals with the administration of cryptographic keys.
- **Generation**, **distribution**, **storage**, **safety**, and **distribution** of keys are the major functionalities of a key management system.
- As cryptographic keys can be both **symmetric** as well as **asymmetric**, the management of these keys to provide reliable services is a very challenging, yet important task in modern-day cryptographic communications and networking.
- The usability and efficiency of any modern-day cryptosystem are as good as the **key management system**.
- Supposing that despite using state-of-the-art cryptographic systems, the keys have to be somehow transmitted to the receiver of the message.
- At this point, the keys are the most vulnerable to hijacking or unauthorized capture. If the key itself is compromised, the layer of cryptographic encryption is automatically compromised and breached.

Key Management

- A **key management system** must be robust enough to handle the **challenges** of scalability, security, availability, heterogeneity, and governmental policies. The overview of these challenges are outlined as follows:

1. **Scalability**: The key management system **must be able to scale its operations on demand**. An increase in the number of users must be easily managed by the system, in turn allowing for the storage and management of a large number of keys.
2. **Security**: The **stored keys and credentials** must be protected from unauthorized use or attacks, allowing the cryptosystem to function uncompromised.
3. **Availability**: The keys and the management servers **must be accessible by authorized users** at all times.
4. **Heterogeneity**: The use of **multiple databases**, a **variety of standards**, and **applications** must be supported.
5. **Governmental Policies**: The system must be robust enough to accommodate governmental or institutional regulations and policies at very short notice. This should also enable policy-driven management of user access and privacy of users. يكون النظام قويًا بما يكفي لاستيعاب اللوائح والسياسات الحكومية أو المؤسسية في غضون مهلة قصيرة جدًا

Key Management

- A modern-day **key management system** has the following **basic components**:

1) Inventory.
2) Key exchange.
3) Key use.
4) Key storage.

- These components and their functionalities can be enumerated as follows:

i. Inventory: It is responsible for **creating** and **maintaining** a concise list قائمة مختصرة of all the crypto keys, their permissions, access rights, locations, and user mappings. The inventory is also responsible for managing certificate lists from a multitude of certifying authorities. The key inventory should be designed to take immediate measures such as **replacing keys in case of breach of security**.

Key Management

ii. Key exchange: Key exchange is a crucial part of the key management system as any slip up خلل او خطأ in the security of keys during transfer would compromise the purpose of the key management system. Modern-day cryptosystems use **techniques** such as **smart-card based key exchange**, **encrypting the key with another key**, **encrypting the symmetric key with an asymmetric key**, and others.

ii. Key use: The use of key-based encryption does not guarantee cent percent defense against attackers. The encryption, as mentioned previously, only buys the communicating parties enough time so that the message becomes obsolete, causing the key breaking exercise to become redundant. In most cases, symmetric key cryptosystems change the key after each message. **This feature is highlighted by the key lifetime**. If the **same key is used for a very long time, the chances of an attacker gaining access to personal encrypted communication using these keys rapidly rise**. The key management systems also manage the key lifetimes.

Key Management

iv. Key storage: The **secure storage of keys** ensures the success of intrusion-free communication. The distributed storage of keys has various security mechanisms in place for user access passwords to ensure **no unauthorized access to the keys**.

Internet Security

- **Internet security**, as the name suggests, **focuses more on** the security of Internet accesses and devices on the Internet; it is not only restricted to simple networks.
- As the Internet is a huge and complex place made up of billions of devices and users, the chances of malicious or ill-intended breach of security becomes inevitable if the Internet is not secure.
- Attacks such as spyware, malware, Trojans, key-loggers, viruses, worms, ransomware, and other such attacks necessitates the presence of Internet security.
- In contrast, a **regular network may not be exposed to such attacks or threats**.
- **For example**, a small organizational network, which is isolated from the Internet and has networked devices within the purview of its organization only, will be faced by **attacks only if someone from the inside initiates** it; this type of attack is easy to track and initiate timely counter-measures.

Internet Security

- The **domain of Internet security mainly revolves around** تدور حول the **three** TCP/IP (transmission control protocol/Internet protocol) layers:

1) Network layer.
2) Transport layer.
3) Application layer.

Network layer security

- The **network layer security** encompasses تتضمن,تشمل security mechanisms and measures between two networked devices.
- The devices can be **networked computers**, **routers**, **servers**, and **others**.
- **This layer supports security** for both **TCP**, as well as **UDP** (user datagram protocol) **packets arriving and going out of** the networked devices.
- One of the most **common examples of network layer security protocol** is **IP Security (IPSec)**, which provides **packet-level security** at the network level.

Network layer security

- IPSec itself consists of two modes:

1) Transport mode.
2) Tunnel mode.

1. The transport mode is responsible for **providing security only to the packet payload**; it does not cover the IP header of the packet.

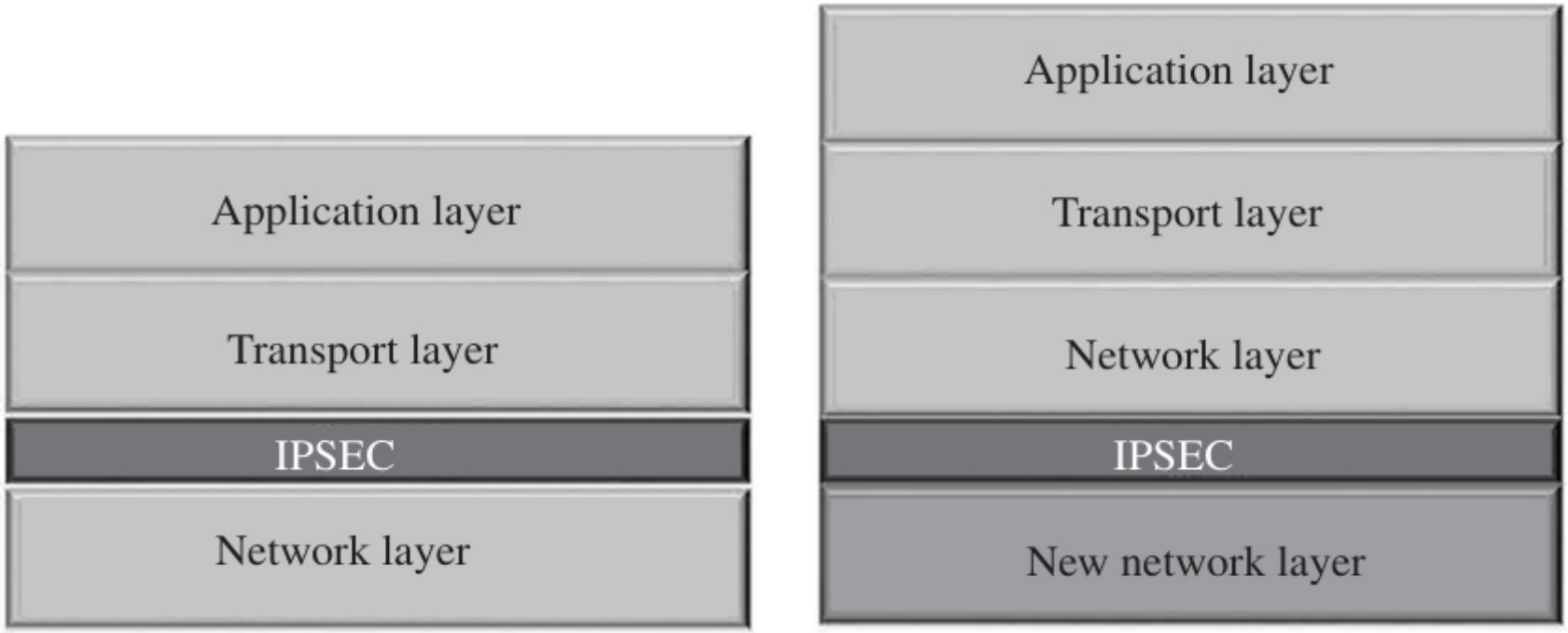
2. the IPSec tunnel mode **protects both the header as well as the payload** by encapsulating it in a new payload and adding a new IP header to the encapsulated packet.

Network layer security

- It is worthwhile to mention that, in the **transport mode**, the **IPSec layer** is logically positioned **between** the network and the transport layers of the TCP/IP stack.
- In contrast, the **IPSec layer** in the **tunnel mode** is positioned **below** the network layer and above a newly created network layer.
- Additionally, **IPSec** defines **two** well-known **security protocols**:

1) Authentication header (AH).
2) Encapsulating security payload (ESP).

IPSec modes


Application layer
Transport layer
IPSEC
Network layer
Application layer
Transport layer
Network layer
IPSEC
New network layer

Network layer security

- These two protocols are tasked with providing security authentication and encryption of packets **at the IP level**.
- Similar to the features of cryptographic techniques, **IPSec provides** for the characteristics of access control, message integrity, entity authentication, and confidentiality.
- Another **essential aspect of IPSec** is known as the security association (SA).
- SA is responsible for establishing logical connection credentials between two communication devices at the network level. It changes the connectionless nature of the IP services to a **security-enabled connection-oriented service**.

Transport layer security

- The transport layer security is based on **utilizing the services of TCP to establish a connection-oriented protocol**. This is why UDP based protocols are not supported by transport layer security mechanisms.
- The **transport layer security** protocols first encapsulate the packets in their packets, followed by encapsulation of TCP over the new packets.
- The **transport layer security services** logically exist between the TCP/IP stack's transport and application layers. These security protocols mainly aim to provide the features of **authenticity**, **confidentiality**, and **integrity** to client-server systems.

Transport layer security

- Two of the most **popular transport layer security protocols** are as follows:

1) Secure socket layer (SSL).
2) Transport layer security (TLS).

1) Secure socket layer (SSL)

- In SSL, a client communicating with a web server (or website) connects to it through a browser. **The browser** requests for the server's credentials, against which an SSL certificate with the server's **public key is sent**; this is verified against a **list of trusted certifying authorities** by the **browser**.

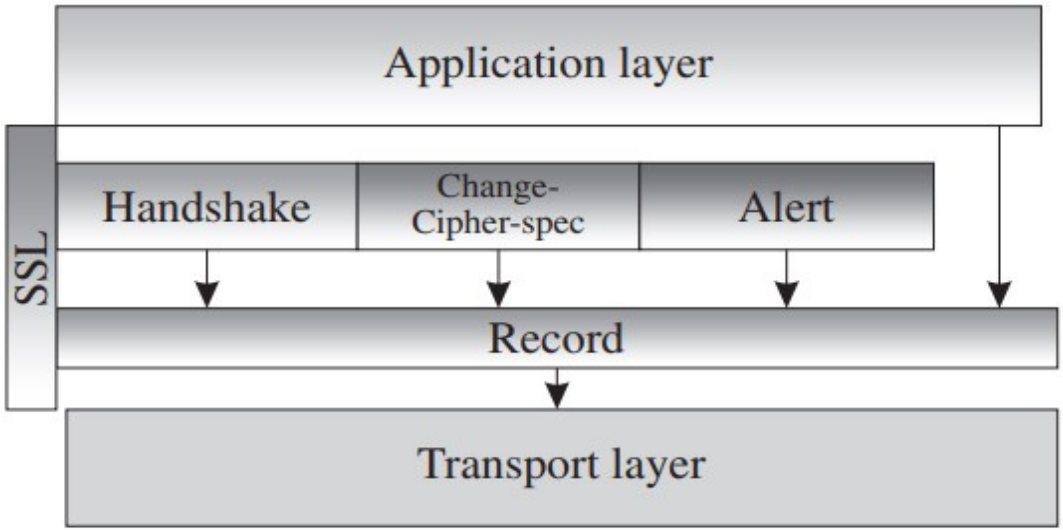
- Additionally, the validity and authenticity of the certificate are verified. Upon validation of the server's certificate, **the browser sends back** a session key (symmetric) using the **server's public key**.

- Subsequently, the **server** decrypts the session key and **sends back an acknowledgment for session establishment**. Upon establishment of the session between the **server** and the **browser**, the **session key** is used to encrypt the communication between them.

1) Secure socket layer (SSL)

- The **SSL protocol** is made up of the following **four** protocols.

1) Handshake Protocol.
2) ChangeCipherSpec Protocol.
3) Alert Protocol.
4) Record Protocol.



Position of the SSL protocol

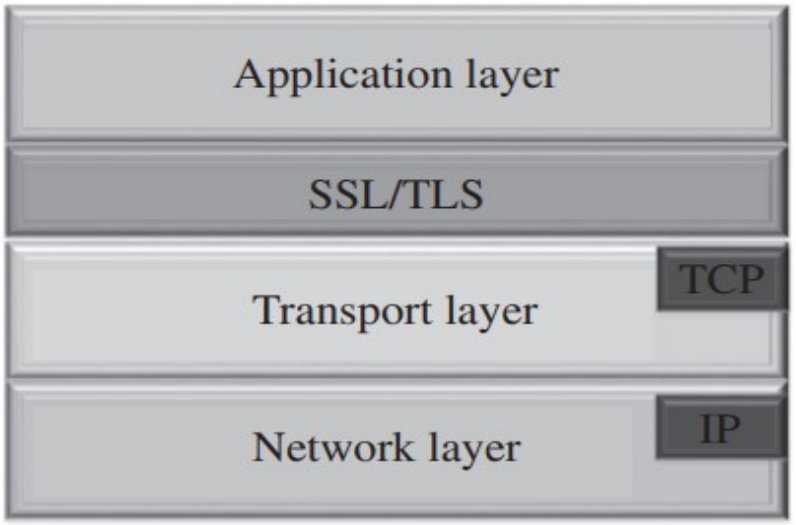
1) Secure socket layer (SSL)

1) Handshake Protocol: This protocol is responsible for **establishing client–server/ server–client connections**, negotiating encryption algorithms, and authenticating the communicating entities.
2) ChangeCipherSpec Protocol: This protocol is **used to change encryption settings that might have been set during the handshake process**. A message notifies the client and server about the need for a change in encryption; this is handled by the changecipherspec protocol.
3) Alert Protocol: This protocol is **used for notifying the communicating systems of alerts and unusual conditions** during communication between the entities.
4) Record Protocol: This protocol is responsible for **breaking down the data from the upper layers into fixed sizes and compressing them.** Additionally, it is responsible for **encrypting messages** from the **upper** layers coming down to the **lower** layers.

2) Transport layer security (TLS)

- The TLS, which is a **successor of the SSL**, resides in the application layer and is **functionally very similar to the SSL**. It is **composed of two layers.**

1) TLS Record Protocol.
2) TLS Handshake Protocol.



Position of the transport layer security protocol

2) Transport layer security (TLS)

1) TLS Record Protocol: This provides connection security.

2) TLS Handshake Protocol: This allows client-server authentication and exchange of encryption algorithms and keys.

Application layer security

- Application layer security protocols are designed to reside wholly within the application layer and **provide security to applications** such as e-mails, which is in contrast مغاير to network and transport layer security protocols.
- **Two** well-known application layer security protocols are as follows:

1) Pretty good privacy (PGP).
2) Secure/multipurpose internet mail extension (S/MIME).

- Again, unlike the transport and network layer security protocols, application layer protocols must take into consideration that some communications can be **one time or even unidirectional** لمرة واحدة أو حتى أحادية الاتجاه .
- For example, the act of sending e-mails may or may not elucidate a response mail from the receiver.

Firewall

- Firewalls are **network security mechanisms** that monitor and grant وافق access to clean network traffic while blocking unscrupulous or malicious traffic.
- The firewall's **access control policies** are **governed by a set of rules**, which help them decide **what to block and what to allow** through the network.
- The **mechanisms** of the firewall can be **hardware-based**, **software-based**, or **both**.

Acknowledgment

- **These lecture slides are based on:**

1) **Chapter 1(P 3-10)** from the book "Internet of Things A to Z Technologies and Applications" by Qusay F. Hassan (Editor) (z-lib.org)
2) **Chapter 1(P 23)** Internet of Things A Hands-On Approach by Arshdeep Bahga, Vijay Madisetti (z-lib.org)
3) **Part I (section 1.3 p7-9)** from the book Fundamentals of IoT Communication Technologies
4) **Article** (Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into **the building blocks**, component interactions, and architecture layers. Procedia computer science, 132, 109-117).
5) **Chapter 1(P 3-19)** from the book "Introduction to IoT" by (Sudip Misra, Anandarup Mukherjee, Arijit Roy)

INTERNET OF THINGS (IoT)

END OF LECTURE (2)

Keep connected with the classroom

btukscx

THANK YOU FOR YOUR ATTENTION