Basics of Network Security

Computing for Internet of Things

Dr. Arijit Roy

Overview

Introduction

- The range of operations dependent on computers, computer networks, and the Internet is vast.
- Healthcare, banking, governance, security, military, research, power, agriculture, and others are nowadays largely dependent on networked systems.
- The huge implications of the failure of one of these domains due to computer-based security lapses are undeniable. This necessitates 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 which are not connected to a network or the Internet.
- The main aspects of securing a system are – security, privacy, and authenticity.

Network Attacks

- The various forms of network attacks are classified into two broad categories
  1. General cyber threats
  2. Threats to web databases
- Attacks such as authentication violation, non-repudiation, Trojan horses, viruses, fraud, sabotage, denial of service, and even natural disasters are categorized as general cyber threats.
- Attacks such as access control violations, integrity violations, confidentiality violations, privacy violations, authenticity violations, and identity thefts are categorized as threats to web databases.
- Most of the commonly available tools for security are anti-viruses, anti-malware, anti-spyware, and firewalls.

Attack Prevention

Some basic practices on the computer or over networks can easily ward-off most of the security threats. Some of these practices are:

1. Choosing passwords wisely so that it is a mixture of alphabets (preferably, both uppercase and lowercase characters), numbers, special characters, and changing them periodically.
2. Avoiding sharing of passwords or credentials, or storing/recording them in an obvious manner such as on a piece of paper, or on your desktop.
3. Keeping systems up to date and patched on time.
4. The use of anti-virus, anti-spyware and firewalls tend to reduce the scope of threats.
5. Avoiding download of suspicious attachments and clicking on random links or pages.

Security

Security in networks and computer systems work with the following three goals:

1. Confidentiality
2. Integrity
3. Availability

This is often referred to as the CIA triad.

Confidentiality

- Confidentiality pertains to protection of stored and transmitted information over the network in such a manner that the information itself is concealed and protected from unauthorized access.
- Attacks such as snooping and traffic analysis pose a direct threat to the confidentiality of information.
- The breach of confidentiality can occur if the nature of information, information itself, or the address of the sender or receiver is revealed to an unauthorized third party.

Integrity

- The integrity of any stored or transmitted information may arise due to both intended or unintended actions.
- Whenever changes are made to any information in a system or network by unauthorized entities, a breach of system or network integrity is presumed.
- Attacks such as replays and modification 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.

Availability

- The unavailability of any information to authorized entities over a network implies infringement of availability, which is one of the three members of the CIA triad.
- Attacks such as denial of service or distributed denial of service directly affect the availability of information.
- These attacks may completely block attempts to access the information or any part of it over the network by flooding the network with unscrupulous traffic.
- These attacks may result in temporary or permanent loss of the information from the network or the system.

Confidentiality Schemes

(a) Cryptography

(b) Steganography

Figure: Data confidentiality schemes

Cryptography

- Cryptography, which roughly stands for *Hidden Writing* in Greek, is an ancient science of passing secret information by hiding its contents or making the contents obscure to the normal or unsuspecting eyes.
- Modern-day cryptography is found in almost all forms of networked communication and transactions.
- The mathematically intensive and processing heavy cryptographic algorithms, which form the base of information encryption over networks are theoretically breakable but without any possible means or within a possible time-frame.
- Broadly, cryptography is divided into
  1. Symmetric Key
  2. Asymmetric Key
- Cryptography serves the following five purposes in modern-day networked systems – 1) Confidentiality, 2) Authentication, 3) Integrity, 4) Non-repudiation, and 5) Key exchange

Ciphers

- Modern cryptosystems use a variety of ciphers, which fall under the category of symmetric key.
- The simplest example of a symmetric key cryptosystem is a substitution additive cipher, where the message to be encoded (P) is substituted by increasing the position of the alphabet by a fixed number key (k) to obtain the ciphertext ($C = E_k(P)$).
- The Data Encryption Standard (DES) is a popular modern-day symmetric key cryptographic scheme. DES falls under the category of block ciphers.

Symmetric Key Cryptography

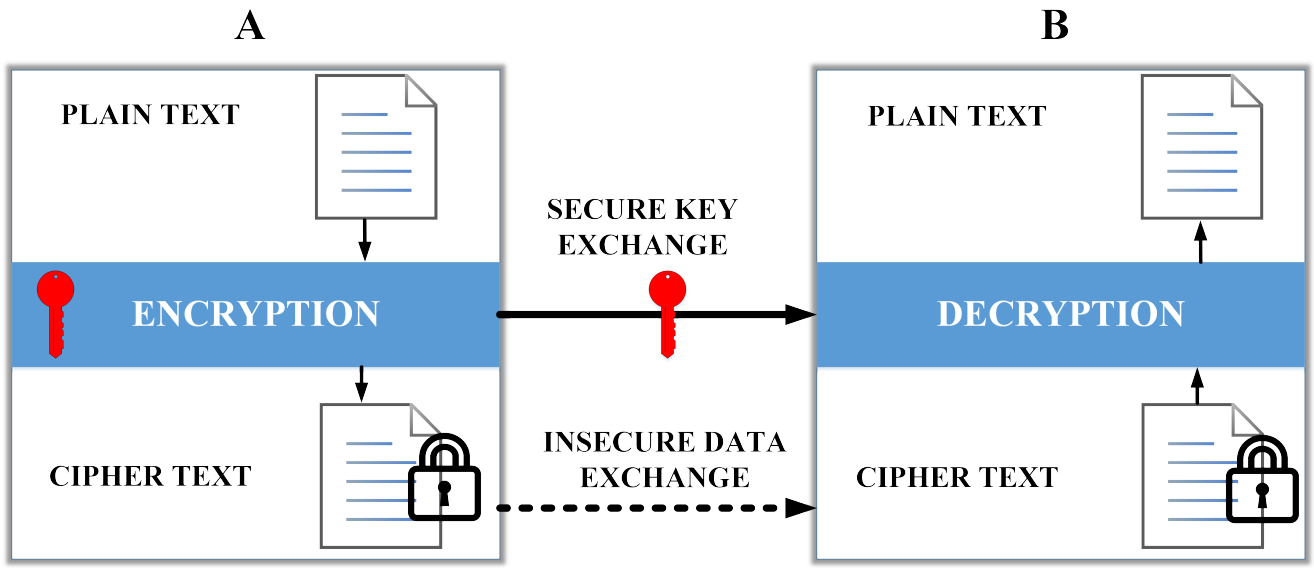


Figure: A symmetric key cryptographic mechanism

Asymmetric Key Cryptography

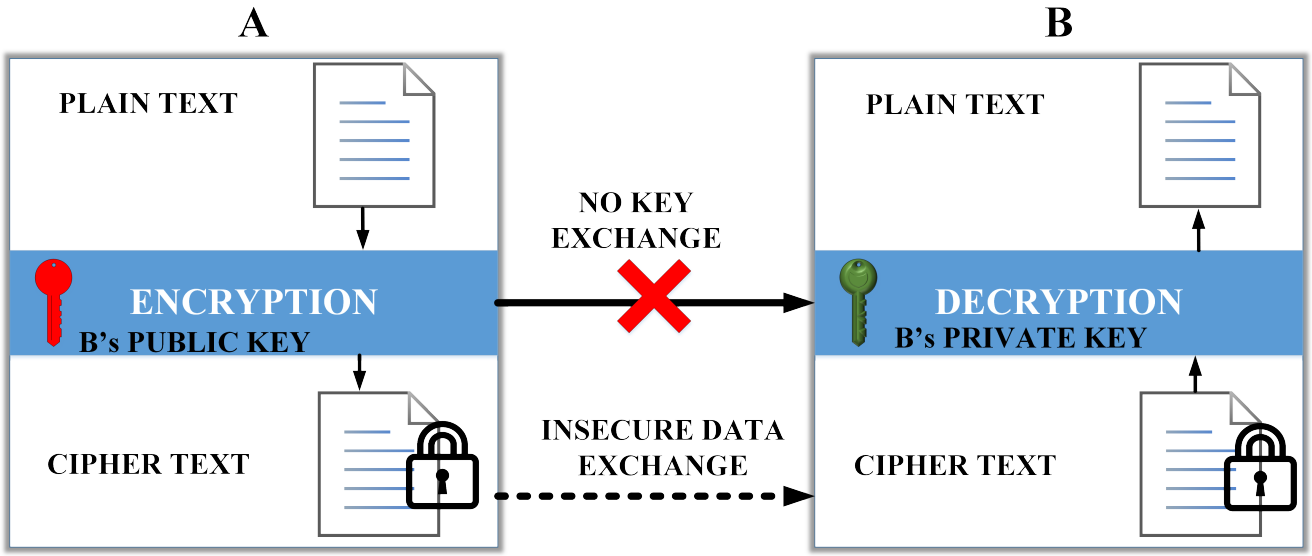


Figure: An asymmetric key cryptographic mechanism

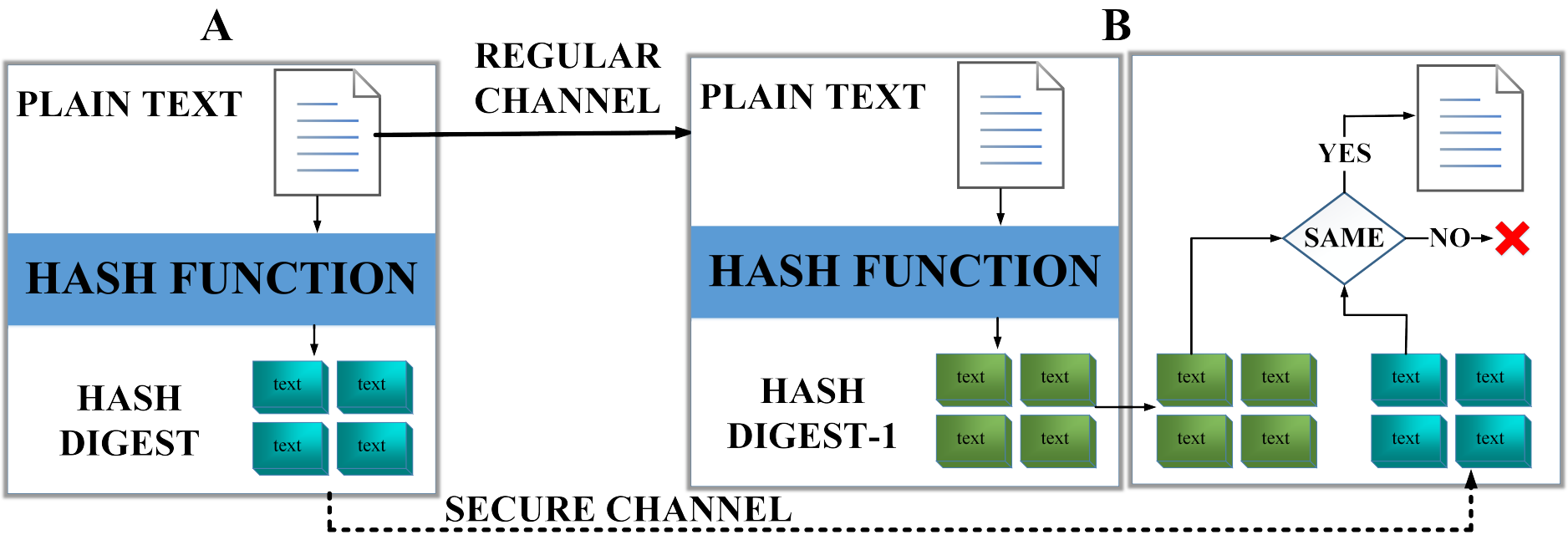
Need for Message Integrity

- The types of information being transmitted over networks worldwide are huge.
- With the increase in widespread 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 to the various quality of service aspects.
- The concept of confidentiality is not inherent for all message types being transmitted over the networks.
- There are operations which focus more on the integrity of the transmitted messages, rather than on its confidentiality.
- 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 and fraudulent manipulations.

Hashing

- The most popular scheme of ensuring message integrity over a network is the use of hashing.
- Some of the more popular hashing techniques include algorithms such as SHA, MD5, and others.
- A hash function applied on a message creates a digital fingerprint for that message, which is referred to as its digest.
- 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.

Hashing


A
B
PLAIN TEXT
REGULAR CHANNEL
PLAIN TEXT
HASH FUNCTION
HASH FUNCTION
HASH DIGEST
HASH DIGEST-1
text
YES
SAME
NO
SECURE CHANNEL

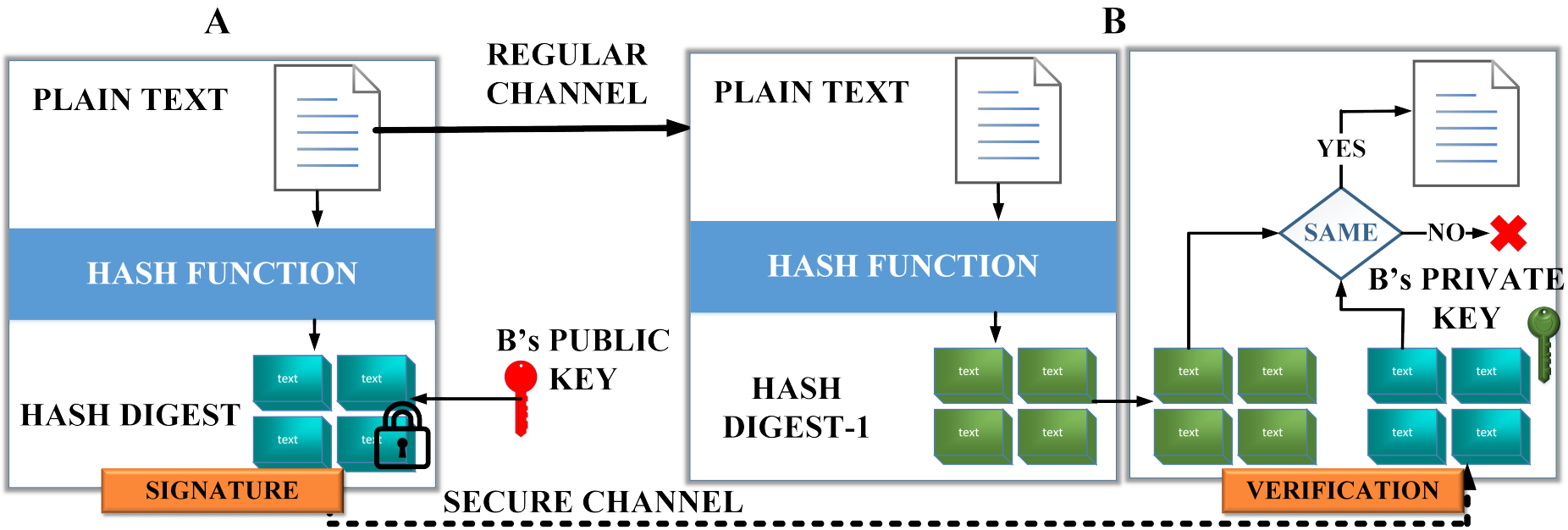
Hashing

- The authenticity of a message (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 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, only then the authenticity of the message is ensured.
- 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 is primarily used to bind the content of a message with a person/user/signatory.
- 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 similar to the public key cryptography. Each signatory has a public and a private key.
- The private key is used for signing the message as 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.

Digital Signatures



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 the 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, and 4) Invisible digital signatures.

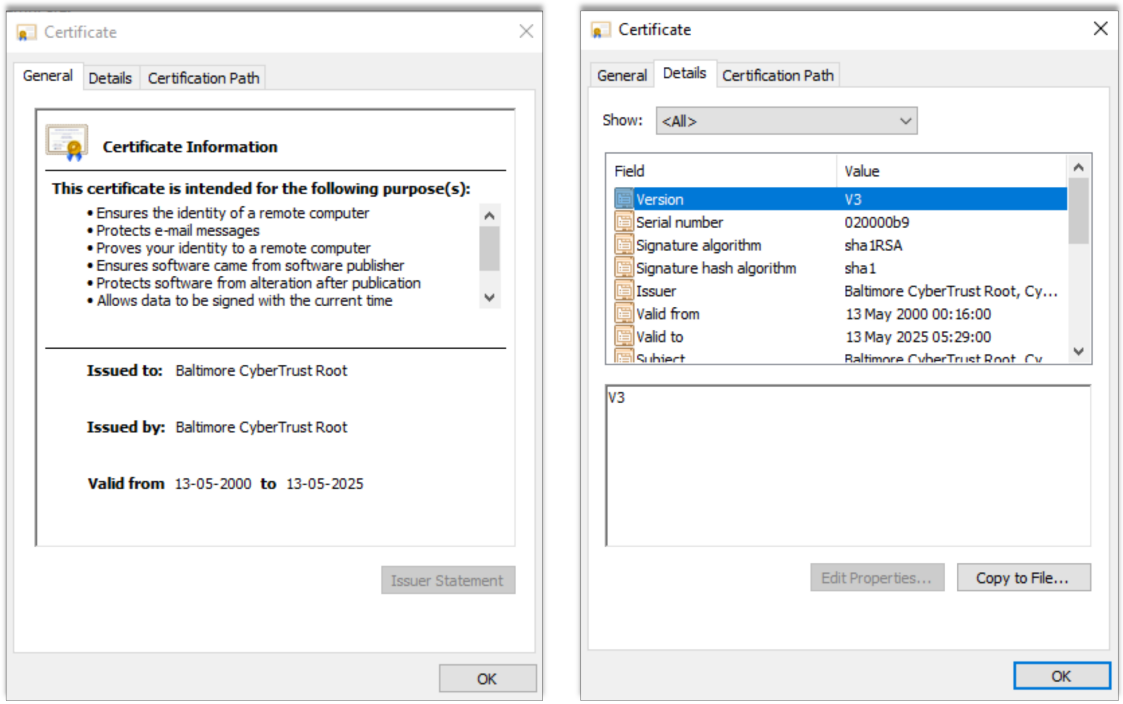


Figure: A screenshot of third-party certificate on a host device

Key Management

- Key management is one of the crucial aspects of modern-day cryptography and deals with the administration of cryptographic keys.
- The process of generation, distribution, storage, safety and distribution of keys are the major functionalities of a key management system.
- As the 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.
- Key management is one of the crucial aspects of modern-day cryptography and deals with the administration of cryptographic keys.
- The process of generation, distribution, storage, safety and distribution of keys are the major functionalities of a key management system.
- As the cryptographic keys can be both symmetric as well as

Key Management

- 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.
- Any key management system must be robust enough to handle the challenges of scalability, security, availability, heterogeneity, and governmental policies.

Key Management

The overview of these challenges are outlined as:

1. **Scalability**: The key management system must be able to scale its operations on-demand. 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, 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 a very short time.

Key Management

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

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

Inventory

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

Key exchange

1. Key exchange is a crucial part of the key management system, as any slip-up in the security of keys during transfer would compromise the purpose of the key management system.
2. Symmetric cryptosystems used a separate secure channel to distribute the keys, which acted as an additional overhead for the whole communication system.
3. Developments in cryptographic algorithms such as the Diffie-Hellman key exchange scheme ensured that these keys could be easily shared, even over insecure channels.
4. 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.

Key use

1. The use of key-based encryption does not guarantee cent percent defense against attackers.
2. The encryption, as mentioned previously, only buys the communicating parties enough time that the message becomes redundant after that time duration, causing the key breaking exercise to become redundant.
3. In most of the cases, symmetric key cryptosystems change the key after each message.
4. This feature is highlighted by the key lifetime.
5. 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 rises.
6. The key management systems also manage the key lifetimes.

Key storage

1. The secure storage of keys ensures the success of an intrusion-free communication.
2. The distributed storage of keys have various security mechanisms in place – user access passwords – to ensure no unauthorized access to the keys.

The End