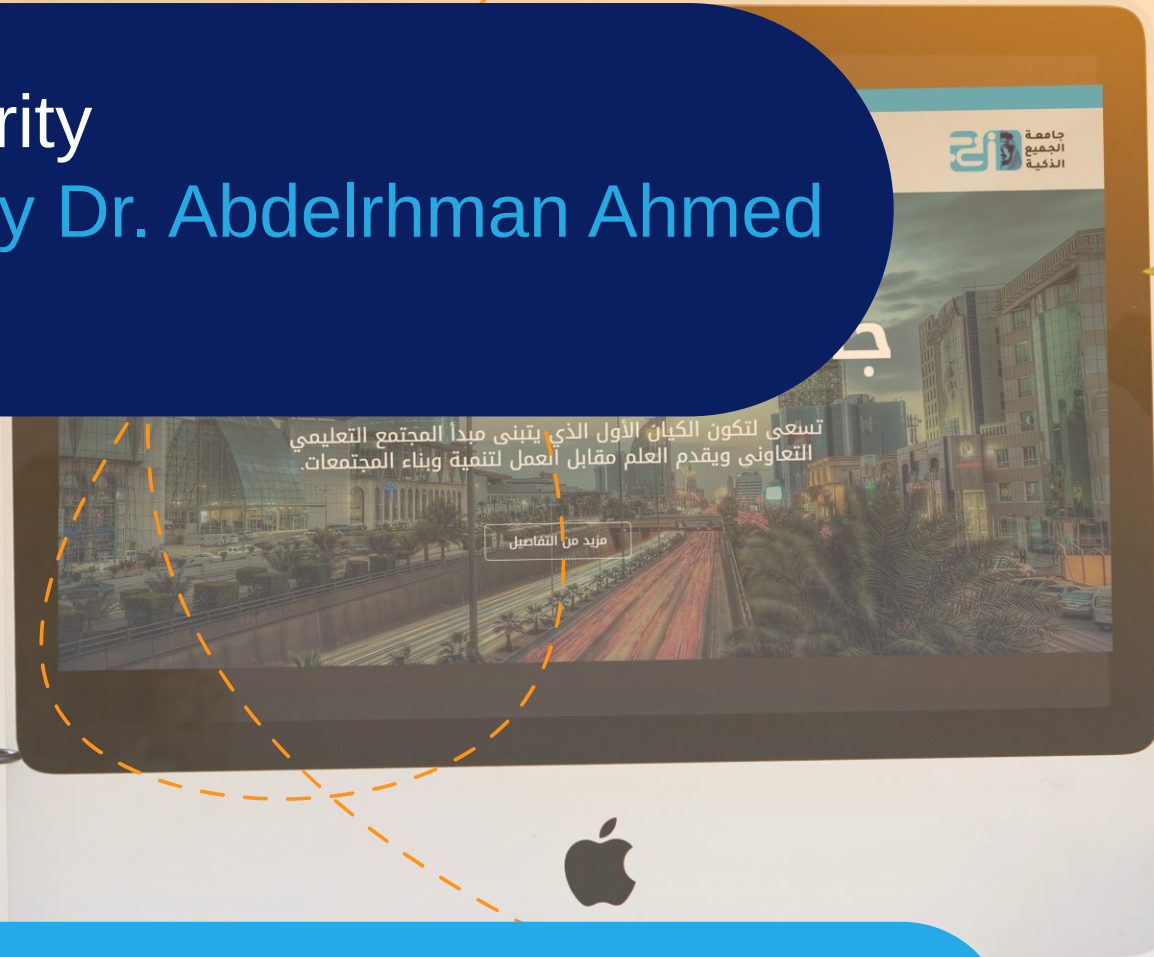


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 8



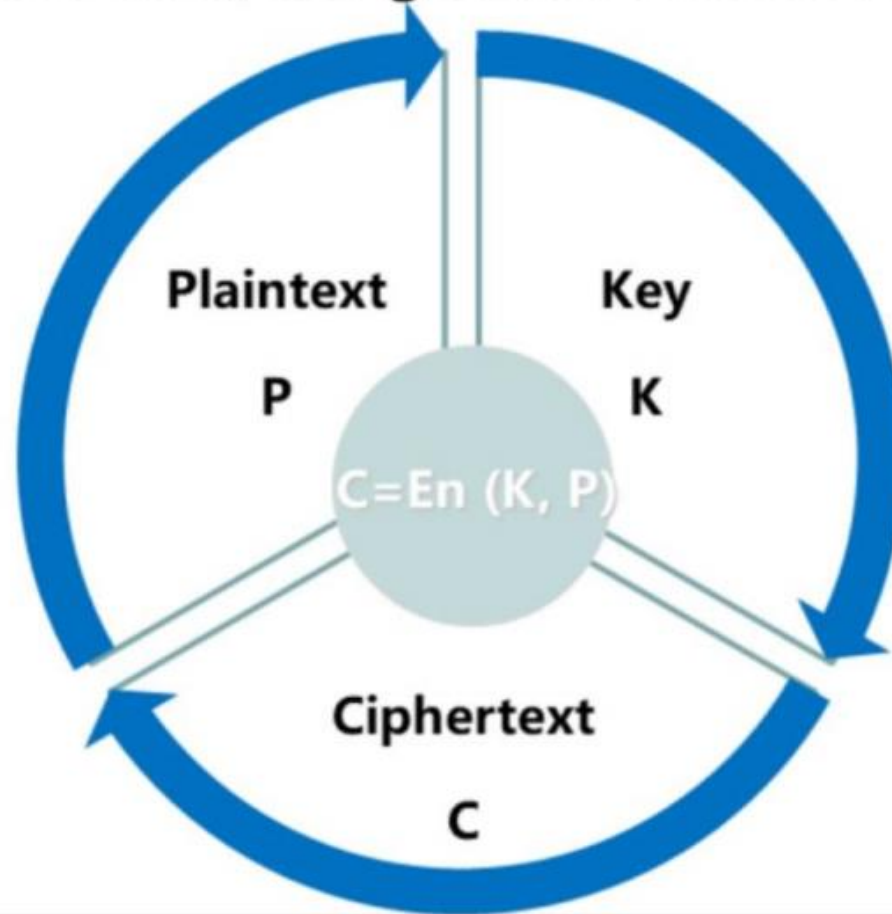
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

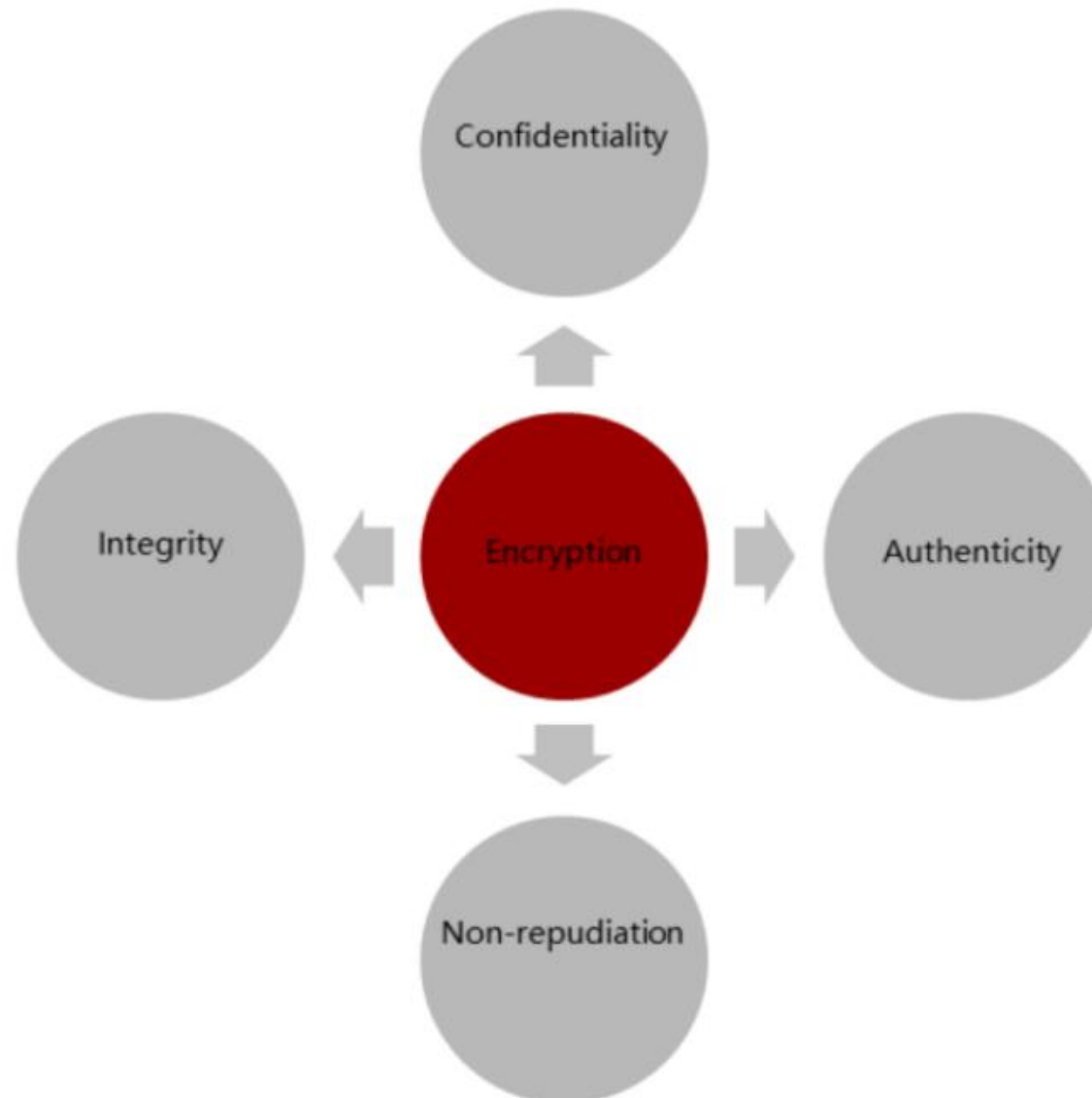
Encryption and Decryption Mechanisms

- Data encapsulated based on the TCP/IP protocol stack is transmitted in plaintext over the Internet, resulting in potential risks. For example, passwords and bank account information may be stolen or tampered with, and users' identities may be impersonated. After encryption and decryption technologies are applied on the network, transmitted data is protected to reduce the risk of information being leaked.

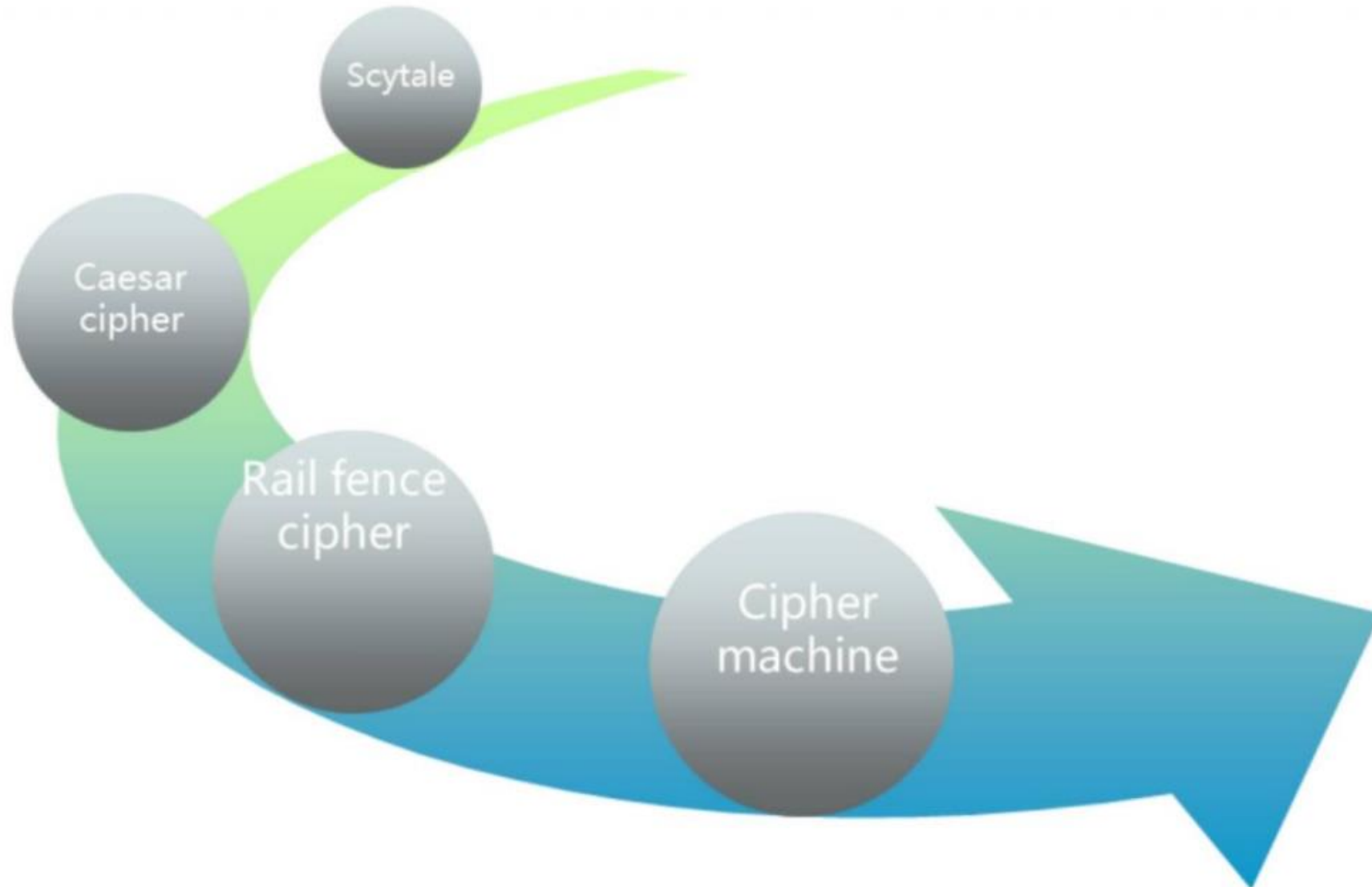
- **Upon completion of this course, you will be able to:**
 - ❑ **Describe the development of encryption and decryption technologies.**
 - ❑ **Describe the processes of various encryption and decryption methods.**
 - ❑ **Understand the mechanisms of encryption and decryption algorithms.**

- Cryptography is the conversion of plaintext (data to be hidden) into ciphertext (unreadable data) using mathematical methods.





- **Encryption** is the process of making information only readable to certain receivers and incomprehensible to other users. It achieves this by enabling the original content to be shown only after the correct key is used to decrypt the information. Encryption protects data from being obtained and read by unauthorized users. It prevents interception and theft of private information over networks. Encryption guarantees the confidentiality, integrity, authenticity, and non-repudiation of information.
- **Confidentiality:** implemented through data encryption. It allows only some users to access and read the information, making the information incomprehensible to unauthorized users. This is the main objective of encryption. It ensures that only the corresponding receivers can read it by using mathematical equations.
- **Integrity:** implemented through data encryption, hash algorithm, or digital signature. It ensures that data is not changed (tampered with, deleted, added, and replayed) by unauthorized users during the storage and transmission processes. For users that require high-level security, data encryption alone is not enough, because data can still be cracked and changed by unauthorized users.
- **Authenticity:** implemented through data encryption, hash algorithm, or digital signature. It provides services relevant to the authentication of the data sender and receiver.
- **Non-repudiation:** implemented through symmetric or asymmetric encryption and digital signature, with the help of trustworthy registration or certification organizations. It prevents users from denying things they have said or done.

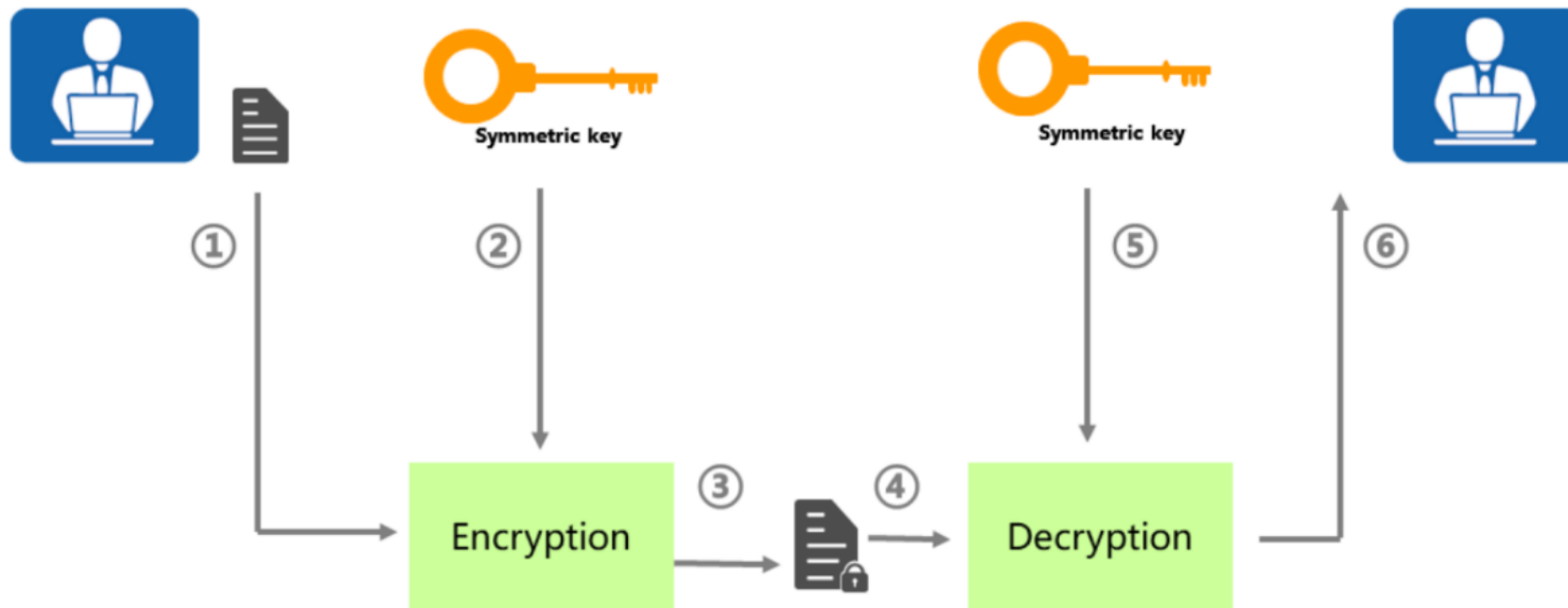


- As a method for information security protection, cryptography is not a modern invention. It dates back to a long time ago, when human beings tried to learn how to communicate while keeping their correspondence confidential. Ancient Greeks might be the first people to use techniques to encrypt information, which they did prior to the 5th century B.C. They used a rod called a scytale, with a piece of parchment wrapped around it, on which a message was written. Then the parchment was sent to the receiver. Anyone who did not know the diameter of the rod, which was the key in this case, could not understand the information on the message.
- In about 50 B.C., the Roman emperor Caesar invented a method for encrypting information during times of war, which was later called the Caesar cipher. The principles are that each letter in the simple text is replaced by the third letter further along in the alphabet, and the last three letters in the alphabet are replaced by the first three letters respectively. For example, after encryption, HuaweiSymantec becomes KxdzhlvBPdqwhf.
- Recent encryption technologies were mainly used for military purposes, such as the War of Independence and the Civil War in the US, and two World Wars. During the War of Independence in the US, the rail fence cipher was used. In this method, the simple text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out.
- During World War I, Germany wrote codes based on a dictionary. For example, 10-4-2 means the 2nd word in the 4th paragraph on the 10th page of a dictionary. In World War II, the most well-known cipher machine was the Enigma machine used by Germans to encrypt information.

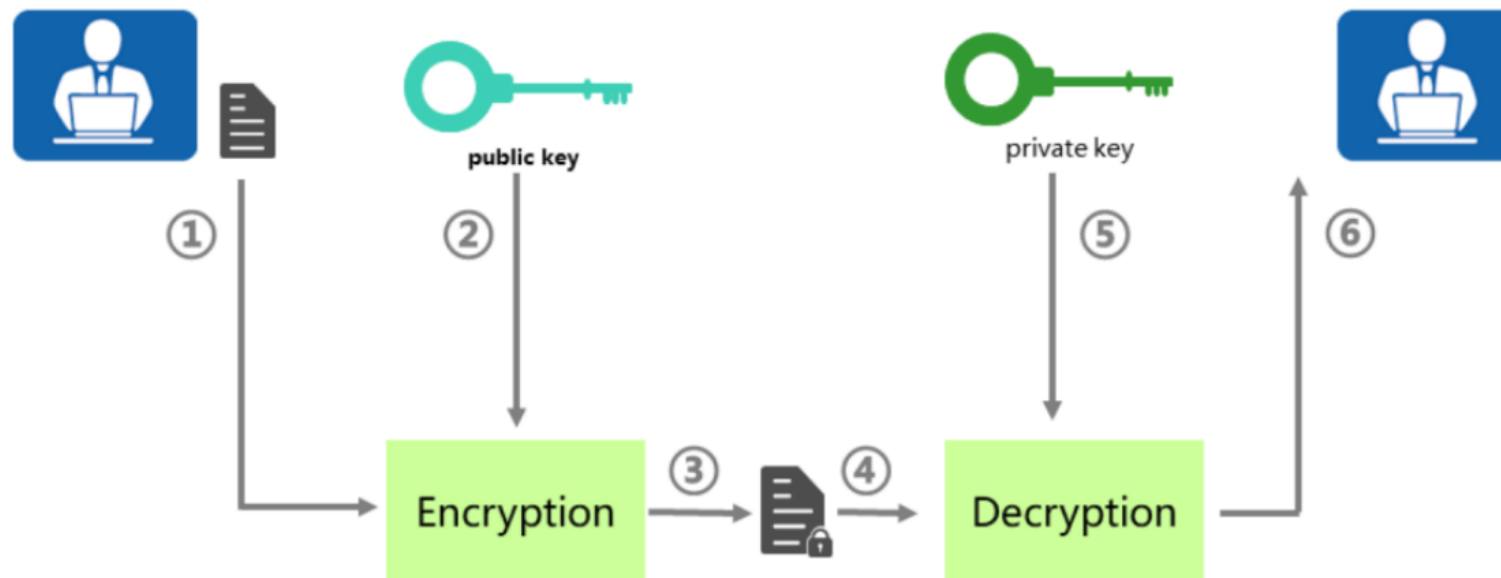
- **Symmetric encryption (also called shared-key encryption)**
- **The same key is used for encryption and decryption.**
- **Asymmetric encryption**
- ❖ **Two different keys are used for encryption and decryption:**
 - ❑ **The private key is for data protection.**
 - ❑ **The public key is used by users in the same system to check the validity of the information and its sender.**

Symmetric Encryption

- Users A and B negotiate a symmetric key in advance. The encryption and decryption process is as follows:
 - User A uses the symmetric key to encrypt data and sends the encrypted data to user B.
 - After receiving the encrypted data, user B decrypts the data using the symmetric key and obtains the original plaintext.

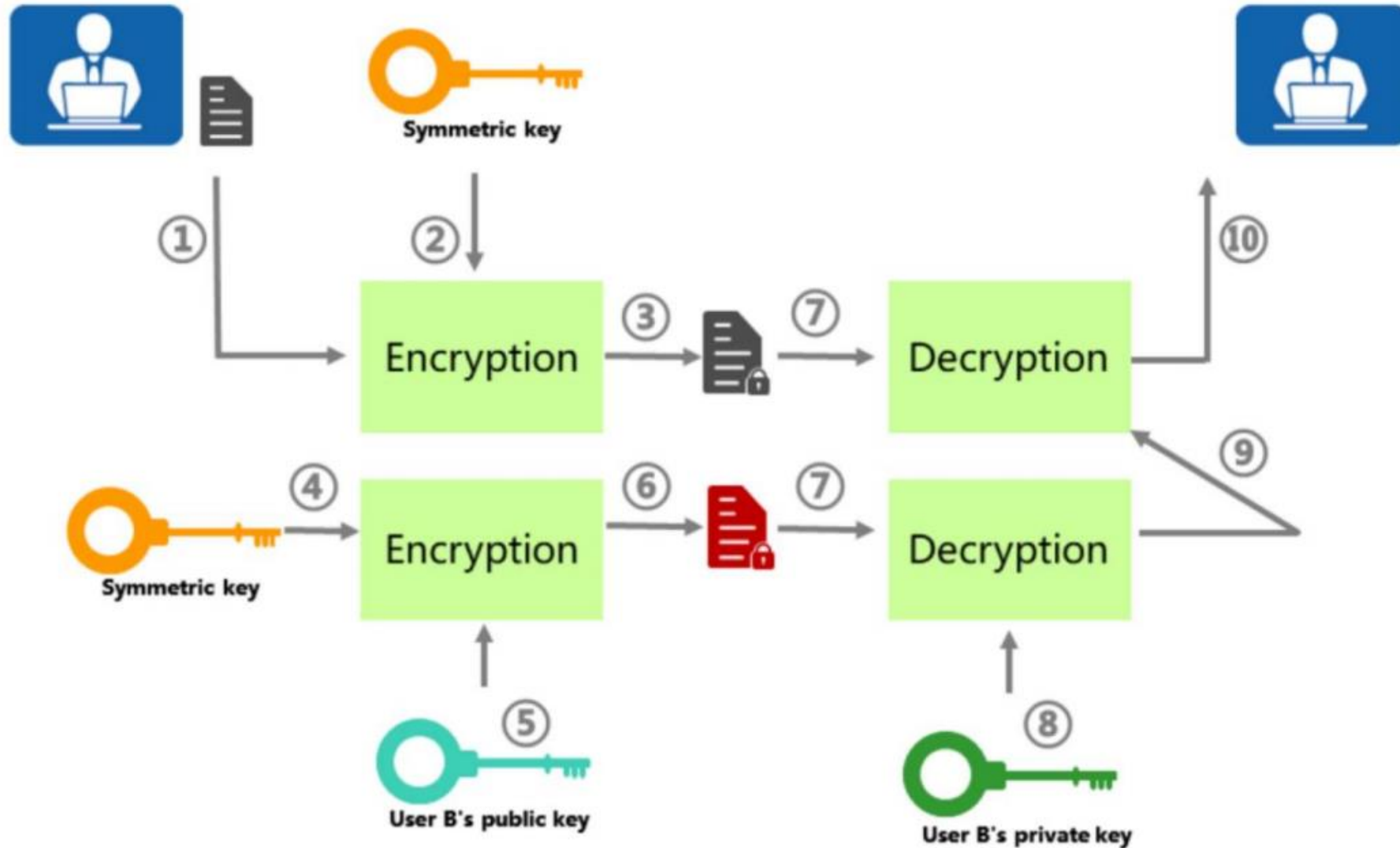


- User A obtains the public key of user B in advance. The encryption and decryption process is as follows:
 - User A uses user B's public key to encrypt data and sends the encrypted data to user B.
 - After receiving the encrypted data, user B decrypts the data using their private key and obtains the original plaintext.

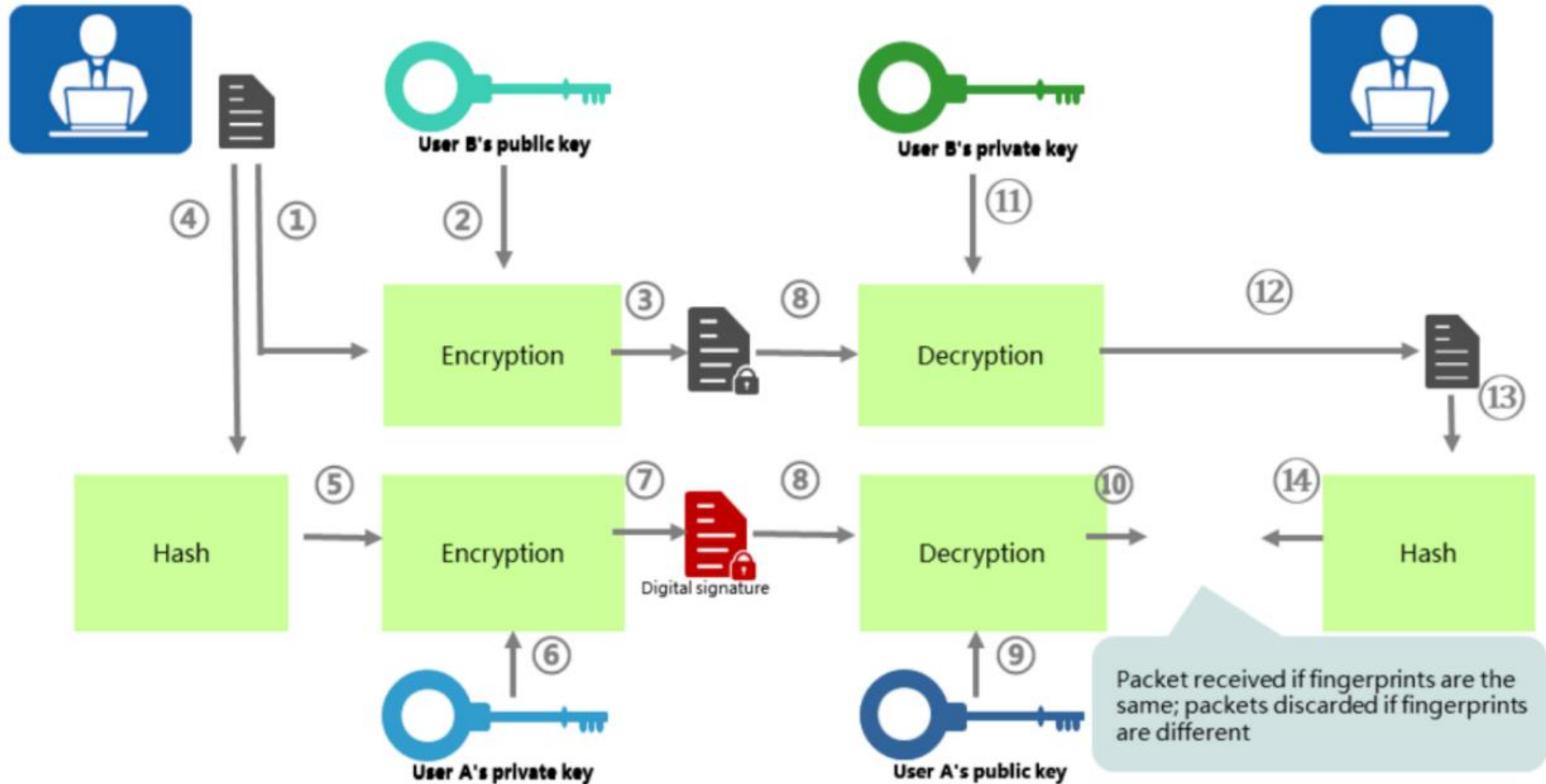


- Symmetric key cryptography features high efficiency, simple algorithms, and low system overhead. It is suitable for encrypting a large volume of data. However, it is difficult to implement because the two parties must exchange their keys securely before communication. In addition, it is difficult to expand because each pair of communicating parties needs to negotiate keys, and n users need to negotiate $n*(n-1)/2$ different keys.
- Attackers cannot use one key in a key pair to figure out the other key. The data encrypted by a public key can only be decrypted by the private key of the same user. However, it takes a long time for the public key cryptography to encrypt a large amount of data, and the encrypted packets are too large, consuming much bandwidth.
- Public key cryptography is suitable for encrypting sensitive information such as keys and identities to provide higher security.

	Strength	Weakness
Symmetric encryption	Fast encryption and decryption	Transmission of keys
Asymmetric encryption	High security of keys	Encryption and decryption are speed-sensitive.



- A digital envelope contains the symmetric key encrypted using the peer's public key. When receiving a digital envelope, the receiver uses its own private key to decrypt the digital envelope and obtains the symmetric key.
- Assume that user A has the public key of user B. The encryption and decryption process is as follows:
 - User A uses a symmetric key to encrypt data.
 - User A uses the public key of user B to encrypt the symmetric key and generate a digital envelope.
 - User A sends the digital envelope and encrypted data to user B.
 - User B uses its own private key to decrypt the digital envelope and obtains the symmetric key.
 - User B uses the symmetric key to decrypt the data and obtains the original data.
- The digital envelope has the advantages of both symmetric key cryptography and public key cryptography. That is, it speeds up key distribution and encryption while improving key security, extensibility, and efficiency.
- However, the digital envelope still has a vulnerability. The attacker may obtain information from user A, use its own symmetric key to encrypt the forged information, use the public key of user B to encrypt its own symmetric key, and send the information to user B. After receiving the information, user B decrypts it and considers the information to be sent from user A. To address this problem, the digital signature is used, ensuring that the received information was sent from the correct sender.



- Digital signature is generated by the sender by encrypting the digital fingerprint using its own private key. The receiver uses the sender's public key to decrypt the digital signature and obtain the digital fingerprint.
- A digital fingerprint, also called information digest, is generated by the sender using the hash algorithm on plaintext information. The sender sends both digital fingerprint and plaintext to the receiver, who uses the same hash algorithm to calculate the digital fingerprint on the plaintext. If the two fingerprints are the same, the receiver knows that the information has not been tampered with.
- Assume that user A has the public key of user B. The encryption and decryption process is as follows:
 - ❑ User A uses the public key of user B to encrypt data.
 - ❑ User A performs hash on the plaintext and generates a digital fingerprint.
 - ❑ User A uses its own private key to encrypt the digital fingerprint, generating the digital signature.
 - ❑ User A sends both the ciphertext and digital signature to user B.
 - ❑ User B uses the public key of user A to decrypt the digital signature, obtaining the digital fingerprint.
 - ❑ After receiving the ciphertext from user A, user B uses its own private key to decrypt the information, obtaining the plaintext information.
 - ❑ User B performs hash on the plaintext and generates a digital fingerprint.
 - ❑ User B compares the generated fingerprint with the received one. If the two fingerprints are the same, user B accepts the plaintext; otherwise, user B discards it.

- The digital signature proves that information is not tampered with and verifies the sender's identity. The digital signature and digital envelope can be used together.
- However, the digital signature still has a vulnerability. If the attacker modifies the public key of user B and user A obtains the modified key, the attacker can intercept information sent from user B to user A, sign the forged information using its own private key, and send the forged information encrypted using user A's public key to user A. After receiving the encrypted information, user A decrypts the information and verifies that the information has not been tampered with. In addition, user A considers the information to be sent by user B. The digital certificate can fix this vulnerability.

- **Stream cipher**

- ☐ **RC4**

- **Block cipher**

- ☐ **DES**

- ☐ **3DES**

- ☐ **AES**

- ☐ **IDEA**

- ☐ **RC2, RC5, RC6**

- ☐ **SM1.SM4**

- **Asymmetric cipher algorithms**

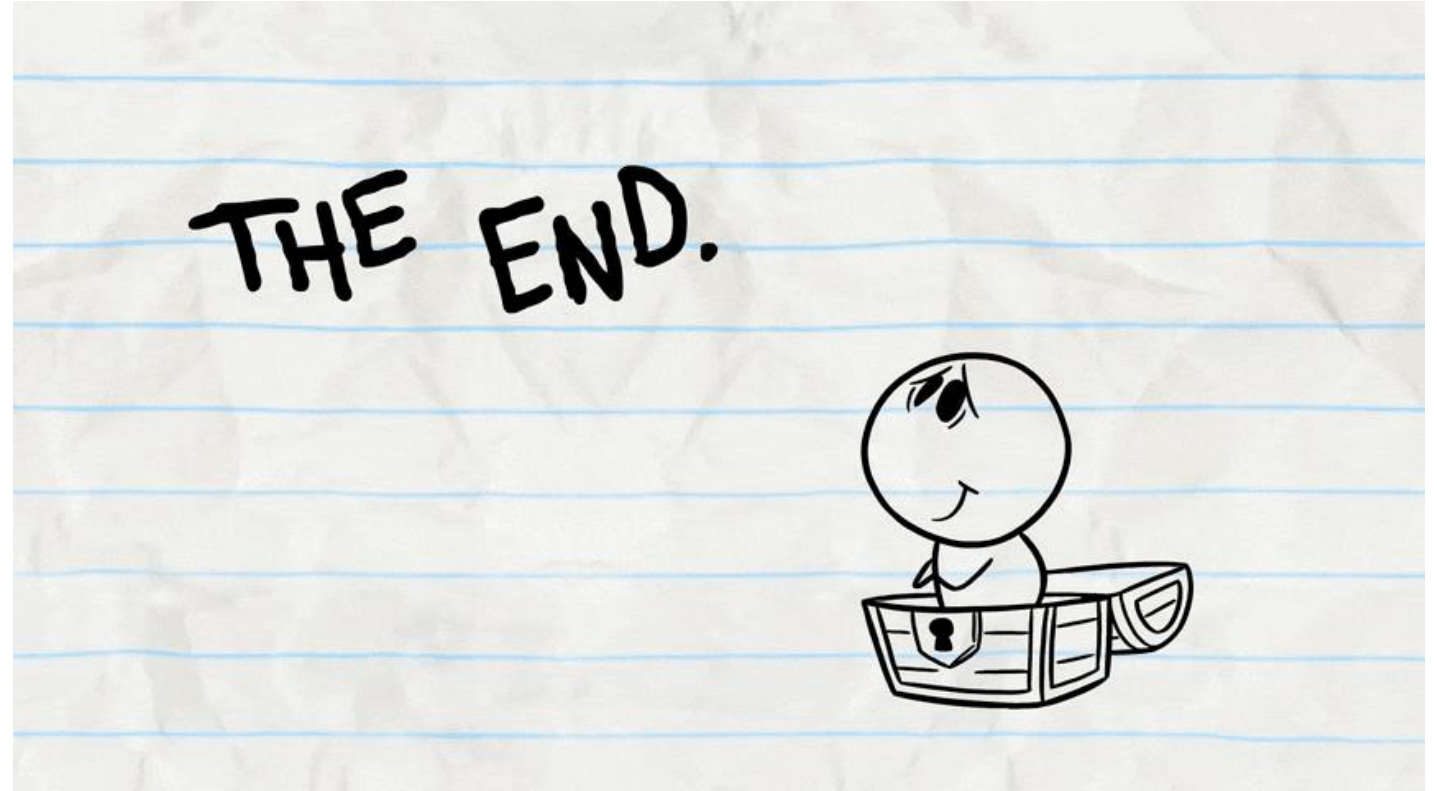
- ☐ **DH**
- ☐ **RSA**
- ☐ **DSA**

- **Hash algorithm: Converts the input of any length into the output of a fixed length.**
- **Common hash algorithms**
 - ❑ **Message Digest Algorithm 5 (MD5)**
 - ❑ **Secure Hash Algorithm (SHA)**
 - ❑ **Senior Middle 3 (SM3)**

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY