An toan thong tin_ Nhom 09

Nhà của tôi / Các khoá học của tôi / 2020_2021_HK1_Daitra / An toan thong tin_ Nhom 09 / Chapter 11 - Asymetric and PKI / Test_C10-C11

Bắt đầu vào lúc	Tuesday, 12 January 2021, 12:15 PM
State	Finished
Kết thúc lúc	Tuesday, 12 January 2021, 12:16 PM
Thời gian thực hiện	9 giây
Điểm	0,00/30,00
Điểm	**0,00** out of 10,00 (**0**%)

Câu hỏi 1

Không trả lời

Đạt điểm 1,00

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

Select one:

○ a. DSA

○ b. Diffie-Hellman

○ c. Blowfish

○ d. 3DES

○ e. DES

Your answer is incorrect.

The correct answer is: Diffie-Hellman

Câu hỏi 2

Không trả lời

Đạt điểm 1,00

A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

Select one or more:

□ a. Revoke the digital certificate

□ b. Restore the certificate using a recovery agent

□ c. Issue a new digital certificate

□ d. Restore the certificate using a CRL

□ e. Mark the key as private and import it

Your answer is incorrect.

The correct answers are: Revoke the digital certificate, Issue a new digital certificate

Câu hỏi 3

Không trả lời

Đạt điểm 1,00

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

Select one:

○ a. Certification authority

○ b. Certificate revocation list

○ c. Key escrow

○ d. Registration authority

Your answer is incorrect.

The correct answer is: Certification authority

Câu hỏi 4

Không trả lời

Đạt điểm 1,00

Digital certificates can be used to ensure which of the following? (Select TWO)

Select one or more:

□ a. Authorization

□ b. Confidentiality

□ c. Availability

□ d. Non-repudiation

□ e. Verification

Your answer is incorrect.

The correct answers are: Confidentiality, Non-repudiation

Câu hỏi 5

Không trả lời

Đạt điểm 1,00

An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

Select one:

○ a. Confidentiality

○ b. Integrity

○ c. Remediation

○ d. Availability

Your answer is incorrect.

The correct answer is: Integrity

Câu hỏi 6

Không trả lời

Đạt điểm 1,00

Digital certificates can be used to ensure which of the following? (Select TWO).

Select one or more:

□ a. Non-repudiation

□ b. Verification

□ c. Confidentiality

□ d. Authorization

□ e. Availability

Your answer is incorrect.

The correct answers are: Confidentiality, Non-repudiation

Câu hỏi 7

Không trả lời

Đạt điểm 1,00

Which of the following is true about asymmetric encryption?

Select one:

○ a. A message encrypted with a shared key, can be decrypted by the same key.

○ b. A message encrypted with the public key can be decrypted with the private key

○ c. A message encrypted with the public key can be decrypted with a shared key.

○ d. A message encrypted with the private key can be decrypted by the same key

Your answer is incorrect.

The correct answer is: A message encrypted with the public key can be decrypted with the private key

Câu hỏi 8

Không trả lời

Đạt điểm 1,00

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

Select one:

○ a. Digital Signatures

○ b. Hashing

○ c. Steganography

○ d. Encryption

Your answer is incorrect.

The correct answer is: Digital Signatures

Câu hỏi 9

Không trả lời

Đạt điểm 1,00

How many keys are required to fully implement a symmetric algorithm with 10 participants?

Select one:

○ a. 10

○ b. 45

○ c. 100

○ d. 20

Your answer is incorrect.

The correct answer is: 45

Câu hỏi 10

Không trả lời

Đạt điểm 1,00

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

Select one:

○ a. Digital Signature

○ b. Private Key

○ c. Session Key

○ d. Public Key

Your answer is incorrect.

The correct answer is: Private Key

Câu hỏi 11

Không trả lời

Đạt điểm 1,00

How many encryption keys are required to fully implement an asymmetric algorithm with 10 participants?

Select one:

○ a. 45

○ b. 10

○ c. 20

○ d. 100

Your answer is incorrect.

The correct answer is: 20

Câu hỏi 12

Không trả lời

Đạt điểm 1,00

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

Select one or more:

□ a. The CA's private key

□ b. Ann's private key

□ c. Ann's public key

□ d. The CA's public key

□ e. Joe's private key

□ f. Joe's public key

Your answer is incorrect.

The correct answers are: Ann's private key, Joe's public key

Câu hỏi 13

Không trả lời

Đạt điểm 1,00

Which of the following symmetric key algorithms are examples of block ciphers? (Select Two).

Select one or more:

□ a. AES

□ b. 3DES

□ c. MD5

□ d. PGP

□ e. RC4

Your answer is incorrect.

The correct answers are: 3DES, AES

Câu hỏi 14

Không trả lời

Đạt điểm 1,00

Which of the following are restricted to 64-bit block sizes? (Select TWO).

Select one or more:

□ a. DES

□ b. PGP

□ c. AES256

□ d. AES

□ e. 3DES

□ f. RSA

Your answer is incorrect.

The correct answers are: DES, 3DES

Câu hỏi 15

Không trả lời

Đạt điểm 1,00

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

Select one:

○ a. Integrity of downloaded software.

○ b. Integrity of the server logs.

○ c. Availability of the FTP site.

○ d. Confidentiality of downloaded software.

Your answer is incorrect.

The correct answer is: Integrity of downloaded software.

Câu hỏi 16

Không trả lời

Đạt điểm 1,00

Which of the following uses both a public and private key?

Select one:

○ a. SHA

○ b. MD5

○ c. AES

○ d. RSA

Your answer is incorrect.

The correct answer is: RSA

Câu hỏi 17

Không trả lời

Đạt điểm 1,00

A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?

Select one:

○ a. IPSec

○ b. SSH

○ c. AES

○ d. PGP

Your answer is incorrect.

The correct answer is: SSH

Câu hỏi 18

Không trả lời

Đạt điểm 1,00

Which one of the following cannot be achieved by a secret key cryptosystem?

Select one:

○ a. Availability

○ b. Nonrepudiation

○ c. Key distribution

○ d. Confidentiality

Your answer is incorrect.

The correct answer is: Nonrepudiation

Câu hỏi 19

Không trả lời

Đạt điểm 1,00

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

Select one:

○ a. Sender’s public key

○ b. Sender’s private key

○ c. Recipient’s public key

○ d. Recipient’s private key

Your answer is incorrect.

The correct answer is: Sender’s public key

Câu hỏi 20

Không trả lời

Đạt điểm 1,00

Which of the following is BEST used as a secure replacement for TELNET?

Select one:

○ a. HMAC

○ b. GPG

○ c. SSH

○ d. HTTPS

Your answer is incorrect.

The correct answer is: SSH

Câu hỏi 21

Không trả lời

Đạt điểm 1,00

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

Select one:

○ a. TwoFish

○ b. 3DES

○ c. AES

○ d. Blowfish

Your answer is incorrect.

The correct answer is: 3DES

Câu hỏi 22

Không trả lời

Đạt điểm 1,00

Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?

Select one:

○ a. Sender’s private key

○ b. Sender’s public key

○ c. Recipient’s private key

○ d. Recipient’s public key

Your answer is incorrect.

The correct answer is: Recipient’s public key

Câu hỏi 23

Không trả lời

Đạt điểm 1,00

Which of the following is used to verify data integrity?

Select one:

○ a. 3DES

○ b. RSA

○ c. AES

○ d. SHA

Your answer is incorrect.

The correct answer is: SHA

Câu hỏi 24

Không trả lời

Đạt điểm 1,00

Which of the following concepts is used by digital signatures to ensure integrity of the data?

Select one:

○ a. Hashing

○ b. Key escrow

○ c. Non-repudiation

○ d. Transport encryption

Your answer is incorrect.

The correct answer is: Hashing

Câu hỏi 25

Không trả lời

Đạt điểm 1,00

Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?

Select one:

○ a. His private key

○ b. A pre-shared private key

○ c. His public key

○ d. Ann’s public key

Your answer is incorrect.

The correct answer is: His private key

Câu hỏi 26

Không trả lời

Đạt điểm 1,00

Symmetric encryption utilizes _________, while asymmetric encryption utilizes ________.

Select one:

○ a. Private keys, session keys

○ b. Private keys, public keys

○ c. Shared keys, private keys

○ d. Public keys, one time

Your answer is incorrect.

The correct answer is: Private keys, public keys

Câu hỏi 27

Không trả lời

Đạt điểm 1,00

An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)

Select one or more:

□ a. Ephemeral Key generation

□ b. AES

□ c. Diffie-Hellman

□ d. Symmetrical encryption

□ e. Asymmetrical encryption

□ f. RSA

Your answer is incorrect.

The correct answers are: Diffie-Hellman, RSA

Câu hỏi 28

Không trả lời

Đạt điểm 1,00

Digital signatures are used for ensuring which of the following items? (Select TWO).

Select one or more:

□ a. Confidentiality

□ b. Integrity

□ c. Non-Repudiation

□ d. Algorithm strength

□ e. Availability

Your answer is incorrect.

The correct answers are: Integrity, Non-Repudiation

Câu hỏi 29

Không trả lời

Đạt điểm 1,00

What is the length of the cryptographic key used in the Data Encryption Standard (DES) cryptosystem?

Select one:

○ a. 256 bits

○ b. 192 bits

○ c. 128 bits

○ d. 56 bits

Your answer is incorrect.

The correct answer is: 56 bits

Câu hỏi 30

Không trả lời

Đạt điểm 1,00

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?

Select one:

○ a. AES

○ b. Diffie-Hellman

○ c. SHA-256

○ d. 3DES

Your answer is incorrect.

The correct answer is: Diffie-Hellman

◄ Chapter 11 - Public - key Encryption

Chuyển tới...

Chapter 12 - Network security ►