77

CompTIA Security+ Certification Practice Test 12 (Exam SY0-401)

Send results by email

Name Enter your name

Email Enter your email

Send Results

▸ Block ciphers work by encrypting each plaintext digit one at a time.

○ ○ ○ True

○ ✔ 👎 False (✖ Missed)

⛔ Your answer to this question is incorrect.

▸ Which IPsec mode provides encryption for the entire packet?

○ ✔ 👎 Tunnel (✖ Missed)

○ ○ ○ Host-to-host

○ ○ ○ Payload

○ ○ ○ Transport

⛔ Your answer to this question is incorrect.

▸ An IPsec mode providing encryption only for the payload (the data part of the packet) is known as:

○ ○ ○ Protected mode

○ ○ ○ Tunnel mode

○ ✔ 👎 Transport mode (✖ Missed)

○ ○ ○ Safe mode

⛔ Your answer to this question is incorrect.

▸ What is the purpose of non-repudiation?

○ ○ ○ Hiding one piece of data in another piece of data

○ ○ ○ Ensuring that received data hasn't changed in transit

○ ✔ 👎 Preventing someone from denying that they have taken specific action (✖ Missed)

○ ○ ○ Transforming plaintext into ciphertext

⛔ Your answer to this question is incorrect.

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. **Learn more**

I agree

▸ Taking hashes ensures that data retains its:

○ ○ ○ Confidentiality

○ ✔ 👎 Integrity (✖ Missed)

○ ○ ○ Order of volatility

○ ○ ○ Availability

⛔ Your answer to this question is incorrect.

▸ What is the name of a storage solution used to retain copies of private encryption keys?

○ ○ ○ Trusted OS

○ ✔ 👎 Key escrow (✖ Missed)

○ ○ ○ Proxy server

○ ○ ○ Recovery agent

⛔ Your answer to this question is incorrect.

▸ What is the purpose of steganography?

○ ○ ○ Checking data integrity

○ ○ ○ Calculating hash values

○ ✔ 👎 Hiding data within another piece of data (✖ Missed)

○ ○ ○ Data encryption

⛔ Your answer to this question is incorrect.

▸ A digital signature is a hash of a message that uniquely identifies the sender of the message and provides a proof that the message hasn't changed in transit.

○ ✔ 👎 True (✖ Missed)

○ ○ ○ False

⛔ Your answer to this question is incorrect.

▸ What are the features of Elliptic Curve Cryptography (ECC)? (Select 2 answers)

☝ ✔ ☑ Asymmetric encryption (☑ Your answer)

☐ ☐ ☐ Shared key

☝ ✔ ☑ Suitable for small wireless devices (☑ Your answer)

☐ ☐ ☐ High processing power requirements

☐ ☐ ☐ Symmetric encryption

☑ You correctly answered this question.

▸ Which of the following answers refer to the applications / features of quantum cryptography? (Select 2 answers)

☐ ☐ ☐ High availability

☝ ✔ ☑ Protection against eavesdropping (☑ Your answer)

☐ ☐ ☐ Loop protection

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. **Learn more**

I agree

Secure key exchange (Your answer)

Host-based intrusion detection

You correctly answered this question.

SHA, MD5, and RIPEMD are examples of:

Trust models

Encryption algorithms

Hash functions (Your answer)

Virus signatures

You correctly answered this question.

Which of the answers listed below refer(s) to the Advanced Encryption Standard (AES): (Select all that apply)

Symmetric-key algorithm (Your answer)

128-, 192-, and 256-bit keys (Your answer)

Asymmetric-key algorithm

Block cipher algorithm (Your answer)

Stream cipher algorithm

You correctly answered this question.

Unlike stream ciphers which process data by encrypting individual bits, block ciphers divide data into separate fragments and encrypt each fragment separately.

True (Your answer)

False

You correctly answered this question.

Which of the following are symmetric-key algorithms? (Select 3 answers)

AES (Your answer)

DES (Your answer)

RSA

Diffie-Hellman

3DES (Your answer)

You correctly answered this question.

Which of the following answers refers to a solution for secure exchange of cryptographic keys? (Select best answer)

Data Encryption Standard (DES)

In-band key exchange

Diffie–Hellman (Missed)

Out-of-band key exchange

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. **Learn more**

I agree

⛔ Your answer to this question is incorrect.

▸ One of the answers below lists some of the past and current authentication protocols used in Microsoft networks arranged from oldest / obsolete up to the current recommendation. Which of the answers lists the protocols in the correct order?

- ✔ ☑ LANMAN › NTLM › NTLMv2 › Kerberos (☑ Your answer)
- NTLM › NTLMv2 › Kerberos › LANMAN
- NTLM › NTLMv2 › LANMAN › Kerberos
- Kerberos › NTLM › NTLMv2 › LANMAN

☑ You correctly answered this question.

▸ A computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet is known as:

- SMTP
- ✔ 👎 PGP (✖ Missed)
- ⛔ OCSP (✖ Your answer)
- OVAL

⛔ Your answer to this question is incorrect.

▸ GNU Privacy Guard (GPG) provides similar functionality and an alternative to:

- PAP
- IMAP4
- ✔ 👎 PGP (✖ Missed)
- Windows Firewall

⛔ Your answer to this question is incorrect.

▸ Which of the protocols listed below uses elliptic curve cryptography for secure exchange of cryptographic keys?

- ECC
- LANMAN
- ✔ ☑ ECDHE (☑ Your answer)
- OCSP

☑ You correctly answered this question.

▸ Which of the following answers refers to a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers?

- Telnet
- ✔ ☑ SSH (☑ Your answer)
- Bcrypt
- TFTP

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. **Learn more**

I agree

☑ You correctly answered this question.

▸ In cryptography, the term "key stretching" refers to a mechanism for extending the length of the cryptographic key in order to make it more secure against brute force attacks.

☆ ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ Examples of key stretching algorithms include: (Select 2 answers)

☆ ✔ ☑ PBKDF2 (☑ Your answer)

☐ ☐ ☐ RC4

☐ ☐ ☐ NTLMv2

☆ ✔ ☑ Bcrypt (☑ Your answer)

☐ ☐ ☐ FCoE

☑ You correctly answered this question.

▸ Which of the solutions listed below allow(s) to check whether a digital certificate has been revoked? (Select all that apply)

☐ ☐ ☐ CIRT

☆ ✔ ☑ CRL (☑ Your answer)

☆ ✔ ☑ OCSP (☑ Your answer)

☐ ☐ ☐ CRC

☐ ☐ ☐ ICMP

☑ You correctly answered this question.

▸ Which of the following provides the fastest way for validating a digital certificate?

○ ○ ○ ICMP

☆ ○ ⛔ CRL (✖ Your answer)

○ ○ ○ Key escrow

○ ✔ 👎 OCSP (✖ Missed)

⛔ Your answer to this question is incorrect.

▸ Copies of lost private encryption keys can be retrieved from a key database by:

○ ○ ○ Power users

☆ ✔ ☑ Recovery agents (☑ Your answer)

○ ○ ○ End users

○ ○ ○ Backup operators

☑ You correctly answered this question.

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. **Learn more**

I agree