CompTIA Security+ Certification Exam SY0-701 Practice Test 4

▸ Which of the following answers refers to a legacy symmetric-key block cipher encryption algorithm?

👍 ○ ▬ RC4 (✖ Your answer)

○ ✔ 👎 DES (✖ Missed)

○ ○ ○ RSA

○ ○ ○ DSA

▬ Your answer to this question is incorrect or incomplete.

▸ Which of the answers listed below refers to a deprecated stream cipher used in some legacy applications, such as WEP?

○ ○ ○ RSA

👍 ○ ▬ DES (✖ Your answer)

○ ○ ○ SSL

○ ✔ 👎 RC4 (✖ Missed)

▬ Your answer to this question is incorrect or incomplete.

▸ Which of the following answers refers to a deprecated (largely replaced by AES) symmetric-key block cipher encryption algorithm?

👍 ○ ▬ ECDSA (✖ Your answer)

○ ○ ○ RSA

○ ✔ 👎 IDEA (✖ Missed)

○ ○ ○ DSA

⊟ Your answer to this question is incorrect or incomplete.

▶ What is the recommended replacement for DES?

○ ○ ○ DSA

○ ○ ○ RSA

○ ○ ○ RC4

👆 ✔ ☑ AES (☑ Your answer)

☑ You correctly answered this question.

▶ An IV is a random or pseudorandom value used in cryptography to ensure that the same plaintext input does not produce the same ciphertext output, even when the same encryption key is used. The IV is typically used with encryption algorithms in block cipher modes to enhance security by introducing randomness to the encryption process.

👆 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▶ Which of the answers listed below refers to a logical operation commonly used in the context of cybersecurity, particularly in encryption and obfuscation techniques?

○ ○ ○ AND

○ ○ ○ OR

○ ○ ○ NOT

👆 ✔ ☑ XOR (☑ Your answer)

☑ You correctly answered this question.

▶ Which of the following answers refers to a block cipher mode that works by chaining the ciphertext blocks together, such that each ciphertext block depends on the previous block?

👍 ✔ ☑ CBC (☑ Your answer)

○ ○ ○ GCM

○ ○ ○ ECB

○ ○ ○ CFB

☑ You correctly answered this question.

▶ Which block mode transforms a block cipher into a stream cipher enabling the encryption of individual bits or bytes of data?

○ ✔ 👎 CFB (✖ Missed)

○ ○ ○ CBC

○ ○ ○ GCM

👍 ○ ▬ ECB (✖ Your answer)

▬ Your answer to this question is incorrect or incomplete.

▶ A block cipher mode that combines a unique counter with encryption key to generate a stream of pseudorandom data blocks which are then used for encrypting data is called:

👍 ○ ▬ CBC (✖ Your answer)

○ ○ ○ GCM

○ ○ ○ CFB

○ ✔ 👎 CTM (✖ Missed)

▬ Your answer to this question is incorrect or incomplete.

▶ Which of the block cipher modes listed below is the simplest/weakest and therefore not recommended for use?

👍 ○ ▬ CBC (✖ Your answer)

○ ○ ○ GCM

○ ✔ 👎 ECB (✖ Missed)

○ ○ ○ CTM

⊟ Your answer to this question is incorrect or incomplete.

▶ Which block cipher mode combines CTM for encryption with an authentication mechanism to ensure both data confidentiality and integrity?

○ ○ ○ CBC

○ ✔ 👎 GCM (✖ Missed)

👆 ○ ⊟ ECB (✖ Your answer)

○ ○ ○ CFB

⊟ Your answer to this question is incorrect or incomplete.

▶ In cryptography, the number of bits in a key used by a cryptographic algorithm is referred to as key size or key length. The key length determines the maximum number of combinations required to break the encryption algorithm, therefore typically a longer key means stronger cryptographic security.

👆 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▶ Which AES key length provides the highest level of security?

○ ○ ○ 128-bit key

○ ○ ○ 192-bit key

👆 ✔ ☑ 256-bit key (☑ Your answer)

○ ○ ○ 320-bit key

☑ You correctly answered this question.

▶ Which of the following answers refers to an embedded microcontroller used for secure boot, disk encryption, and system integrity verification?

👆 ✔ ☑ TPM (☑ Your answer)

○ ○ ○ SoC

○ ○ ○ UEFI

○ ○ ○ HSM

☑ You correctly answered this question.

▸ Which of the answers listed below refers to a piece of hardware and associated software/firmware designed to provide cryptographic and key management functions?

○ ○ ○ EFS

👆 ✔ ☑ HSM (☑ Your answer)

○ ○ ○ SFC

○ ○ ○ TPM

☑ You correctly answered this question.

▸ Which of the following answers refers to a centralized server that is used to distribute cryptographic keys and authenticate users and services within a computer network?

○ ○ ○ PKI

○ ○ ○ RAS

👆 ✔ ☑ KDC (☑ Your answer)

○ ○ ○ NAS

☑ You correctly answered this question.

▸ In a Kerberos-protected network, this type of secure token is granted to users during their initial login to enable them access to multiple network services without the need to re-enter their login credentials.

○ ○ ○ OTP

👆 ✔ ☑ TGT (☑ Your answer)

○ ○ ○ AS

○ ○ ○ TGS

☑ You correctly answered this question.

▸ In cryptography and security, the term "Secure enclave" typically refers to a protected and isolated hardware or software environment within a computing device, such as a smartphone, tablet, or computer, where sensitive data and cryptographic operations can be stored and processed securely.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ The term "Obfuscation" is used to describe techniques employed to obscure or hide the true meaning or nature of data, making it challenging for unauthorized parties to decipher or reverse-engineer the information.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ What is the purpose of steganography?

○ ○ ○ Checking data integrity

○ ○ ○ Verifying hash values

👍 ✔ ☑ Hiding data within another piece of data (☑ Your answer)

○ ○ ○ Encrypting data

☑ You correctly answered this question.

▸ In the field of data security, the term "Tokenization" refers to the process of replacing sensitive data with nonsensitive information which holds a reference to the original data and enables its

processing but has no value when breached.

○ ✔ 👎 True (❌ Missed)

👍 ○ ➖ False (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ Replacing password characters in a password field with a series of asterisks is an example of:

👍 ✔ ☑ Data masking (☑ Your answer)

○ ○ ○ Tokenization

○ ○ ○ Anonymization

○ ○ ○ Pseudo-anonymization

☑ You correctly answered this question.

▶ A hash function is a mathematical algorithm that maps data of arbitrary size to a fixed-size hash value, typically represented as a short string of characters. The hash function result, also known as a digest or checksum, provides a unique representation of the original data input. The functionality of hash functions relies on the fact that if there is any change to the data after the original hash was generated, the new hash value calculated after content modification will be different from the original result because hash functions are designed to be sensitive to changes in the input data.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▶ Hash functions find use in a variety of applications, including:

○ ○ ○ Cryptography

○ ○ ○ Data integrity verification

○ ○ ○ Password verification and storage

○ ○ ○ Digital signatures

○ ○ ○ Blockchain technology

👆 ✔ ☑ All of the above (☑ Your answer)

☑ You correctly answered this question.

▶ Which of the answers listed below refers to a cryptographic hash function that has been widely used in the past but is now considered deprecated for security-sensitive applications due to known vulnerabilities?

👆 ✔ ☑ MD5 (☑ Your answer)

〇 〇 〇 SHA

〇 〇 〇 CRC

〇 〇 〇 HMAC

☑ You correctly answered this question.

Your Final Report	
Total marks	25
Total Questions	25
Questions correctly answered	17
Success ratio	68%
Marks secured	17
Percentage secured	68%

Security+

CompTIA Security+ Certification Exam SY0-601 Practice Tests

CompTIA Security+ Certification SY0-601 Practice Tests by Exam Topic

Exam Glossaries

Security+

CompTIA Security+ Certification Exam SY0-701 Practice Tests

-->