CompTIA Security+ Certification Exam SY0-701 Practice Test 5

▸ Which of the following answers refers to a family of cryptographic hash functions designed for various security-related applications, including digital signatures, password storage, secure communications, and data integrity verification?

○ ○ ○ RSA

○ ○ ○ AES

○ ○ ○ PKCS

👍 ✔ ☑ SHA (☑ Your answer)

☑ You correctly answered this question.

▸ Which of the hash functions listed below offers the highest level of security?

👍 ○ ☒ MD5 (✖ Your answer)

○ ✔ 👎 SHA-3 (✖ Missed)

○ ○ ○ RIPEMD-160

○ ○ ○ HMAC

☒ Your answer to this question is incorrect or incomplete.

▸ Which of the following combines a cryptographic hash function with a secret key to provide a means of verifying both the authenticity and integrity of a message or data?

○ ○ ○ MD5

○ ○ ○ DSA

✔ ☑ HMAC (☑ Your answer)

○ ○ ○ DES

☑ You correctly answered this question.

▸ Which of the answers listed below refers to a non-cryptographic hash function often used for error-checking purposes?

○ ○ ○ MD5

👆 ✔ ☑ CRC (☑ Your answer)

○ ○ ○ SHA

○ ○ ○ RIPEMD

☑ You correctly answered this question.

▸ Which of the following answers refers to a type of additional input that increases password complexity and provides better protection against brute-force, dictionary, and rainbow table attacks?

○ ○ ○ Seed

○ ○ ○ IV

👆 ✔ ☑ Salt (☑ Your answer)

○ ○ ○ Shim

☑ You correctly answered this question.

▸ A pseudo-random data added to a password before hashing is referred to as:

○ ○ ○ Shim

○ ✔ 👎 Salt (✖ Missed)

○ ○ ○ IV

👆 ○ ▬ Seed (✖ Your answer)

▬ Your answer to this question is incorrect or incomplete.

▸ Which cryptographic technique is used to prevent the effectiveness of rainbow tables in cracking hashed passwords?

○ ○ ○ Data masking

○ ○ ○ Two-Factor Authentication (2FA)

👍 ○ ▬ Key stretching (✖ Your answer)

○ ✔ 👎 Salting (✖ Missed)

▬ Your answer to this question is incorrect or incomplete.

▸ Which of the answers listed below refers to a cryptographic technique that verifies the authenticity and integrity of digital documents or messages by using a unique encrypted identifier from the sender?

👍 ✔ ☑ Digital signature (☑ Your answer)

○ ○ ○ Cryptographic hash function

○ ○ ○ Digital certificate

○ ○ ○ Asymmetric encryption

☑ You correctly answered this question.

▸ Which of the following answers refer to algorithms used for generating and verifying digital signatures? (Select 3 answers)

👍 ✔ ☑ ECDSA (☑ Your answer)

👍 ✔ ☑ RSA (☑ Your answer)

☐ ☐ ☐ ECDHE

👍 ✔ ☑ DSA (☑ Your answer)

☐ ☐ ☐ GPG/PGP

☑ You correctly answered this question.

▸ Which of the answers listed below refer to DSA? (Select 2 answers)

☐ ✔ 👎 Specifically designed for creating and verifying digital signatures (✖ Missed)

☐ ☐ ☐ Primarily used for secure communication and digital signatures

👍 ✔ ☑ Not well suited for data encryption (DSA is not an encryption algorithm) (☑ Your answer)

☐ ☐ ☐ Used for both encryption and digital signatures in various applications

👍 ☐ ➖ Based on the mathematical properties of large prime numbers (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the following answers refer to the characteristic features of RSA? (Select 2 answers)

☐ ☐ ☐ Based on the discrete logarithm problem

👍 ✔ ☑ Primarily used for secure communication and digital signatures (☑ Your answer)

☐ ✔ 👎 Used for data encryption (✖ Missed)

👍 ☐ ➖ Specifically designed for creating and verifying digital signatures (✖ Your answer)

☐ ☐ ☐ Not well suited for data encryption

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the answers listed below best describe the characteristics of ECDSA? (Select 2 answers)

👍 ✔ ☑ Used for digital signatures (☑ Your answer)

☐ ☐ ☐ Can be used for both encryption and digital signatures

☐ ✔ 👎 Does not include a native encryption function (✖ Missed)

👍 ☐ ➖ Enables the encryption of data (✖ Your answer)

☐ ☐ ☐ Based on the mathematical properties of large prime numbers

➖ Your answer to this question is incorrect or incomplete.

▶ Given the computational limitations of IoT devices, smartcards, and mobile devices, which of the following digital signature algorithms would be the most efficient choice due to its smaller key size and lower processing requirements?

○ ○ ○ RSA

○ ○ ○ ECDHE

○ ○ ○ DSA

○ ✔ 👎 ECDSA (✖ Missed)

👆 ○ ▬ ECC (✖ Your answer)

▬ Your answer to this question is incorrect or incomplete.

▸ Key stretching is a cryptographic technique that enhances the security of sensitive data, such as cryptographic keys and passwords. It works by repeatedly applying a resource-intensive function or algorithm to the input data, thus increasing the computational effort required to derive the original key or password, which makes the data more resistant to brute-force, dictionary, or rainbow table attacks.

○ ✔ 👎 True (✖ Missed)

👆 ○ ▬ False (✖ Your answer)

▬ Your answer to this question is incorrect or incomplete.

▸ Which of the following is an example of a key stretching algorithm?

○ ○ ○ RIPEMD

○ ○ ○ SHA

○ ○ ○ HMAC

👆 ✔ ☑ PBKDF2 (☑ Your answer)

☑ You correctly answered this question.

▸ The term "Open public ledger" is used to describe a distributed database stored across multiple computers in a P2P network.

👆 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

▸ Blockchain technology is an example of:

◯ ◯ ◯ Online payment gateway

◯ ◯ ◯ Centralized database

👆 ✔ ☑ Open public ledger (☑ Your answer)

◯ ◯ ◯ Cloud storage system

☑ You correctly answered this question.

▸ Which of the answers listed below refers to a set of standards and specifications that define various cryptographic techniques, including formats for public keys, private keys, digital signatures, and digital certificates?

◯ ◯ ◯ ITIL

👆 ◯ ⊟ RFC (✖ Your answer)

◯ ✔ 👎 PKCS (✖ Missed)

◯ ◯ ◯ ISO/IEC

⊟ Your answer to this question is incorrect or incomplete.

▸ Which of the following defines a file format for storing and exchanging personal identity information, including private keys and digital certificates?

◯ ◯ ◯ P10

👆 ◯ ⊟ P11 (✖ Your answer)

◯ ✔ 👎 P12 (✖ Missed)

◯ ◯ ◯ P13

⊟ Your answer to this question is incorrect or incomplete.

▶ A type of digital document that verifies the identity of an individual, device, service, or organization in online communications is known as:

○ ○ ○ Encryption key

○ ✔ 👎 Digital certificate (✖ Missed)

○ ○ ○ Identity token

👆 ○ ➖ Digital signature (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ What is the role of Registration Authority (RA) in PKI? (Select 2 answers)

☐ ✔ 👎 Accepting requests for digital certificates (✖ Missed)

👆 ☐ ➖ Validating digital certificates (✖ Your answer)

☐ ✔ 👎 Authenticating the entity making the request (✖ Missed)

☐ ☐ ☐ Providing backup source for cryptographic keys

👆 ☐ ➖ Issuing digital certificates (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the answers listed below refers to a trusted third party responsible for issuing, revoking, and managing digital certificates?

○ ○ ○ RA

○ ○ ○ DN

👆 ✔ ☑ CA (☑ Your answer)

○ ○ ○ CSP

☑ You correctly answered this question.

▶ Which of the following answers refers to a means for periodic publication of all digital certificates that have been revoked?

👆 ✔ ☑ CRL (☑ Your answer)

○ ○ ○ OSPF

○ ○ ○ RA

○ ○ ○ CSR

☑ You correctly answered this question.

▸ Which of the answers listed below refers to a protocol that enables on-demand querying of the revocation status of a digital certificate?

○ ○ ○ CSP

👆 ✔ ☑ OCSP (☑ Your answer)

○ ○ ○ DN

○ ○ ○ CRL

☑ You correctly answered this question.

▸ What is the fastest way to check the validity of a single digital certificate?

○ ○ ○ CSR

○ ○ ○ DN

○ ○ ○ CRL

👆 ✔ ☑ OCSP (☑ Your answer)

☑ You correctly answered this question.

Your Final Report	
Total marks	31
Total Questions	25
Questions correctly answered	13
Success ratio	52%
Marks secured	18
Percentage secured	58.06%

CompTIA Security+ Certification Exam SY0-601 Practice Tests

Security+ Practice Test 1 (/comptia-security-plus-practice-test-1-exam-sy0-601)

Security+ Practice Test 2 (/comptia-security-plus-practice-test-2-exam-sy0-601)

Security+ Practice Test 3 (/comptia-security-plus-practice-test-3-exam-sy0-601)

Security+ Practice Test 4 (/comptia-security-plus-practice-test-4-exam-sy0-601)

Security+ Practice Test 5 (/comptia-security-plus-practice-test-5-exam-sy0-601)

Security+ Practice Test 6 (/comptia-security-plus-practice-test-6-exam-sy0-601)

Security+ Practice Test 7 (/comptia-security-plus-practice-test-7-exam-sy0-601)

Security+ Practice Test 8 (/comptia-security-plus-practice-test-8-exam-sy0-601)

Security+ Practice Test 9 (/comptia-security-plus-practice-test-9-exam-sy0-601)

Security+ Practice Test 10 (/comptia-security-plus-practice-test-10-exam-sy0-601)

Security+ Practice Test 11 (/comptia-security-plus-practice-test-11-exam-sy0-601)

Security+ Practice Test 12 (/comptia-security-plus-practice-test-12-exam-sy0-601)

Security+ Practice Test 13 (/comptia-security-plus-practice-test-13-exam-sy0-601)

Security+ Practice Test 14 (/comptia-security-plus-practice-test-14-exam-sy0-601)

Security+ Practice Test 15 (/comptia-security-plus-practice-test-15-exam-sy0-601)

Security+ Practice Test 16 (/comptia-security-plus-practice-test-16-exam-sy0-601)

Security+ Practice Test 17 (/comptia-security-plus-practice-test-17-exam-sy0-601)

Security+ Practice Test 18 (/comptia-security-plus-practice-test-18-exam-sy0-601)

Security+ Practice Test 19 (/comptia-security-plus-practice-test-19-exam-sy0-601)

Security+ Practice Test 20 (/comptia-security-plus-practice-test-20-exam-sy0-601)

Security+ Practice Test 21 (/comptia-security-plus-practice-test-21-exam-sy0-601)

Security+ Practice Test 22 (/comptia-security-plus-practice-test-22-exam-sy0-601)

Security+ Practice Test 23 (/comptia-security-plus-practice-test-23-exam-sy0-601)

Security+ Practice Test 24 (/comptia-security-plus-practice-test-24-exam-sy0-601)

Security+ Practice Test 25 (/comptia-security-plus-practice-test-25-exam-sy0-601)

Security+ Practice Test 26 (/comptia-security-plus-practice-test-26-exam-sy0-601)

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

Social Engineering Quiz (/comptia-security-plus-certification-exam-sy0-601-social-engineering-quiz)

Malware Quiz (/comptia-security-plus-certification-exam-sy0-601-malware-quiz)

Password Attacks Quiz (/comptia-security-plus-certification-exam-sy0-601-password-attacks-quiz)

Exam Glossaries

Security+

CompTIA Security+ Certification Exam SY0-701 Practice Tests

CompTIA Security+ SY0-701 Exam Objectives (https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-701-exam-objectives-(5-0).pdf)

-->