# CompTIA Security+ Certification Exam SY0-701 Practice Test 3

▶ The MIME specification extends the email message format beyond plain text, enabling the transfer of graphics, audio, and video files over the Internet mail system. S/MIME is an enhanced version of the MIME protocol that enables email security features by providing encryption, authentication, message integrity, and other related services.

👍 ✔ ☑ True (☑ Your answer)

○ ○ ○ False

☑ You correctly answered this question.

---

▶ What is the name of a network protocol that enables secure file transfer over SSH?

○ ○ ○ TFTP

👍 ✔ ☑ SFTP (☑ Your answer)

○ ○ ○ Telnet

○ ○ ○ FTPS

☑ You correctly answered this question.

---

▶ SFTP is an extension of the FTP protocol that adds support for SSL/TLS encryption.

👍 ○ ▬ True (✖ Your answer)

○ ✔ 👎 False (✖ Missed)

▬ Your answer to this question is incorrect or incomplete.

---

A type of cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked

computers is known as:

- 👆 ⚪ ⊟ RDP (✖ Your answer)

- ⚪ ✔ 👎 SSH (✖ Missed)

- ⚪ ⚪ ⚪ Telnet

- ⚪ ⚪ ⚪ SCP

⊟ Your answer to this question is incorrect or incomplete.

---

▶ Which of the answers listed below refers to a suite of protocols and technologies providing encryption, authentication, and data integrity for network traffic?

- 👆 ⚪ ⊟ TLS (✖ Your answer)

- ⚪ ⚪ ⚪ SSH

- ⚪ ✔ 👎 IPsec (✖ Missed)

- ⚪ ⚪ ⚪ VPN

⊟ Your answer to this question is incorrect or incomplete.

---

▶ Which part of IPsec provides authentication, integrity, and confidentiality?

- ⚪ ⚪ ⚪ SPD

- ⚪ ⚪ ⚪ PFS

- 👆 ⚪ ⊟ AH (✖ Your answer)

- ⚪ ✔ 👎 ESP (✖ Missed)

⊟ Your answer to this question is incorrect or incomplete.

---

▶ A system that uses public network (such as the Internet) as a means for creating private encrypted connections between remote locations is referred to as:

- ⚪ ⚪ ⚪ WWAN

- 👆 ✔ ☑ VPN (☑ Your answer)

- ⚪ ⚪ ⚪ PAN

○ ○ ○ VLAN

☑ You correctly answered this question.

▶ Which protocol enables secure, real-time delivery of audio and video over an IP network?

○ ○ ○ S/MIME

👆 ○ ◼ RTP (✖ Your answer)

○ ○ ○ SIP

○ ✔ 👎 SRTP (✖ Missed)

◼ Your answer to this question is incorrect or incomplete.

▶ An encryption protocol primarily used in Wi-Fi networks implementing the WPA2 security standard is called:

👆 ○ ◼ TKIP (✖ Your answer)

○ ✔ 👎 CCMP (✖ Missed)

○ ○ ○ SSL

○ ○ ○ IPsec

◼ Your answer to this question is incorrect or incomplete.

▶ A security protocol designed to improve the security of existing WEP implementations is known as:

👆 ○ ◼ WPA2 (✖ Your answer)

○ ○ ○ RC4

○ ○ ○ CCMP

○ ✔ 👎 TKIP (✖ Missed)

◼ Your answer to this question is incorrect or incomplete.

▶ Which of the following answers refer(s) to deprecated/insecure encryption protocols and cryptographic hash functions? (Select all that apply)

👍 ✔ ☑ DES (☑ Your answer)

☐ ☐ ☐ AES-256

👍 ✔ ☑ MD5 (☑ Your answer)

☐ ☐ ☐ ECC

👍 ✔ ☑ SHA-1 (☑ Your answer)

👍 ✔ ☑ SSL (☑ Your answer)

👍 ✔ ☑ RC4 (☑ Your answer)

☑ You correctly answered this question.

---

▸ Which cryptographic protocol is designed to provide secure communications over a computer network and is the successor to SSL?

○ ○ ○ IPsec

👍 ✔ ☑ TLS (☑ Your answer)

○ ○ ○ AES

○ ○ ○ CCMP

☑ You correctly answered this question.

---

▸ Examples of techniques used for encrypting information include symmetric encryption (also called public-key encryption) and asymmetric encryption (also called secret-key encryption, or session-key encryption).

👍 ○ ⬛ True (✖ Your answer)

○ ✔ 👎 False (✖ Missed)

⬛ Your answer to this question is incorrect or incomplete.

---

▸ In asymmetric encryption, any message encrypted with the use of a public key can only be decrypted by applying the same algorithm and a matching private key (and vice versa).

○ ✔ 👎 True (✖ Missed)

👎 ⭕ ➖ False (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the algorithms listed below are not symmetric ciphers? (Select 3 answers)

☐ ☐ ☐ AES

👍 ☐ ➖ DES (✖ Your answer)

☐ ✔ 👎 DHE (✖ Missed)

👍 ✔ ☑ ECC (☑ Your answer)

☐ ☐ ☐ IDEA

👍 ☐ ➖ RC4 (✖ Your answer)

☐ ✔ 👎 RSA (✖ Missed)

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the following algorithms do(es) not fall into the category of asymmetric encryption? (Select all that apply)

👍 ✔ ☑ AES (☑ Your answer)

☐ ✔ 👎 DES (✖ Missed)

☐ ☐ ☐ DHE

☐ ☐ ☐ ECC

☐ ✔ 👎 IDEA (✖ Missed)

👍 ✔ ☑ RC4 (☑ Your answer)

👍 ☐ ➖ RSA (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

▶ The term "KEK" refers to a type of cryptographic key often used in key management systems to add an additional layer of security when encrypting and decrypting other cryptographic keys.

○ ✔ 👎 True (✖ Missed)

👍 ○ ➖ False (✖ Your answer)

➖ Your answer to this question is incorrect or incomplete.

---

▶ Which of the answers listed below refers to a shared secret authentication method used in WPA, WPA2, and EAP?

○ ✔ 👎 PSK (✖ Missed)

○ ○ ○ 802.1X

👍 ○ ➖ SAE (✖ Your answer)

○ ○ ○ TKIP

➖ Your answer to this question is incorrect or incomplete.

---

▶ Which of the following answers refers to a protocol used to set up secure connections and exchange of cryptographic keys in IPsec VPNs?

👍 ○ ➖ SSL (✖ Your answer)

○ ✔ 👎 IKE (✖ Missed)

○ ○ ○ ESP

○ ○ ○ DHE

➖ Your answer to this question is incorrect or incomplete.

---

▶ Which of the answers listed below refers to a key exchange protocol that generates temporary keys for each session, providing forward secrecy to protect past and future communications?

○ ○ ○ PFS

○ ○ ○ SHA

👍 ○ ➖ PGP (✖ Your answer)

○ ✔ 👎 DHE (✖ Missed)

➖ Your answer to this question is incorrect or incomplete.

▶ Which of the following answers refers to a cryptographic key exchange protocol that leverages ECC for enhanced security and efficiency?

○ ○ ○  S/MIME

○ ✔ 👎  ECDHE (✖ Missed)

○ ○ ○  DHE

👆 ○ ⬛  ECDSA (✖ Your answer)

⬛ Your answer to this question is incorrect or incomplete.

---

▶ Which of the answers listed below refers to a solution designed to strengthen the security of session keys?

👆 ○ ⬛  ECB (✖ Your answer)

○ ✔ 👎  PFS (✖ Missed)

○ ○ ○  EFS

○ ○ ○  PFX

⬛ Your answer to this question is incorrect or incomplete.

---

▶ Which of the following answers refers to a public-key cryptosystem that leverages the mathematical properties of large prime numbers to facilitate secure key exchange, create digital signatures, and encrypt data?

👆 ○ ⬛  ECC (✖ Your answer)

○ ✔ 👎  RSA (✖ Missed)

○ ○ ○  PKI

○ ○ ○  DSA

⬛ Your answer to this question is incorrect or incomplete.

---

▶ Which cryptographic solution would be best suited for low-power devices, such as IoT devices, embedded systems, and mobile devices?

○ ✔ 👎 ECC (✖ Missed)

👆 ○ ◼ DES (✖ Your answer)

○ ○ ○ RSA

○ ○ ○ AES

◼ Your answer to this question is incorrect or incomplete.

▸ Which of the cryptographic algorithms listed below is the least vulnerable to attacks?

👆 ✔ ☑ AES (☑ Your answer)

○ ○ ○ DES

○ ○ ○ RC4

○ ○ ○ 3DES

☑ You correctly answered this question.

| Your Final Report | |
|---|---|
| **Total marks** | 34 |
| **Total Questions** | 25 |
| **Questions correctly answered** | 6 |
| **Success ratio** | 24% |
| **Marks secured** | 13 |
| **Percentage secured** | 38.24% |

**Security+**

# 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 14 (/comptia-security-plus-practice-test-14-exam-sy0-601)

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

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

**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)**

-->