Chp 7 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/8/2022 8:25:53 pm • Time spent: 07:01

Score: 98% Passing Score: 80%

Question 1: ✔ Correct

Which utility would you MOST likely use on OS X to encrypt and decrypt data and messages?

- ➡ GPG
- IPsec
- PGP
- VPN

EXPLANATION

GNU Privacy Guard (GPG) is a command line utility that's used to encrypt and decrypt data and messages. GPG is a open source utility and can be used on many different systems, including Windows, Linux, Android, and Apple's OS X.

Pretty Good Privacy (PGP) is an older utility used to encrypt and decrypt data and messages. PGP was purchased a while ago and commercialized. It's owned by NortonLifeLock, formally known as Symantec, and provides products that can protect all sorts of devices, even smartphones. While PGP can be used on OS X, GPG is used by default.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. A VPN is not used on OS X to encrypt and decrypt data and messages.

IPSec is a protocol used to encrypt VPN communication.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_ipsec_secp7.question.fex

Question 2: ✔ Correct

You create a new document and save it to a hard drive on a file server on your company's network. Then you employ an encryption tool to encrypt the file using AES. This activity is an example of accomplishing which security goal?

- Availability
- ➡ Confidentiality
- Non-repudiation
- Integrity

EXPLANATION

Encrypting a file while it is stored on a hard drive is usually done to provide protection for the object's confidentiality.

Hashing is used to provide integrity. Using mechanisms like backups and avoiding single points of failure provide availability protection. Non-repudiation is usually provided for during a secured communication, not while a file is stored on a hard drive.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_confident_secp7.question.fex

Question 3: ✔ Correct

You've used BitLocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TPM chip, so you've used an external USB flash drive to store the BitLocker startup key.

You use EFS to encrypt the C:\Secrets folder and its contents.

Which of the following is true in this scenario? (Select two.)

- [ ] Only the user who encrypted the C:\Secrets\confidential.docx file is able to boot the computer from the encrypted hard disk.
- [ ] The EFS encryption process will fail.
- [x] By default, only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it.
- [x] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will be saved in an unencrypted state.
- [ ] Any user who is able to boot the computer from the encrypted hard disk will be able to open the C:\Secrets\confidential.docx file.
- [ ] If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will remain in an encrypted state.

EXPLANATION

BitLocker uses full volume encryption, while EFS is used to encrypt individual files and folders. The following are true in this scenario:

- If the C:\Secrets\confidential.docx file is copied to an external USB flash drive, the file will be saved in an unencrypted state.
- Only the user who encrypted the C:\Secrets\confidential.docx file will be able to open it by default.

With BitLocker enabled, any user who has the appropriate startup key or PIN is able to boot the system from the encrypted drive. However, only the user who encrypted the C:\Secrets\ folder will be able to access files within it unless additional user accounts are explicitly added.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_encrypt_03_secp7.question.fex

Question 4: ✔ Correct

Hashing algorithms are used to perform which of the following activities?

- Provide a means for exchanging small amounts of data securely over a public network.
- Encrypt bulk data for communications exchange.
- Create a message digest.
- Provide for non-repudiation.

EXPLANATION

Hashing algorithms are used to create a message digest to ensure that data integrity is maintained. A sender creates a message digest by performing the hash function on the data files that are transmitted. The receiver performs the same action on the data received and compares the two message digests. If they are the same, the data was not altered.

Symmetric algorithms are used to encrypt bulk data for communications exchange. Asymmetric algorithms provide a means for exchanging small amounts of data securely over a public network. Both symmetric and asymmetric algorithms provide non-repudiation.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_cryp_hash_digest_secp7.question.fex

Question 5: ✔ Correct

Which of the following database encryption methods encrypts the entire database and all backups?

- ➡ (●) Transparent Data Encryption (TDE)
- ( ) Column-level
- ( ) Application-level
- ( ) Bitlocker

EXPLANATION

Transparent Data Encryption (TDE) encrypts the entire database and all backups. TDE:

- encrypts data at rest, which is data not being currently used.
- is called transparent because when an authorized user needs to access the data, it is automatically decrypted so the user does not see the process or need to do anything extra.

Column-level encryption allows the administrator to encrypt each column separately.

In application-level encryption, the program that is used to create or modify the data is responsible for encrypting the data.

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_trans_data_secp7.question.fex

Question 6: ✔ Correct

Which of the following are true of Triple DES (3DES)?

- Uses the Rijndael block cipher
- ➡ Key length is 168 bits
- Can easily be broken
- Uses 64-bit blocks with 128-bit keys

EXPLANATION

Triple DES:

- Applies DES three times
- Uses a 168-bit key

Advanced Encryption Standard (AES) uses the Rijndael block cipher.

DES can easily be broken.

International Data Encryption Algorithm (IDEA) uses 64-bit blocks with 128-bit keys.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_length_secp7.question.fex

Question 7: ✔ Correct

You are concerned that if a private key is lost, all documents encrypted with your private key will be inaccessible. Which service should you use to solve this problem?

- RA
- ➡ Key escrow
- OCSP
- CSP

EXPLANATION

Key escrow backs up private keys to a third-party organization outside of the company. If the private key is lost, you can recover the key from escrow.

Online Certificate Status Protocol (OCSP) is a protocol used to check the status of an individual digital certificate to verify whether it is good or has been revoked. A Cryptographic Service Provider (CSP) resides on the client and generates the key pair. A registration authority (RA) verifies the information included in a certificate request.

REFERENCES

7.5.10 Certificate Concepts Facts

q_cert_concepts_escrow_02_secp7.question.fex

Question 8: ✔ Correct

Which of the following is used to verify that a downloaded file has not been altered?

- Private key
- Hash
- Symmetric encryption
- Asymmetric encryption

EXPLANATION

A hash is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. For example, when users post files for download, they often create a hash value for the file. After you download the file, you can create a hash using the same algorithm. If the hash values match, you know that the file you have matches the original file.

Symmetric encryption is typically used for fast data encryption. Asymmetric encryption is used for encrypting small amounts of data or exchanging keys used with symmetric encryption. A private key is one of the keys used in asymmetric encryption.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_cryp_hash_hash_01_secp7.question.fex

Question 9: ✔ Correct

Which technology was developed to help improve the efficiency and reliability of checking the validity status of certificates in large, complex environments?

- Certificate Revocation List
- Private key recovery
- Key escrow
- ➡ Online Certificate Status Protocol

EXPLANATION

Online Certificate Status Protocol (OCSP) is the technology developed to improve the efficiency and reliability of checking the validity status of certificates in large, complex environments. OCSP allows clients to query a CA or registration authority (RA) and quickly learn whether a certificate is valid or has been revoked.

OCSP is a significant improvement over the CRL mechanism. CRLs were static lists that were distributed periodically to CAs and RAs. However, CRLs were often out of date. Key escrow and private key recovery are not related to certificate status checking.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_ocsp_secp7.question.fex

Question 10: ✔ Correct

Which of the following is a direct integrity protection?

- Symmetric encryption
- Digital envelope
- Asymmetric encryption
- ➡ Digital signature

EXPLANATION

A digital signature is a direct integrity protection. It includes the use of hashing, which detects changes to integrity.

Digital envelopes, symmetric encryption, and asymmetric encryption do not provide direct integrity protection, nor do they use hashing to provide integrity protection.

REFERENCES

5.10.3 Network Application Facts

7.2.3 Combining Cryptographic Methods

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_digital_01_secp7.question.fex

Question 11: ✔ Correct

When a sender encrypts a message using their own private key, which security service is being provided to the recipient?

- Availability
- Integrity
- Non-repudiation
- Confidentiality

EXPLANATION

When a sender encrypts a message using their own private key, the security service of non-repudiation is being provided to the recipient. The encrypted message can be freely decrypted using the public key. Because only the sender knows the private key, encrypting the message with the private key proves that only the sender could have sent the message.

Integrity is provided when hashing is used. Because the public key is freely available, the encryption does not provide confidentiality (anyone with the public key could read the message contents). Availability is not provided by any form of cryptography.

REFERENCES

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_non_rep_secp7.question.fex

Question 12: ✔ Correct

A private key has been stolen. Which action should you take to deal with this crisis?

- Delete the public key
- Place the private key in escrow
- Add the digital certificate to the CRL
- Recover the private key from escrow

EXPLANATION

If a private key--a digital certificate or digital signature--is compromised (especially by theft), it should be added to the CRL. This prevents any future use of the key/certificate and prevents impersonation attacks.

There is no need to delete the public key because CRLs deal with any attempted use of the private key. The private key should have been placed in escrow at the beginning of its lifetime if key recovery was desired. In this situation, key recovery is not necessary.

REFERENCES

7.5.10 Certificate Concepts Facts

q_cert_concepts_crl_01_secp7.question.fex

Question 13: ✔ Correct

Which of the following security solutions would prevent a user from reading a file that she did not create?

- BitLocker
- VPN
- IPsec
- ➡ EFS

EXPLANATION

EFS is a Windows file encryption option that encrypts individual files so that only the user who created the file can open it. Decryption is automatic when the file owner opens it. Other users cannot open the encrypted file unless specifically authorized.

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_encrypt_02_secp7.question.fex

Question 14: ✔ Correct

What is the most obvious means of providing non-repudiation in a cryptography system?

- Shared secret keys
- Digital signatures
- Hashing values
- Public keys

EXPLANATION

Digital signatures, which are private keys from an asymmetric cryptographic system, are the most obvious means of providing non-repudiation. Only a single person is in possession of their private key. If a message is found with their digital signature, they are the only user who could possibly have created and transmitted it.

Public keys are useful for restricting delivery, such as using them as digital envelopes, but they don't provide non-repudiation. Hashing values protect integrity, but they don't provide non-repudiation. Shared secret keys do not provide true non-repudiation because two entities hold copies of the shared key.

REFERENCES

5.10.3 Network Application Facts

7.2.3 Combining Cryptographic Methods

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_digital_02_secp7.question.fex

Question 15: ✔ Correct

You would like to implement BitLocker to encrypt data on a hard disk, even if it is moved to another system. You want the system to boot automatically without providing a startup key on an external USB device.

What should you do?

- Use a PIN instead of a startup key.
- ➡ Enable the TPM in the BIOS.
- Save the startup key to the boot partition.
- Disable USB devices in the BIOS.

EXPLANATION

When a system boots, the startup key is required to unlock the encrypted volume. The system startup key can be saved in the Trusted Platform Module (TPM). With the startup key saved in the TPM, the system can start without additional intervention.

The system will not start without the startup key. Without a TPM, the startup key must be stored on a USB drive. You can require a PIN in addition to a startup key, but the PIN cannot replace the startup key. Storing the startup key on the boot drive would expose it to compromise.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_file_encryption_tpm_01_secp7.question.fex

Question 16: ✔ Correct

Which type of password attack employs a list of pre-defined passwords that it tries against a login prompt?

- Birthday attack
- ➡ Dictionary attack
- Collision attack
- Downgrade attack

EXPLANATION

A dictionary attack is a type of brute-force attack. A hacker uses a list of words and phrases to try to guess the decryption key.

- Dictionary attacks work well if weak passwords are used.
- Using longer and uncommon passphrases is the best way to secure data against these attacks.

A collision attack tries to find two inputs that produce the same hash value. This type of attack is often used on digital signatures.

A birthday attack combines a collision attack and brute-force attack. The name is taken from the birthday probability math problem.

A downgrade attack forces the system to use an older, less secure communication protocol.

REFERENCES

7.1.13 Cryptographic Attack Facts

q_cryp_attacks_dict_secp7.question.fex

Question 17: ✔ Correct

Which of the following algorithms are used in asymmetric encryption? (Select two.)

- [x] Diffie-Hellman
- [ ] AES
- [ ] Blowfish
- [x] RSA
- [ ] Twofish

EXPLANATION

RSA and Diffie-Hellman are asymmetric algorithms. RSA, one of the earliest encryption algorithms, can also be used for digital signatures. The Diffie-Hellman Protocol was created in 1976 but is still in use today in technologies such as SSL, SSH, and IPsec.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_asym_02_secp7.question.fex

Question 18: ✔ Correct

Which of the following would require that a certificate be placed on the CRL?

- The certificate validity period is exceeded.
- The encryption key algorithm is revealed.
- ➡ The private key is compromised.
- The signature key size is revealed.

EXPLANATION

Certificates are published to the Certificate Revocation List (CRL) when a condition compromises the integrity of the certificate. If the private key is compromised (discovered), the certificate is no longer proof of identity.

Certificates do not need to be placed on the CRL if their validity period expires. In this case, the certificate simply expires. Knowing the signature key size or the encryption key algorithm does not compromise the integrity of the certificate.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_crl_03_secp7.question.fex

Question 19: ✔ Correct

A receiver wants to verify the integrity of a message received from a sender. A hashing value is contained within the digital signature of the sender.

Which of the following must the receiver use to access the hashing value and verify the integrity of the transmission?

- Receiver's public key
- Receiver's private key
- Sender's private key
- Sender's public key

EXPLANATION

Digital signatures are created using the sender's private key. Therefore, only the sender's public key can be used to verify and open any data encrypted with the sender's private key. The recipient's private and public keys are not involved in this type of cryptography situation. Often, the hashing value of a message is protected by the sender's private key (their digital signature). The recipient must extract the original hashing value.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_asys_sys_encrypt_hash_secp7.question.fex

Question 20: ✔ Correct

In the certificate authority trust model known as a hierarchy, where does trust start?

- Registration authority
- Issuing CA
- Third-party CA
- ➡ Root CA

EXPLANATION

Trust starts at the Root CA in all trust models.

An Issuing CA can be a Root CA or a CA at any level below the root.

A third-party CA may be the source of trust, but even then, the trust starts at a Root CA located somewhere.

A registration authority (RA) is a limited-functionality CA where certificates are verified, but no new certificates can be issued.

REFERENCES

7.5.4 Certificate Types Facts

q_cert_types_ca_secp7.question.fex

Question 21: ✔ Correct

Which of the following should you set up to ensure encrypted files can still be decrypted if the original user account becomes corrupted?

- GPG
- DRA
- PGP
- VPN

EXPLANATION

If a user account becomes corrupted or the password is forgotten, any encrypted files are lost. To help remedy this, a data recovery agent (DRA) can be set up. The DRA is simply another account that can decrypt the encrypted files.

Pretty Good Privacy (PGP) is an older utility used to encrypt and decrypt data and messages.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site.

GNU Privacy Guard (GPG) is a command line utility that's used to encrypt and decrypt data and messages.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_dra_secp7.question.fex

Question 22: ✔ Correct

Which term means a cryptography mechanism that hides secret communications within various forms of data?

- Algorithm
- Ciphertext
- Cryptanalysis
- ➡ Steganography

EXPLANATION

Steganography is the cryptography mechanism that hides secret communications within various forms of data.

Ciphertext is the encrypted form of a message that makes it unreadable to all but those the message is intended for.

Cryptanalysis is the method of recovering original data that has been encrypted without having access to the key used in the encryption process.

A cipher or algorithm is the process or formula used to convert a message or otherwise hide its meaning.

REFERENCES

7.1.2 Cryptography Facts

q_cryp_concepts_stegano_secp7.question.fex

Question 23: ✔ Correct

What is the main function of a TPM hardware chip?

- Control access to removable media
- Generate and store cryptographic keys
- Provide authentication credentials on a hardware device
- Perform bulk encryption in a hardware processor

EXPLANATION

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard. This hardware is used to store and generate cryptographic keys. These keys are used for encryption and authentication, but the TPM does not perform the actual encryption.

A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors perform bulk encryption in hardware rather than software. These processors typically encrypt data using AES or encrypt network traffic using IPsec.

REFERENCES

- 4.2.1 Operating System Hardening
- 4.2.2 Hardening Facts
- 4.2.3 Hardening an Operating System
- 4.2.4 Managing Automatic Updates
- 4.2.6 Configuring Microsoft Defender Firewall
- 4.2.8 Configuring Windows Defender with Firewall Advanced Security
- 7.2.4 Hardware-Based Encryption Devices
- 7.2.5 Cryptographic Implementation Facts
- 7.4.9 File Encryption Facts

q_comb_cryp_tpm_01_secp7.question.fex

Question 24: ✔ Correct

Which of the following is the weakest hashing algorithm?

- ➡ MD5
- SHA-1
- DES
- AES

EXPLANATION

MD5 is the weakest hashing algorithm. It produces a message digest of 128 bits. The larger the message digest, the more secure the hash. SHA-1 is more secure because it produces a 160-bit message digest.

Both DES and AES are symmetric encryption algorithms. DES is weaker than AES.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_weak_secp7.question.fex

Question 25: ✔ Correct

Mary wants to send a message to Sam in such a way that only Sam can read it. Which key should be used to encrypt the message?

- ➡ Sam's public key
- Sam's private key
- Mary's public key
- Mary's private key

EXPLANATION

Sam's public key should be used to encrypt the message. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key.

Encrypting the message using Mary's private key would mean that anyone could read the data using Mary's public key. Encrypting with Mary's public key would mean that only Mary would be able to decrypt it using her private key.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_key_01_secp7.question.fex

Question 26: ✔ Correct

An SSL client has determined that the certificate authority (CA) issuing a server's certificate is on its list of trusted CAs. What is the next step in verifying the server's identity?

- The post-master secret must initiate subsequent communication.
- ➡ The CA's public key must validate the CA's digital signature on the server certificate.
- The master secret is generated from common key code.
- The domain on the server certificate must match the CA's domain name.

EXPLANATION

Once an SSL client has identified a CA as trusted, it uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.

SSL clients verify a server's identity using the following steps:

1. The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing certificate authority is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against man-in-the-middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_ca_02_secp7.question.fex

Question 27: ✕ Incorrect

Which of the following encryption mechanisms offers the least security because of weak keys?

- ~~IDEA~~
- AES
- DES
- TwoFish

EXPLANATION

DES offers the least encryption security of all the cryptography systems in this list. DES has a limitation of 56-bit keys, the weakest of those listed here. The strength of a cryptosystem lies not only in long keys but in the algorithm, initialization vector or method, the proper use of the keyspace, and the protection and management of keys.

AES (128-, 192-, and 256-bit keys), TwoFish (up to 256-bit keys), and IDEA (128-bit keys) all support stronger keys than DES.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_weak_01_secp7.question.fex

Question 28: ✔ Correct

Which form of cryptography is best suited for bulk encryption because it is so fast?

- ➡ Symmetric key cryptography
- Hashing cryptography
- Public key cryptography
- Asymmetric cryptography

EXPLANATION

Symmetric cryptography is best suited for bulk encryption because it is much faster than asymmetric cryptography.

Hashing is not used for encryption; it is only used to verify the integrity of data. Public key cryptography, also known as asymmetric cryptography, is best suited for small amounts of data. Often, asymmetric cryptography is used to exchange symmetric cryptography keys, and then the symmetric cryptography keys are used to encrypt communication traffic.

REFERENCES

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_encrypt_secp7.question.fex

Question 29: ✔ Correct

Which of the following can be classified as a stream cipher?

- AES
- Twofish
- Blowfish
- RC4

EXPLANATION

The most frequently used implementation of symmetric key stream ciphers is Rivest's cipher v4, known as RC4. RC4 uses a variable key up to 256 bits and is commonly used with WEP and SSL. It uses the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA).

Blowfish, Twofish, and AES are all block ciphers.

REFERENCES

7.1.7 Cryptography Algorithms Facts

q_cryp_algorithm_stream_secp7.question.fex

Question 30: ✔ Correct

A birthday attack focuses on which of the following?

- ➡ Hashing algorithms
- VPN links
- E-commerce
- Encrypted files

EXPLANATION

A birthday attack focuses on hashing algorithms. Birthday attacks exploit the probability that two messages using the same hash algorithm produce the same message digest. This is also known as exploiting collision. If two different messages or files produce the same hashing digest, a collision has occurred.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_birthday_01_secp7.question.fex

Question 31: ✔ Correct

When two different messages produce the same hash value, what has occurred?

- Collision
- Hash value
- Birthday attack
- High amplification

EXPLANATION

A collision occurs when two different messages produce the same hash value.

A birthday attack is a brute force attack in which the attacker hashes messages until one with the same hash is found. A hash value is the result of a compressed and transformed message (or some type of data) into a fixed-length value. High amplification means a small change in the message results in a big change in the hashed value.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_collision_secp7.question.fex

Question 32: ✔ Correct

When a cryptographic system is used to protect data confidentiality, what actually takes place?

- Data is available for access whenever authorized users need it.
- ➡ Unauthorized users are prevented from viewing or accessing the resource.
- Encrypted data transmission is prohibited.
- Data is protected from corruption or change.

EXPLANATION

Cryptography is the science of converting data into a secret code to hide a message's meaning during transmission. Cryptography systems provide the following security services:

- Confidentiality by ensuring that only authorized parties can access data.
- Integrity by verifying that data has not been altered in transit.
- Authentication by proving the identity of the sender or receiver.
- Non-repudiation by validating that communications have cone from a particular sender at a particular time.

REFERENCES

7.1.2 Cryptography Facts

7.1.5 Symmetric and Asymmetric Encryption Facts

q_cryp_concepts_basic_secp7.question.fex

Question 33: ✔ Correct

Which standard is most widely used for certificates?

- 802.1x
- ➡ X.509
- SSL v.3.0
- HTTP 1.1

EXPLANATION

The standard for certificates that is most widely used is X.509. This standard defines the key elements that must exist within a certificate. This standard is used by public key infrastructure (PKI), SSL, IPsec, DES, and many other infrastructure components and technologies.

HTTP 1.1 is the latest version of the protocol used to transmit web resources from a web server to a web client. SSL v.3.0 uses certificates, but this is the standard for the secure session protocol for protecting web communications. 802.1x is a networking protocol that defines how to support Extensible Authentication Protocol (EAP) over a wired or wireless LAN.

REFERENCES

7.5.8 Extended Validation Facts

q_cryp_validation_x509_secp7.question.fex

Question 34: ✔ Correct

A PKI is an implementation for managing which type of encryption?

- Steganography
- Hashing
- Asymmetric
- Symmetric

EXPLANATION

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates. Certificates use asymmetric encryption with a public and private key pair.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_pki_02_secp7.question.fex

Question 35: ✔ Correct

You have downloaded a file from the internet. You generate a hash and check it against the original file's hash to ensure the file has not been changed. Which information security goal is this an example of?

- Integrity
- Non-repudiation
- Confidentiality
- Authenticity

EXPLANATION

Creating a hash of a file can be used to validate that the file has not been altered. This validates the integrity of the file.

Applying a digital signature proves that the file is authentic and comes from the correct person.

Applying a digital signature provides non-repudiation. This means that the sender cannot later deny having sent the file.

Confidentiality is achieved through the encrypting of data or obfuscation of data.

REFERENCES

7.2.2 Cryptography Uses and Limitations Facts

q_cryp_limits_integrity_secp7.question.fex

Question 36: ✔ Correct

Your computer system is a participant in an asymmetric cryptography system. You've crafted a message to be sent to another user. Before transmission, you hash the message and then encrypt the hash using your private key. You then attach this encrypted hash to your message as a digital signature before sending it to the other user.

Which protection does the private key-signing activity of this process provide?

- Integrity
- ➡ Non-repudiation
- Confidentiality
- Availability

EXPLANATION

Signing a digital signature with the private key provides non-repudiation.

A digital signature activity as a whole does not provide protection for confidentiality because the original message is sent in clear form. Hashing of any sort at any time, including within a digital signature, provides protection for integrity. No form of cryptography provides protection for availability.

REFERENCES

7.2.5 Cryptographic Implementation Facts

q_comb_cryp_non_rep_secp7.question.fex

Question 37: ✔ Correct

Which of the following does not or cannot produce a hash value of 128 bits?

- RIPEMD
- MD2
- MD5
- SHA-1

EXPLANATION

SHA-1 produces hash values of 160 bits.

MD5 and MD2 both produce hash values of 128 bits.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_cryp_hash_hash_03_secp7.question.fex

Question 38: ✔ Correct

Which of the following is a message authentication code that allows a user to verify that a file or message is legitimate?

- RIPEMD
- SHA
- HMAC
- MD5

EXPLANATION

Hash-Based Message Authentication Code (HMAC) is a type of message authentication code. Like a digital signature, HMAC allows a user to verify that a file or message is legitimate.

SHA is a family of hashes that is used in many different security protocols.

MD5 was developed in 1991 and is no longer viable for security purposes.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_hmac_secp7.question.fex

Question 39: ✔ Correct

You want a security solution that protects the entire hard drive and prevents access even if the drive is moved to another system. Which solution should you choose?

- VPN
- EFS
- BitLocker
- IPsec

EXPLANATION

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

EFS is a Windows file encryption option, but it only encrypts individual files. Encryption and decryption is automatic and dependent upon the file's creator and whether other uses have read permissions.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

REFERENCES

7.4.9 File Encryption Facts

q_file_encryption_encrypt_01_secp7.question.fex

Question 40: ✔ Correct

An attacker is attempting to crack a system's password by matching the password hash to a hash in a large table of hashes he or she has.

Which type of attack is the attacker using?

- RIPEMD
- Rainbow
- Brute force
- Cracking

EXPLANATION

A rainbow attack uses rainbow tables. A rainbow table is a table of passwords and their generated hashes. A hacker can use this table to try to match hashes instead of the actual password.

Cracking is the process of finding a password.

A brute force attack does not use a table of hashes.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_birthday_02_secp7.question.fex