Exam Report: 15.1.9 Practice Questions

Date: 5/26/2020 7:23:05 pm
Time Spent: 1:03

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following terms is the encrypted form of a message that is unreadable except to its intended recipient?

- ciphertext
- steganography
- plain text
- encryption algorithm

Explanation

Ciphertext is the encrypted form of a message that is unreadable except to its intended recipient.

Plain text is the readable form of an encrypted message. The term plain text should not be confused with the term clear text, which is information that is not encrypted. Plain text is information that will eventually be put into an encryption algorithm.

An encryption algorithm is a process or formula used to convert a message or hide its meaning otherwise.

Steganography hides data or a message so that only the sender or the recipient suspects that the hidden data exists.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_CSYS_TERMS_01_EH1]

Question 2: Correct

Bob encrypts a message using a key and sends it to Alice. Alice decrypts the message using the same key. Which of the following types of encryption keys is being used?

- Asymmetric
- Block cipher
- Symmetric
- Digital signature

Explanation

To use a symmetric key, both parties exchange a shared secret key before communications begin.

Asymmetric keys come in pairs and are used in asymmetric encryption. One key is used by the sender to encrypt; the other is used by the receiver to decrypt.

A digital signature is added to a digital certificate to demonstrate the certificate's authenticity.

A block cipher is an encryption algorithm that uses symmetric keys to encrypt blocks of plain text.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_01_EH1]

Question 3: Incorrect

Which of the following is a characteristic of Triple DES (3DES)?

- ~~Uses 64-bit blocks with 128-bit keys~~
- Uses a 168-bit key
- Is easy to break
- Uses the Rijndael block cipher

Explanation

Triple DES (3DES):

- Applies DES three times
- Uses a 168-bit key
- Is used in IPsec as its strongest and slowest encipherment

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

DES is easy to break.

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

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_02_EH1]

Question 4: Correct

Which of the following is the most frequently used symmetric key stream cipher?

- Blowfish
- Advanced Encryption Standard (AES)
- Ron's Cipher v4 (RC4)
- Ron's Cipher v5 (RC5)

Explanation

RC4 is the most frequently used symmetric key stream cipher. RC4 is commonly used with WEP and SSL.

AES, RC5, and Blowfish are all symmetric block ciphers.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_03_EH1]

Question 5: Incorrect

Which of the following is a characteristic of the Advanced Encryption Standard (AES) symmetric block cipher?

- Is used by Pretty Good Privacy (PGP) email encryption.
- ~~Uses up to 16 rounds of substitution and transposition.~~
- Uses the Rijndael block cipher.

Is easy to break.

Explanation

AES is an iterative symmetric key block cipher that uses the following:

- The Rijndael Block Cipher, which is resistant to all known attacks.
- A variable-length block and key length (128-, 192-, or 256-bit keys).

DES is easy to break.

Twofish uses up to 16 rounds of substitution and transposition.

IDEA is used by Pretty Good Privacy (PGP) email encryption.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_05_EH1]

Question 6: Incorrect

Which of the following forms of cryptography is best suited for bulk encryption because of its speed?

- Symmetric cryptography
- Hashing cryptography
- ~~Asymmetric cryptography~~
- Public key 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 data's integrity.

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

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_06_EH1]

Question 7: Correct

Which of the following is the number of keys used in symmetric encryption?

- One
- Two
- Four
- Five

Explanation

Private key, or symmetric, encryption uses a single shared key. Both communicating parties must possess the shared key to encrypt and decrypt messages. The biggest challenge to symmetric cryptography is the constant need to protect the shared private key. This protection must be applied at all times, including during the initial transmission of the shared key between the parties.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography

[e_cryptography_eh1.exam.xml Q_CRY_SYMM_07_EH1]

Question 8: Correct

Which of the following is considered an out-of-band distribution method for private key encryption?

- Using a private fiber network.
- Sending a secured email.
- Using a key distribution algorithm.
- Copying the key to a USB drive.

Explanation

Out-of-band distribution involves manually distributing the key--for example, copying the key to a USB drive and sending it to the other party.

Sending an email, using a key distribution algorithm, or using a private fiber network are all in-band distribution methods.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_08_EH1]

Question 9: Correct

Which of the following best describes a feature of symmetric encryption?

- Does not work well for bulk encryption of less sensitive data.
- Uses only one key to encrypt and decrypt data.
- Does not require the exchange of the shared secret key.
- Uses only one algorithm type.

Explanation

Symmetric encryption, also known as secret key encryption, pre-shared key, or private key encryption, uses only one key to encrypt and decrypt data.

Symmetric encryption uses two algorithm types, block and stream.

Symmetric encryption is well suited for bulk encryption of less sensitive data because it is less CPU-intensive than other encryption methods.

Before communications begin, both parties must exchange the shared secret key using a secure channel.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_09_EH1]

Question 10: Incorrect

You work for a company that is implementing symmetric cryptography to process payment applications such as card transactions where personally identifiable information (PII) needs to be protected to prevent identity theft or fraudulent charges. Which of the following algorithm types would be best for transmitting large amounts of data?

- Stream
- Steganography
- ~~Cryptanalysis~~
- Block

Explanation

Block ciphers encrypt by transposing plain text to ciphertext in chunks (block by block). Block ciphers are fast and can process large amounts of data.

Stream ciphers use a sequence of bits known as a keystream, which is the key used for encryption. The encryption is performed on each bit within the stream in real time. Common uses for symmetric key stream ciphers include ATM card PINs and smart cards. Stream ciphers are best used for small amounts of data, usually less than 64 bits.

Steganography is a cryptography term that means to hide data or a message so that only the sender or the recipient suspects that the hidden data exists. Stenographic messages are in clear text.

Cryptanalysis is not a symmetric algorithm type, but a cryptography term meaning the method of recovering original data that has been encrypted without having access to the key used in the encryption process.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_SYMM_10_EH1]

Question 11: Incorrect

Which of the following is the number of keys used in asymmetric (public key) encryption?

- One
- Two
- Three
- ~~Four~~

Explanation

Public key (asymmetric) encryption uses two keys, a public key and a private key. The sender transmits a confidential message encrypted with the recipient's public key. The message can only be decrypted with the associated private key possessed solely by the recipient.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_01_EH1]

Question 12: Incorrect

Which of the follow is a characteristic of Elliptic Curve Cryptography (ECC)?

- Uses multiplication of large prime numbers.
- ~~Is used to sign a certificate using a private key and to verify a certificate using a public key.~~
- Uses symmetric encryption.
- Is suitable for small amounts of data and small devices, such as smartphones.

Explanation

ECC is an approach to cryptography based on groups of numbers and elliptic curve. ECC is an asymmetric encryption algorithm that is suitable for small amounts of data for small devices, such as smartphones.

ECC doesn't use symmetric encryption.

RSA is an asymmetric algorithm that uses the multiplication of large prime numbers for encryption.

The Digital Signature Algorithm (DSA) is used to sign a certificate using a private key and verify a certificate using a public key.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_ENCR_ALGOR_01_EH1]

Question 13: Incorrect

Which of the following cryptographic algorithms is used in asymmetric encryption?

- Blowfish
- Diffie-Hellman
- ~~AES~~
- Twofish

Explanation

Diffie-Hellman is an asymmetric cryptographic algorithm.

Twofish, AES, and Blowfish are symmetric cryptographic algorithms.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_ENCR_ALGOR_02_EH1]

Question 14: Incorrect

Above all else, which of the following must be protected to maintain the security and benefit of an asymmetric cryptographic solution, especially if it is widely used for digital certificates?

- ~~Cryptographic algorithm~~
- Public keys
- Private keys
- Hash values

Explanation

The strength of an asymmetric cryptographic system lies in the secrecy and security of its private keys. A digital certificate and a digital signature are little more than unique applications of a private key. If the private keys are compromised for a single user, for a secured network, or for a digital certificate authority, the entire realm of trust is destroyed.

A public key can be shared without compromising asymmetric cryptography or digital certificates.

Cryptographic algorithms are easy to find in the public realm.

Hash values must be made available to validate digital certificates.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_ENCR_FEATURES_01_EH1]

Question 15: Correct

Mary is using asymmetric cryptography to send a message to Sam so that only Sam can read it. Which of the following keys should she use to encrypt the message?

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

Explanation

Mary should use Sam's public key 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 using Mary's private key would allow anyone to decrypt 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

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_ENCR_FEATURES_02_EH1]

Question 16: Correct

Mary wants to send a message to Sam. She wants to digitally sign the message to prove that she sent it. Which of the following cryptographic keys would Mary use to create the digital signature?

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

Explanation

Mary would use her own private key to create the digital signature. This proves that only Mary could have sent the message because only Mary has access to her private key. Sam would use Mary's public key to verify the digital signature.

Sam's public key would be used to encrypt a message that only Sam should be able to read. Only Sam's corresponding private key could 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 with Mary's public key would mean that only Mary would be able to decrypt it using her private key, but could not prove where the message came from because anyone has access to Mary's public key.

References

TestOut Ethical Hacker Pro - 15.1 Cryptography
[e_cryptography_eh1.exam.xml Q_CRY_ASYM_ENCR_FEATURES_03_EH1]