Exam Report: 9.5.4 Practice Questions

Date: 1/28/2020 4:47:41 pm
Time Spent: 3:33

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 27%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

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

➡ ☐ Is used in IPsec

➡ ☐ Uses a 168-bit key

☑ ~~Uses the Rijndael block cipher~~

☑ ~~Uses 64-bit blocks with 128-bit keys~~

☐ Can easily be broken

Explanation

Triple DES:

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

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

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_01]

Question 2: Incorrect

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

● ~~Advanced Encryption Standard (AES)~~

○ Blowfish

➡ ○ Ron's Cipher v4 (RC4)

○ Ron's Cipher v2 (RC2)

Explanation

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

AES, RC2, and Blowfish are all symmetric *block* ciphers.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_02]

Question 3: Incorrect

Which of the following forms of cryptography is best implemented in hardware?

➡ ○ Symmetric stream

○ Symmetric block

○ Public key

● ~~Asymmetric~~

Explanation

Symmetric stream cryptography is best implemented in hardware because the data size makes it infeasible to have enough RAM or CPU cycles to process the data.

Symmetric block cryptography is primarily implemented in software. Asymmetric cryptography, also known as public key cryptography, is mainly used for key distribution, digital signatures, and data encryption for small amounts of data.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_03]

Question 4: Incorrect

Which of the following symmetric block ciphers does **not** use a variable block length?

● ~~Ron's Cipher v5 (RC5)~~

➡ ○ International Data Encryption Algorithm (IDEA)

○ Elliptic Curve (EC)

○ Advanced Encryption Standard (AES)

Explanation

International Data Encryption Algorithm (IDEA) does not use variable block lengths. In addition to IDEA, the following symmetric block ciphers also do not use variable block lengths:

- Data Encryption Standard (DES)
- Ron's Cipher v2 or Ron's Code v2 (RC2)
- Blowfish
- Twofish
- SkipJack

AES uses variable block lengths. RC5 uses 32-, 64- or 128-bit block lengths. Elliptic Curve (EC) is an asymmetric cipher.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_05]

Question 5: Correct

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

○ TwoFish

➡ ● DES

○ IDEA

○ AES

Explanation

DES offers the least encryption security from 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, 256 bit keys), TwoFish (up to 256 bit keys), and IDEA (128 bit keys) all support stronger keys than DES.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_06]

Question 6: Incorrect

Which version of the Rivest cipher is a block cipher that supports variable bit length keys and variable bit block sizes?

○ RC4

➡ ○ RC5

● ~~RSA~~

○ RC2

Explanation

RC5 is a block cipher that supports variable bit length keys and variable bit block sizes.

RC4 is a stream cipher. RC2 is limited to 64 bit blocks. RSA is not a Rivest cipher; rather, it is an asymmetric cryptography system developed by the same organization.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_07]

Question 7: Incorrect

Which of the following symmetric cryptography systems does not support a variable block size?

○ RC5

○ Rijndael

● ~~AES~~

➡ ○ IDEA

Explanation

IDEA is a symmetric cryptography system that does not support a variable block size. IDEA only supports a 64-bit block size.

RC5, AES, and AES's algorithm Rijndael all support variable block sizes. RC5's supported block sizes are 32, 64, and 128. AES (Rijndael) supports any block size.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_10]

Question 8: Incorrect

You want to encrypt data on a removable storage device. Which encryption method would you choose to use the strongest method possible?

● ~~RSA~~

○ SHA-1

○ 3DES

➡ ○ AES

Explanation

AES is stronger and faster than 3DES when implemented with a large key size (256-bits). DES was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption). 3DES improves upon DES by applying the encryption three times. It is an acceptable alternative to DES.

RSA is an asymmetric encryption algorithm. Asymmetric encryption is not typically used for bulk encryption of data. SHA-1 is a hashing algorithm, not an encryption algorithm.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_18]

▼ **Question 9:** Incorrect

Which of the following is the weakest symmetric encryption method?

➡ ○ DES

○ 3DES

● ~~Blowfish~~

○ AES

○ Twofish

Explanation

DES was one of the first symmetric encryption methods and is now obsolete (known weaknesses can be used to break the encryption).

3DES improves upon DES by applying the encryption three times. It is an acceptable alternative to DES. AES is stronger and faster than 3DES when implemented with a large key size (256-bits). Blowfish and Twofish were alternatives to DES, but AES was chosen to replace DES.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_19]

▼ **Question 10:** Correct

What type of key or keys are used in symmetric cryptography?

○ Two unique sets of key pairs

➡ ● A shared private key

○ A single key pair

○ A unique key for each participant

Explanation

Symmetric cryptography uses a shared private key. Both communication partners must be in possession of the same key in order to exchanged encrypted data.

Asymmetric cryptography uses a unique key pair for each participant. This key pair consists of a public key and a private key.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_12]

▼ **Question 11:** Correct

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

○ Asymmetric cryptography

○ Hashing cryptography

○ Public key cryptography

➡ ● Symmetric 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 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

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_13]

▼ **Question 12:** Correct

How many keys are used with symmetric key cryptography?

➡ ● One

○ Two

○ Four

○ Five

Explanation

Private key, or symmetric, cryptography 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

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_14]

▼ **Question 13:** Incorrect

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

○ Twofish

● ~~AES~~

➡ ○ RC4

○ Blowfish

Explanation

The most frequently used implementation of symmetric key stream ciphers is Ron's code (or Ron'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

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_17]

Question 14: Incorrect

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

● ~~Sending a secured email~~

○ Using a key distribution algorithm

○ Using a private fiber network

➡ ○ Copying the key to a USB drive

Explanation

Out-of-band distribution involves manually distributing the key (for example, as 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 considered in-band distribution methods.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_22]

Question 15: Incorrect

Match the symmetric key distribution mechanism on the left with the appropriate description on the right. Each distribution mechanism may be used once, more than once, or not at all.

The sender's key is sent to a recipient using a Diffie-Hellman key exchange.

~~Out-of-band distribution~~ In-band distribution

The sender's key is copied to a USB drive and handed to the recipient.

~~In-band distribution~~ Out-of-band distribution

The sender's key is sent to the recipient using public key cryptography.

✓ In-band distribution

The sender's key is burned to a CD and handed to the recipient.

✓ Out-of-band distribution

Explanation

Before communications can begin using symmetric encryption, both parties must exchange the shared secret key using a secure channel. Symmetric key encryption can use the following key distribution methods:

- *Out-of-band distribution* involves manually distributing the key, such as copying the key to a USB drive and sending it to the other party.
- *In-band distribution* can use a key distribution algorithm, such as Diffie-Hellman, to send the key to the recipient. It can also use asymmetric encryption technology to encrypt the key for distribution.

References

LabSim for Security Pro, Section 9.5.
[All Questions SecPro2017_v6.exm SYM_ENCRYPT_23]