Covers All Exam Objectives for IINS 640-553

Includes Real-World Scenarios, Hands-On and Written Labs, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CCNA®

Security

STUDY GUIDE

IINS Exam 640-553

Tim Boyles

SYBEX SERIOUS SKILLS.

Table of Contents

Chapter 9. Understanding Cryptographic Solutions 1

Section 9.1. Introduction to Cryptography 2

Section 9.2. Symmetric Encryption 5

Section 9.3. Encryption Algorithms 9

Section 9.4. Summary 11

Section 9.5. Exam Essentials 11

Section 9.6. Written Lab 12

Section 9.7. Hands-on Lab 12

Section 9.8. Review Questions 13

Section 9.9. Answers to Review Questions 16

Section 9.10. Answers to Written Lab 18

Chapter

9

Understanding Cryptographic Solutions

THE FOLLOWING CCNA-SECURITY EXAM TOPICS ARE COVERED IN THIS CHAPTER:

✓ **Implement siteto-site VPNs on Cisco routers using SDM**

- Explain the different methods used in cryptography

In Chapter 9 we are going to discuss cryptographic solutions. We will look at an introduction to cryptography, paying attention to the history of cryptography and how some of the ciphers evolved over the years. Then we will examine symmetric encryption in detail.

In the last section of this chapter, we will look at encryption algorithms and how to make a selection based on your criteria.

Introduction to Cryptography

Cryptography is defined many ways, but the main point to get across is that we are talking about the encryption of a message, file, and so on. We will get into other facets of the study of encryption, but let's look at the basics first.

You may have heard the term*cryptology* , which some use interchangeably with*cryptography* . In reality, the term *cryptology* encompasses the study of*cryptography* , which is the encoding of something, and *cryptanalysis* , which is the breaking of a code. Much as we see in the technology and military sectors today, there is a constant struggle between those trying to keep thing secrets and those trying to discern those secrets. No cipher can be considered unbreakable because there's always someone with the ability or resources to eventually break the code.

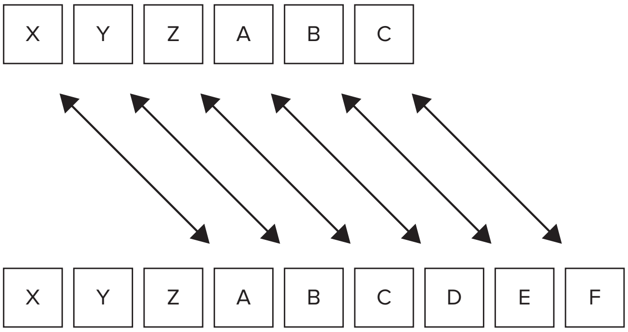
We trace the roots of cryptography back to ancient Rome, where Caesar used a form of cryptography, which we now call the *Caesar cipher* , to encode messages to his commanders in the field. Following that, the Hundred Years' War in France and England brought us the Vigenère cipher, which is known as a polyalphabetic cipher. The mathematician Babbage later showed us that a polyalphabetic cipher such as Vigenère's was vulnerable to frequency-analysis techniques. Later, electromechanical devices were used to encrypt messages, such as the infamous Enigma machine, used by the Germans during World War II. The British and Polish were able to break the Enigma machine encryption and decrypt many messages, which aided the Allies during the war. Fast-forward to the 1970s, when modern computing got started and the need for encrypted data traffic was born. The first U.S. government standard, Data Encryption Standard (DES), was brought forth in 1976. Today, the Advanced Encryption Standard (AES) is the standard algorithm.

We will look at some of these algorithms in depth and discuss some of the various types of encryption.

Caesa's Cipher

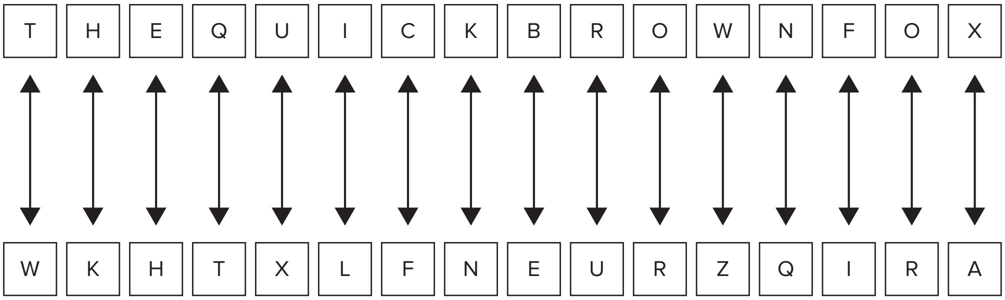
As previously mentioned, Caesar used a simple cipher to get encrypted messages to his commanders. This is known as a substitution cipher, or shift cipher. That is because Caesar used the alphabet and shifted each letter three places in order to make his cipher. Figure 9.1 shows the basis of how this cipher worked.

FIGURE 9.1 Caesar cipher



In the illustration, you can see that for every letter of the alphabet, the substituted letter is three places away. It is very simplistic but was likely effective for the times. In Figure 9.2, you can see what the phrase “the quick brown fox” looks like after the Caesar cipher has been used on it.

FIGURE 9.2 Caesar cipher example


T H E Q U I C K B R O W N F O X
W K H T X L F N E U R Z Q I R A

The Caesar cipher is also known as ROT3, or rotation of 3 places. Fast forward to the 1980s, and members of the Unix community were very active in an online community called Usenet. In the net.jokes newsgroup, ROT13, or rotation of 13 places, was used to hide offensive jokes, answers to riddles, and the like. The number 13 was used because the same number is used to encrypt or decrypt (add 13 or subtract 13).

Over the years, the substitution cipher has been found in everything from kids’ decoder rings all the way up to gangsters’ messages. In 2006, a mafia boss in Sicily was captured because he used a variation of a substitution cipher. On a humorous note, in 1999, Netscape Communicator was found to have used ROT13 as a way of encrypting its email passwords.

Substitution ciphers are very easy to crack, especially if you use frequency analysis to determine where the patterns are. Simple ciphers can be spied with the native eye, without the use of computers.

Vigenère Cipher

We can see the weaknesses of the substitution cipher, presented in the previous section. The next evolution of the cipher was the polyalphabetic cipher. In the 1900s this cipher was attributed to Blaise de Vigenère, a French cryptographer; however, the cipher has been traced back to a book written in the 1500s by Giovanni Batista Belaso, an Italian. Vigenère had merely published an updated version of this cipher, but his name has been widely attached to this type of cipher.

The Vigenère cipher takes a number of substitution ciphers and a keyword that is used between them, making frequency analysis difficult if not impossible. But that doesn't mean the cipher is unbreakable. Indeed, it was initially cracked by Charles Babbage, but he did not publish the solution. The solution was published in the 1900s by Friedrich Kasiski, a German cryptographer.

The Vigenère cipher basically uses the 26 letters of the alphabet together with a secret key to encrypt the text. Let's look at an example using the Vigenère cipher. In this example, we will use a secret key called newkey to encrypt our message, which is "meet me in paris." Refer to the Vigenère table in Figure 9.3.

FIGURE 9.3 Vigenère table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Starting with the*m* from our message, we encode this by using the row starting with*n* for the letter in the *m* column. In this case, the letter is*z* . The next letter would look for the row starting with *e* , using the letter in the*e* column, which would be*i* . Continuing further, the first two words of the message, "meet me," would be encoded as "ziad qc."

One-Time Pads

A one-time pad is also known as a Vernam cipher, which was created by and then patented by Gilbert Vernam in 1917, while employed by AT&T. The Vernam cipher was a stream cipher that used an exclusive OR (XOR) against plaintext with a key. Another cryptographer in the U.S. Army Signal Corps expanded on this idea by using random data as the key.

The idea behind using a Vernam cipher is that the cipher is unbreakable, assuming that the key is used only once (hence the name one-time pad, because they are generally used only one time).

The problems come in when you have to deliver the key to the recipient and then store it. These challenges usually limit the use of Vernam ciphers to only extremely secure communications.

Transposition Ciphers

A transposition cipher is just like it sounds. Letters are transposed so that they no longer exist in the original format. An example might be the original plaintext "SEE YOU IN ST LOUIS." If we engaged a transposition cipher, we might have a result such as "NSETUIYEOIULSSO." Nothing has been changed, just the position of the letter moved or transposed. The transposition cipher is also called permutation.

A form of transposition cipher is the rail fence cipher. In this cipher the words are read like a rail fence. In the example below, we have the words "PICK UP THE PACKAGE AT THE USUAL PLACE," using a three-place key.

```
P....U....E....K....A....E....A....A
.I.K..P..H..P.C.A.E..T..H..U.U.L..L.C
..C.....T....A...G.....T....S....P...E
```

Reading the letters up and down, you see that the letters spell out the phrase.

Transposition is still a part of some modern algorithms, such as Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES).

Symmetric Encryption

Symmetric encryption algorithms are probably the most commonly used encryption algorithms. One of the main advantages of symmetric encryption is speed. Because you are using the same key to encrypt and decrypt, the mathematics behind the calculation is much simpler. This allows the key lengths to be shorter. Examples of symmetric encryption algorithms are DES, 3DES, AES, Blowfish, RC4, and SEAL.

Symmetric vs. Asymmetric Encryption

What's the difference between symmetric and asymmetric encryption? With symmetric encryption, you use the same key to encrypt and decrypt. With asymmetric encryption, you use a key pair. The keys are different; one key is public and the other is private. Symmetric encryption is faster, but asymmetric encryption is better for communication between parties who are not known to each other, because there is no need to share a secret key with an unknown person. For more information, see Chapter 11, "Using Asymmetric Encryption and PKI."

Symmetric Encryption Keys

Symmetric encryption keys can range in length from 40 bits to 256 bits. As you might expect, the shorter the key length, the less protection you might be afforded. There are some generally accepted protection principles for various key lengths. As you can see in Table 9.1, a 256-bit key provides protection against quantum computing, whereas at the other end of the spectrum, 40 bits can be broken very easily with a brute-force attack. Key lengths in between those can be expected to provide protection for a certain number of years, as shown in Table 9.1.

TABLE 9.1 Key-length Protection for Various Algorithms

Approximate Level of Protection	Symmetric Key	Asymmetric Key	Hash
3 years' protection	80	1248	160
10 years' protection	96	1776	192
20 years' protection	112	2432	224
30 years' protection	128	3248	256
Quantum computing protection	256	15424	512

DES Encryption Algorithm

The Data Encryption Standard (DES) has now been in use for over 35 years and still has not been found to have a significant flaw. However, because its key length is relatively short, it can be susceptible to brute-force attacks.

DES uses a 64bit key, but only 56 of the bits are used for encryption. Unfortunately, 16 of those remaining 56 bits are known and 40 bits are unknown. The other 8 bits are used for parity. What that means, essentially, is that DES has a 40-bit key strength.

DES has two operating modes, stream cipher and block cipher. Further, each of these two modes has two types within it. The following list shows the modes and types.

Block cipher modes

- Electronic Code Book (ECB) mode creates the same cipher text from plaintext each time. This mode is susceptible to replay attacks, among others.
- Cipher Block Chaining (CBC) mode uses XOR of the previous ciphertext and then encrypts with the DES key.

Stream cipher modes

- Cipher Feedback (CFB) mode turns a block cipher into a stream cipher and operates similarly to CBC.
- Output Feedback (OFB) mode generates keystream blocks that are XORed with the plaintext to create ciphertext.

Of all of these modes, CBC mode is the most prevalent, because it is used with IPSec. In fact, Cisco's implementation of IPSec using DES (and 3DES) operates in CBC mode.

The following are suggested guidelines for DES usage:

- Change the key frequently because of its susceptibility to brute-force attacks.
- Use a secure channel to transmit keys.
- Use CBC mode, because it is the most secure within DES.

3DES Encryption Algorithm

Triple DES, as the 3DES encryption algorithm has become known, essentially strengthens the original DES algorithm by applying it three times. Because the original DES algorithm is cryptographically strong, it can be made much stronger by encrypting the data three times. This triple encryption makes a brute-force attack unfeasible. The effective key strength can be either 112 bit or 168 bit, which is what Cisco uses. Let's examine how the 3DES algorithm works.

1. A first 56-bit key is used to encrypt the plaintext.
2. A second 56-bit key is used to decrypt the data.
3. A third 56-bit key is used to encrypt the data again.

If you use different first and third keys, you get an effective key strength of 168 bits, which is what Cisco does. If you use the same key in steps 1 and 3, then you have an effective key strength of 112 bits.

The encrypt-decrypt-encrypt sequence creates a much stronger key strength than using three different keys encrypted three times. That method would yield an effective 58-bit key strength, instead of the 168-bit key strength that is 3DES.

3DES is very much in use in today's environment and is still very secure. It's been around a long time without anyone finding a weakness.

Advanced Encryption Algorithm

Advanced Encryption Algorithm (AES) came about after the federal government decided that it needed to create a new standard that would replace DES as the official government encryption cipher. A bake-off of sorts was initiated in 1997. The winner, selected in 2000, was the Rijndael cipher, a mixture of the last names of the two creators, Joan Daemen and Vincent Rijmen. This cipher became an official government standard in 2002.

The Rijndael cipher uses a variable key length and block size in the implementation of the cipher. There are potentially nine different combinations of key length and block size. You may use a key length of 256 bits, 192 bits, or 128 bits to encrypt block sizes of 128 bits, 192 bits, or 256 bits.

The Rijndael cipher operates as an iterated block cipher. It uses multiple transformation cycles on its way to an end output. The Rijndael cipher uses only the original key lengths and block sizes; however, one of the key features of this cipher is that it can be expanded on 32-bit borders for the block size and/or the key length.

AES runs much faster than its predecessor, 3DES. This allows it to run in software more effectively and can be better suited for those applications that require low-latency and/or high throughput.

Because AES is a relatively new algorithm, it has been employed by Cisco for just a few years. The following devices and software versions support AES used in IPSec VPN.

- PIX Firewall Software versions 6.3 and above
- ASA Software versions 7.0 and above
- Cisco IOS 12.2(13)T and above
- Cisco VPN 3000 Concentrator Software versions 3.6 and above

SEAL

The Software-Optimized Encryption Algorithm (SEAL) is an alternative to the more traditional DES, 3DES, or AES algorithms. SEAL uses a 160-bit key and is less processor intensive than some of the other alternatives. SEAL is supported in Cisco IOS 12.3(7) but not with routers that have a hardware encryption card, meaning that it's used only in software. SEAL is available only from Cisco and has the following restrictions:

- SEAL is supported only in the K9 subsystem.
- IPSec must be supported by your router and the peer router.
- No hardware IPSec encryption can be used.

Rivest Ciphers

The Rivest ciphers are also known as the RC ciphers. Ron Rivest is a well-known cryptographer and professor at MIT. He is the author of the Rivest ciphers known as RC2, RC4, and RC5 and coauthor of RC6. Table 9.2 briefly describes the algorithms.

TABLE 9.2 Rivest Ciphers

RC Algorithm	Description
RC2	Variable-length key-block cipher, designed to be an alternative to DES.
RC4	Variable key-length stream cipher used frequently in file encryption products, as well as in Secure Sockets Layer (SSL).
RC5	RC5 has a variable-length key and variable-length block size.
RC6	Block cipher meant to compete for the AES standard.

Of all of these, RC4 is used most prevalently. It is used frequently within SSL to secure web transactions.

Encryption Algorithms

Encryption algorithms are used in security all the time, for purposes ranging from encrypting a laptop to securing a VPN tunnel. Some categorize these two uses as securing the data at rest, such as in a database, and securing the data in transit, such as using it with SSL or a VPN tunnel. In this section we will look briefly at hashes. We will also look at how to choose the correct encryption algorithm for your particular needs.

Real World Scenario

B2B VPN IPSec Tunnel

Your company has signed an agreement to do business with a partner. As part of the agreement, you will need to set up a VPN tunnel with the partner company. You have been told that the business with the partner will involve confidential information. The requirements are that you must use encryption and that it must be fast. Your business partner uses Cisco equipment, as do you. What would be the best choice for an encryption standard for your VPN tunnel?

Providing that the business partner's equipment could support it, the best choice would be AES, which is supported in recent versions of Cisco equipment and software. If the partner's equipment is a bit older, 3DES would be the next choice. Both of those standards are relatively fast compared to other types of algorithms and are secure.

Choosing the Right Encryption Algorithm

An important task when you look at securing your data is to choose the correct encryption algorithm. Generally two criteria are considered essential when discussing an encryption algorithm.

Choose a trustworthy algorithm. A trustworthy encryption algorithm is one that has been vetted through the security community. That is to say, it has been around for many years and has proven to be resistant to attacks.

Protect against brute-force attacks. An encryption algorithm must have sufficient key length to protect the data for the level of confidentiality required. For example, a key length of 40 might not be enough for your application.

The following is a list of trustworthy encryption algorithms:

- DES
- 3DES
- AES
- RC4

You might be questioning why DES would be considered a trustworthy encryption algorithm when it is only 40 bits and can be brute-forced. If you only need to protect some data for a brief time, DES might be a good choice for that particular application. 3DES is good when a higher level of security is needed. AES might be a better choice when you need a high level of security, but low latency and/or high throughput. The point to be made here is that each algorithm has its place.

Hashing Functions

Hashing functions are used to ensure integrity of the data you are trying to protect. Hashes are one-way mathematical functions that are virtually impossible to reverse. Therefore, when you create a hash, it is highly unlikely that a hash value that matches the original would have been tampered with.

A hash means that you are combining an arbitrary bunch of data with the hash function. You get a fixed-length hash value or sum. This hash value or sum is used to verify that the data you sent is the data that was received. Many pieces of software are distributed over the Internet, so in order to verify that they are not tampered with, you need to compare the hash value that was provided by the distributor with the hash value that you get once you receive the software.

NOTE

A number of open-source and commercial software packages use Message Digest 5 (MD5) as their choice for a hash function. One way to verify a software package that has been hashed with MD5 is to use an application like md5sum on Unix platforms or Winmd5sum, which is a third-party open-source program available for the Windows platform.

You may be familiar with cyclic redundancy check (CRC) checksums. Hashes are similar to this but are much more cryptographically secure. A hash is strong enough that any two separate sets of data are virtually assured not to create the same hash value.

Hashing functions are covered in more detail in Chapter 10,"Using Digital Signatures."

Summary

In this chapter you learned about the history of cryptography and the difference between cryptography and cryptanalysis. You also learned about the differences in encryption algorithms.

We explored the different types of symmetric encryption algorithms that can be employed.

Finally, we looked at criteria on how to choose the algorithm that you want to suit your application.

Exam Essentials

Remember the historical evolution of cryptography and the differences between cryptology, cryptography, and cryptanalysis. One of the original works of cryptography was the Caesar cipher, or substitution cipher. A Vigenère cipher is a polyalphabetic cipher. A transposition cipher doesn't change the plaintext but merely rearranges it.

Understand the differences in asymmetric and symmetric encryption and then be able to discuss the various symmetric encryption algorithms. The main differences in symmetric and asymmetric encryption are that in symmetric encryption, the same key is used. Symmetric encryption keys range in length from 40 bits to 256 bits.

Know the different types of symmetric encryption algorithms. The most common types of symmetric encryption algorithm are the DES, 3DES, AES, and SEAL algorithms.

Know the different types of encryption algorithms and how to make a choice that fits your application. The two primary criteria for choosing your encryption algorithm are trustworthiness and protection against brute-force attacks, which is really about key strength.

Written Lab

Write the answers to the following questions:

1. What is the current government standard for encryption?
2. What type of encryption algorithm uses a single key to encrypt/decrypt?
3. What type of cryptography does not change the text but rather changes the position of the text?
4. What is the name of the cipher that uses a polyalphabetic scheme?
5. Which alternative algorithm to 3DES uses a 160-bit key?
6. Which block cipher mode use XOR as part of its algorithm?
7. Which cipher is also called a one-time pad?
8. What is the name of the cipher used in AES?
9. What is the name of the task someone who breaks ciphers performs?

10.Which type of symmetric encryption is not supported in IPSec hardware?

Hands-on Lab

Hands-on Lab 9.1: Creating a Substitution Cipher

1. Using the regular alphabet, create a four-position substitution cipher.
2. Refer to the alphabet shown here to create a four-position substitution cipher:

   ABCDEFGHIJKLMNOPQRSTUVWXYZ
3. The phrase you will be encoding is“IS THIS THING ON.”
4. Starting with the word*IS* , count down four places for each letter, so the*I* will become *M* and the*S* will become*W* .
5. Complete the rest of the words in the phrase.
6. Review the completed encoded phase that follows and see if yours matches up:

   MW XLMW XLMRK SR

Review Questions

1. Which type of cipher substitutes letters of the alphabet, based on a position offset from the original letter?

A. Block cipher

B. Substitution cipher

C. Vigenere cipher

D. Polyalphabetic cipher

2. Which type of cipher is a rail fence cipher?

A. Substitution

B. Block

C. Streaming

D. Transposition

3. What is the minimum level of IOS that supports AES for IPSec encryption?

A. 12.1(3)

B. 12.3(1)

C. 12.2(13)T

D. 12.2(1)T

4. What IPSec protocol would you choose if you had an application that was sensitive to latency but required high security?

A. 3DES

B. AES

C. SEAL

D. RC4

5. What is the name of the attack method that can be used to defeat all cryptography methods?

A. Brute force

B. Spoofing

C. Honeypot

D. Fuzzing

6. Which type of encryption algorithm uses an encryption, decryption, and encryption scheme to achieve a 168-bit key strength?

A. SEAL

B. RC4

C. RC2

D. 3DES

7. Which current encryption algorithm key strength that follows is considered inadequate, subject to brute-force attacks?

   A. 30 bit

   B. 40 bit

   C. 56 bit

   D. 64 bit

8. What type of encryption algorithm uses a 160-bit key?

   A. SEAL

   B. RC4

   C. DES

   D. CBC

9. Which algorithm is frequently used in file-encryption software?

   A. 3DES

   B. RC4

   C. RC2

   D. SEAL

10. What function does a hash perform?

    A. Confidentiality

    B. Compression

    C. Availability

    D. Integrity

11. True or false: the Rijndael cipher is*not* supported on the Cisco VPN 3000 Concentrator.

12. Which of the following key lengths for symmetric encryption provides protection against quantum computing?

    A. 128

    B. 112

    C. 256

    D. 212

13. Using the same key in both of the 3DES encrypt cycles of the process would yield a key strength of ____ bits.

    A. 112

    B. 116

    C. 168

    D. 132

14. Which of the following is *not* a key length option when using AES?

A. 256

B. 192

C. 128

D. 112

15. What is the name of the software used on Unix systems that can determine hash values?

A. Hashsum

B. Md5sum

C. Winmd5sum

D. Md5value

16. Which of the following is not considered a trustworthy symmetric encryption algorithm?

A. IDEA

B. RC2

C. RC4

D. 3DES

17. True or false: a hash can be used to provide confidentiality of data.

18. Which of the following types of encryption algorithm is*not* a symmetric encryption algorithm?

A. DES

B. RSA

C. RC4

D. AES

19. How many possible combinations of AES key length and block size are there?

A. 6

B. 8

C. 9

D. 10

20. If you have to use DES because of compatibility purposes with a business partner, what can you do to mitigate the risk? Choose all that apply.

A. Rotate keys frequently.

B. Use DES twice.

C. Protect your communications regarding keys.

D. Use OFB mode.

Answers to Review Questions

1. B. In a substitution cipher, a different letter that is some number of places away from the original letter of the alphabet is substituted for the original letter. This is also referred to as a Caesar cipher.

2. D. A rail fence cipher is a type of transposition cipher, where the letters of the message aren't changed, just moved.

3. C. The minimum level of IOS that supports AES as an encryption algorithm is 12.2(13)T.

4. B. AES, which is the latest government standard, also runs very fast, so it is beneficial to use in a low-latency application situation.

5. A. Brute-force attacks can be used to defeat all cryptography methods, assuming there are enough time and resources. No one method can be considered unbreakable.

6. D. Triple DES, or 3DES, takes the DES encryption scheme and performs an encryption, decryption, and encryption with three different keys to achieve a 168-bit key strength.

7. B. A 40-bit key strength is considered inadequate because of brute-force attack vulnerability. However, it is adequate if you only need to protect some data for a brief time.

8. A. SEAL uses a 160-bit key for encryption.

9. B. RC4 is frequently used in file-encryption software.

10. D. A hash is used to perform data integrity.

11. False. The Cisco VPN 3000 Concentrator supports AES on version 3.6 and above.

12. C. In symmetric encryption, a key length of 256 is considered to provide protection against quantum computing.

13. A. Using the same key in both encrypt cycles yields a key strength of 112 bits. If different keys are used during the two encrypt cycles, then the key strength is 168 bits.

14. D. The three options for key lengths when using AES as your encryption scheme are 128, 192, and 256 bits.

15. B. The md5sum program is typically part of the Unix distribution and can be used to determine MD5 hash values.

16. B. Of the encryption algorithms listed, only RC2 is not considered a trustworthy algorithm.

17. False. A hash can be used only for data integrity.

18B. DES, RC4, and AES are all symmetric encryption algorithms. RSA is an asymmetric encryption algorithm, covered in Chapter 11, "Using Asymmetric Encryption and PKI."

19C. There are three possible key lengths and three possible block sizes in AES as it is today, which equates to nine possible combinations.

20A, C. The two items on this list that can be done to mitigate the risk of using DES are to rotate the keys frequently and protect your communications regarding keys.

Answers to Written Lab

1. AES

2. Symmetric

3. Transposition

4. Vigenère

5. SEAL

6. CBC

7. Vernam

8. Rijndael

9. Cryptanalysis

10SEAL