Covers all Exam Objectives for CEHv6

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

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

CEH™

Certified Ethical Hacker

STUDY GUIDE

Exam 312-50
Exam ECO-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

Table of Contents

Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Chapter

14

Cryptography

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Overview of cryptography and encryption techniques
- ✓ Describe how public and private keys are generated
- ✓ Overview of MD5, SHA, RC4, RC5, Blowfish algorithms

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Cryptography is the study of encryption and encryption algorithms. In a practical sense, encryption is the conversion of messages from a comprehensible form (cleartext) into an incomprehensible one (cipher text), and back again. The purpose of encryption is to render data unreadable by interceptors or eavesdroppers who do not know the secret of how to decrypt the message. Encryption attempts to ensure secrecy in communications. Cryptography defines the techniques used in encryption. This chapter will discuss encryption algorithms and cryptography.

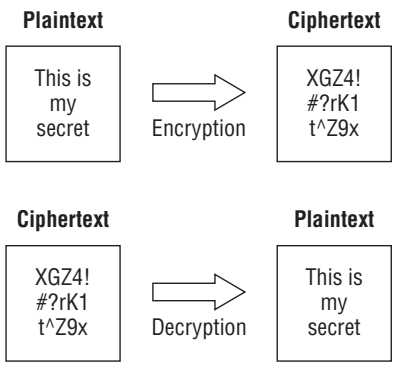
Licensed by Puneet Kumar 2850921

Cryptography and Encryption Techniques

Encryption can be used to encrypt data while it is in transit or while it's stored on a hard drive. Cryptography is the study of protecting information by mathematically scrambling the data so it cannot be deciphered without knowledge of the mathematical formula used to encrypt it. This mathematical formula is known as the encryption algorithm. Cryptography is composed of two words: *crypt* (meaning secret or hidden) and *graphy* (meaning writing). Cryptography literally means secret or hidden writing.

Cleartext is the readable and understandable data, and cipher text is the scrambled text as a result of the encryption process. Cipher text should be unreadable and show no repeatable pattern to ensure the confidentiality of the data. Figure 14.1 shows cleartext versus cipher text.

FIGURE 14.1 Cleartext and cipher text



Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

There are three critical elements to data security. Confidentiality, integrity, and authentication are known as the CIA triad (Figure 14.2). Data encryption provides confidentiality, meaning the data can only be read by authorized users. Message hashing provides integrity, which ensures the data sent is the same data received and the information was not modified in transit. Message digital signatures provide authentication (ensuring users are who they say they are) as well as integrity. Message encrypting and digital signatures together provide confidentiality, authentication, and integrity.

FIGURE 14.2 The CIA triad

Encryption algorithms can use simple methods of scrambling characters, such as *substitution* (replacing characters with other characters) and *transposition* (changing the order of characters). *Encryption algorithms* are mathematical calculations based on substitution and transposition.

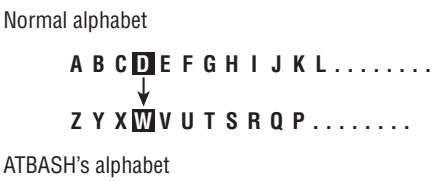
Here are some early cryptographic systems:

Caesar's Cipher A simple substitution cipher (Figure 14.3).

FIGURE 14.3 Substitution cipher

Atbash Cipher Used by the ancient Hebrews, Atbash (Figure 14.4) is a substitution cipher and works by replacing each letter used with another letter the same distance away from the end of the alphabet; for example, A would be sent as a Z and B would be sent as a Y.

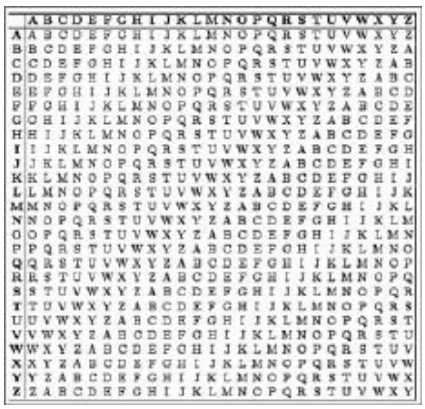
FIGURE 14.4 Atbash cipher



Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Vigenere Cipher Sixteenth-century French cryptographer Blaise de Vigenere created a polyalphabetic cipher to overcome the shortcomings of simple substitution ciphers. The Vigenere cipher (Figure 14.5) uses a table to increase the available substitution values and make the substitution more complex. The substitution table consists of columns and rows labeled "A" to "Z." To get cipher text, first you select the column of plain text and then you select the row of the key. The intersection of row and column is called cipher text. To decode cipher text, you select the row of the key and find the intersection that is equal to cipher text; the label of the column is called plain text.

FIGURE 14.5 Vigenere cipher



	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Vernam Cipher In 1917, AT&T Bell Labs engineer Gilbert Vernam sought to improve the Vigenere cipher and ended up creating the Vernam cipher, or "one-time pad." The Vernam cipher is an encryption algorithm where the plain text is combined with a random key, or "pad," that is the same length as the message. One-time pads are the only algorithm that is provably unbreakable by brute force.

Concealment Cipher A concealment cipher creates a message that is concealed in some way. For example, the following paragraph includes a secret message:

> *I have been trying to buy Sally some nice jewelry, like gold or silver earrings, but prices now have increased.*

The key is to look at every sixth word in a sentence. So the secret message is "buy gold now."

Types of Encryption

The two primary types of encryption are symmetric and asymmetric key encryption.

Symmetric key encryption means both sender and receiver use the same secret key to encrypt and decrypt the data. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

The drawback to symmetric key encryption is there is no secure way to share the key between multiple systems. Systems that use symmetric key encryption need to use an offline method to transfer the keys from one system to another. This is not practical in a large environment such as the Internet, where the clients and servers are not located in the same physical place.

The strength of symmetric key encryption is fast, bulk encryption. Weaknesses of symmetric key encryption include

- Key distribution
- Scalability
- Limited security (confidentiality only)
- The fact that it does not provide nonrepudiation, meaning the sender's identity can be proven

Examples of symmetric algorithms are as follows:

- DES (data encryption standard)
- 3DES
- AES (Advanced Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Twofish
- RC4 (Rivest Cipher 4)

Asymmetric (or public) key cryptography was created to address the weaknesses of symmetric key management and distribution. But there's a problem with secret keys: how can they be exchanged securely over an inherently insecure network such as the Internet? Anyone who knows the secret key can decrypt the message, so it is important to keep the secret key secure. Asymmetric encryption uses two related keys known as a key pair. A public key is made available to anyone who might want to send you an encrypted message. A second, private key is kept secret, so that only you know it.

Any messages (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet as they are by nature available to anyone. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

The relationship between the two keys in asymmetric key encryption is based on complex mathematical formulas. One method of creating the key pair is to use factorization of prime numbers. Another is to use discrete logarithms. Asymmetric encryption systems are based on one-way functions that act as a trapdoor. Essentially the encryption is one-way in that the same key cannot decrypt messages it encrypted. The associated private key

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

provides information to make decryption feasible. The information about the function is included in the public key, whereas information about the trapdoor is in the private key. Anyone who has the private key knows the trapdoor function and can compute the public key.

To use asymmetric encryption, there needs to be a method for transferring public keys. The typical technique is to use X.509 digital certificates (also known simply as certificates). A certificate is a file of information that identifies a user or a server, and contains the organization name, the organization that issued the certificate, and the user's email address, country, and public key.

When a server and a client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

Asymmetric encryption can be used for

- Data encryption
- Digital signatures

Asymmetric encryption can provide

- Confidentiality
- Authentication
- Nonrepudiation

Strengths of asymmetric key encryption include

- Key distribution
- Scalability
- Confidentiality, authentication, and nonrepudiation

The weakness of asymmetric key encryption is that the process is slow and typically requires a significantly longer key. It's only suitable for small amounts of data due to its slow operation.

Stream Ciphers vs. Block Ciphers

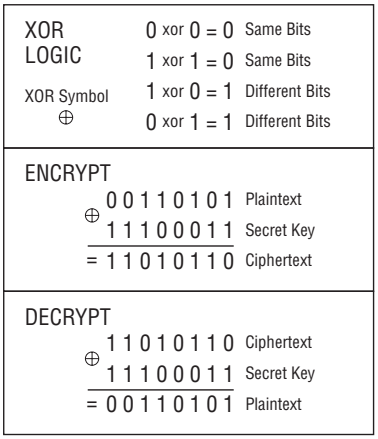
Block ciphers and stream ciphers are the two types of encryption ciphers. Block ciphers are encryption ciphers that operate by encrypting a fixed amount, or "block," of data. The most common block size is 64 bits of data. This chunk or block of data is encrypted as one unit of cleartext. When a block cipher is used for encryption and decryption, the message is divided into blocks of bits. Blocks are then put through one or more of the following scrambling methods:

- Substitution
- Transposition
- Confusion
- Diffusion
- S-boxes

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

A stream cipher encrypts single bits of data as a continuous stream of data bits. Stream ciphers typically execute at a higher speed than block ciphers and are suited for hardware usage. The stream cipher then combines a plain text bit with a pseudorandom cipher bit stream by means of an XOR (exclusive OR) operation. The XOR process (see Figure 14.6) is to compare the plain text and key one bit at a time and, based on the XOR logic, create cipher text. If the plain text and secret key are the same bit, the result is a 0; if they are different, such as 1 and 0, then the resulting encrypted bit is a 1.

FIGURE 14.6 XOR table



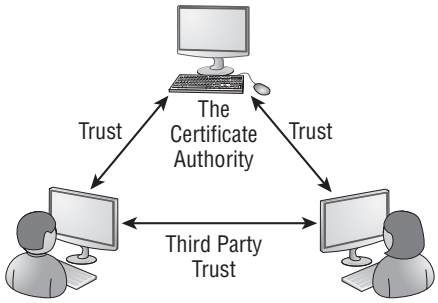
Generating Public and Private Keys

When a client and a server use asymmetric cryptography, both create their own pairs of keys for a total of four keys: the server's public key, the server's private key, the client's public key, and the client's private key. A system's key pair has a mathematical relationship that allows data encrypted with one of the keys to be decrypted with the other key. These keys have a mathematical relationship based on factoring prime numbers such that each key can be used to decrypt data encrypted with the other key. When a client and a server want to mutually authenticate and share information, they each send their own public key to the remote system, but they never share their private keys. Each message is encrypted with the receiver's public key. Only the receiver's private key can decrypt the message. The server would encrypt a message to the client using the client's public key. The only key that can decrypt the message is held by the client, which ensures confidentiality.

A *public key infrastructure (PKI)* is necessary in order to create digital certificates. PKI is a framework that consists of hardware; software; policies that exist to manage, create, store, and distribute keys; and digital certificates. Additionally, a complete PKI solution (like the one in Figure 14.7) involves symmetric algorithms, asymmetric algorithms, hashing, and digital authentication (usually certificates, but could also be Kerberos).

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

FIGURE 14.7 Certificate authority



One of the major strengths of public key encryption is its ability to facilitate communication between parties previously unknown to each other, a process that is made possible by the PKI hierarchy of trust relationships. The important parts of the PKI infrastructure are as follows:

- Digital certificates
- Certificate authorities
- Certificate generation and destruction
- Key management

Real World Scenario

Understanding Certificate Authorities

Using a certificate authority (CA) to validate a client is similar to providing a driver's license for identification. When I am traveling on an airplane, I have to present a valid form of identification to prove my identity. The airport security will generally require a third party such as the state to issue the identification in the case of a driver's license. The security staff might question an ID card that I made at home using my digital camera and color printer. It is also unlikely that they'd accept a library card as a form of identification because it most likely does not contain all the necessary information about me. The state that issues a driver's license is much like the certificate authority: a trusted third party who is trusted to validate my identity. The certificate itself is similar to the driver's license as it contains all the necessary information to validate my identity.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

CAs are the glue that binds the public key infrastructure together. They are essentially neutral third-party organizations that provide notarization services for digital certificates. To obtain a digital certificate from a reputable CA, you must identify and prove identity.

Digital certificates are formatted to the X.509 standard and contain set fields. These fields include

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
- Not Before (a specified date)
- Not After (a specified date)
- Subject
- Subject Public Key Information
- Public Key Algorithm
- Subject Public Key
- Issuer-Unique Identifier (optional)
- Subject-Unique Identifier (optional)
- Extensions (optional)

In Exercise 14.1, you will view a digital certificate from a secure website.

EXERCISE 14.1

Viewing a Digital Certificate

Connect to any website that requires a login, such as a bank, webmail, or e-commerce site. If you do not have a login to a secure website, then create a Google email account (Gmail) at `www.gmail.com` for free. If you are creating a Gmail account, you will need to change the settings to always use HTTPS to secure your email. Once you have logged in using SSL, you will be able to view the x.509 certificate from the web server.

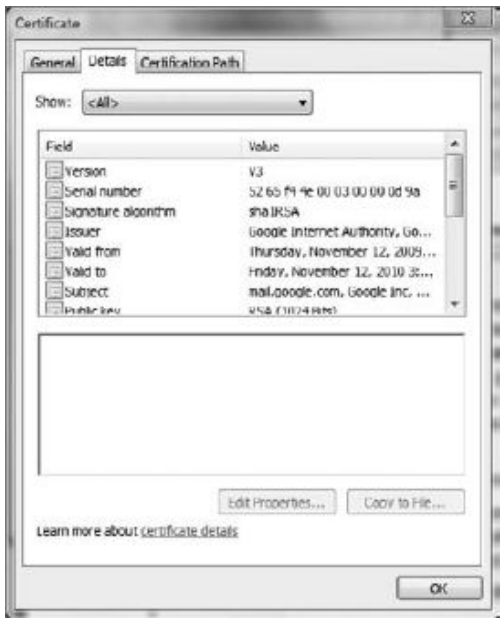
1. Open Internet Explorer and log into the secure website.
2. Click the Page menu and choose Properties, or click the yellow lock icon in the lower-right side on the Internet Explorer screen.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

EXERCISE 14.1 *(continued)*

3. Click the Certificates button on the page's properties sheet.

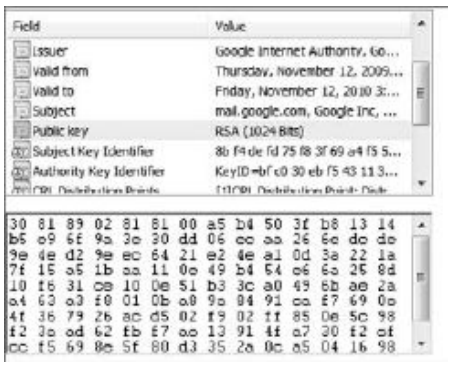
4. Click the Details tab to see all the certificate fields. Click each field to see the values.



Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

EXERCISE 14.1 *(continued)*

5. Determine the issuer of the certificate.
6. Determine the validity date of the certificate.
7. View the public key of the certificate.



Other Uses for Encryption

Integrity is one of the components of the CIA triad and ensures that information remains unchanged and is in its true original form. A hash is a common method of providing integrity of a message. A hash is the conversion of a string of characters into a shorter fixed-length value that represents the original. It is similar to a shorthand version of the full data.

Common hashing algorithms for digital signatures include

- SHA-1
- MD5
- RIPEMD-160

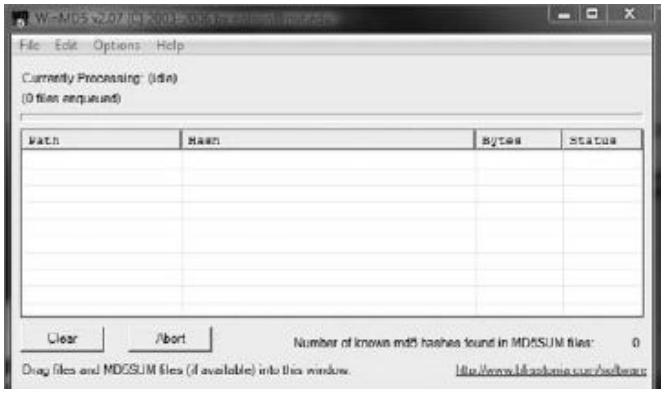
EXERCISE 14.2

Using WinMD5 to Compute File Hashes

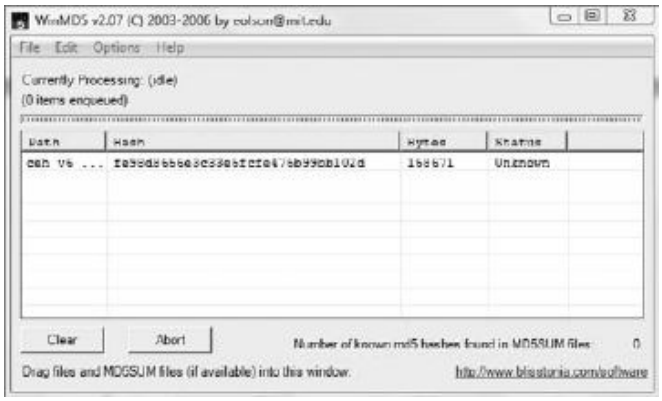
1. Download and install WinMD5 from `www.blisstonia.com/software/WinMD5`.
2. Run the `WinMD5.exe` program.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

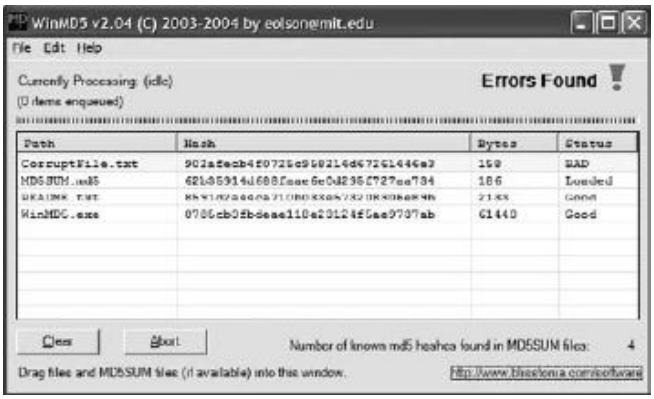
EXERCISE 14.2 *(continued)*



3. Click the File menu in WinMD5 and choose Open. Select any file from your system.



Here is an example of a bad MD5 hash on a file:



Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

If you've downloaded a file from the Internet, you may be concerned that the file is not complete or was corrupted. One of the ways to ensure the file sent is the same file received is through the MD5 hashing algorithm. MD5 hashes are fingerprints of files. You can compare the fingerprints of two files to see if the files themselves are the same.

You have to have the correct fingerprint for a file to compare the file you receive with the original; otherwise, you cannot tell if your file has integrity. When you download a large file, it may contain another file called `MD5SUM` or something similar. This file contains the correct fingerprints. Dragging an `MD5SUM` file onto WinMD5 causes the fingerprints to be compared automatically.

The MD5SUM program allows you to compute the MD5 hashes of files. It also makes it easy to compare the fingerprints against the correct fingerprints stored in an `MD5SUM` file. Red Hat, for example, provides `MD5SUM` files for all of its large downloadable files.

When you perform hashing, two messages with the same digest are extremely unlikely. However, if this does occur and two messages produce the same hash, it is called a collision. Collisions allow for cryptographic attacks against the algorithm.

Cryptography Algorithms

Algorithms vary in key length from 40 bits to 448 bits. The longer the key length, the stronger the encryption algorithm. Using brute force to crack a key of 40 bits takes from 1.4 minutes to 0.2 seconds, depending on the strength of the processing computer. In comparison, a 64-bit key requires between 50 years and 37 days to break, again depending on the speed of the processor. Currently, any key with a length over 256 bits is considered uncrackable.

Message Digest 5 (MD5), Secure Hash Algorithm (SHA), RC4, RC5, and Blowfish are all names for different mathematical algorithms used for encryption. As a CEH, you need to be familiar with these algorithms:

MD5 MD5 is a hashing algorithm that uses a random-length input to generate a 128-bit digest. It is popular to create a digital signature to accompany documents and emails to prove the integrity of the source. The digital signature process involves the creation of an MD5 message digest of the document, which is then encrypted by the sender's private key. MD5 message digests are encrypted by a private key in the digital signature process.

SHA SHA is also a message digest, which generates a 160-bit digest of encrypted data. SHA takes slightly longer than MD5 and is considered a stronger encryption. It is the preferred algorithm for use by the government.

- SHA-0: Message of arbitrary length
  - Output: 160-bit fingerprint or message digest
- SHA-1: Message of arbitrary length
  - Output: 160-bit fingerprint or message digest. Corrected a flaw in the original SHA-0 algorithm.
- SHA-2: Message of arbitrary length
  - Output: 256-bit fingerprint or 512-bit fingerprint

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

RC4 and RC5 RC4 is a symmetric key algorithm and is a *stream cipher*, meaning one bit is encrypted at a time. It uses random mathematical permutations and a variable key size. RC5 is the next-generation algorithm: it uses a variable block size and variable key size. RC5 has been broken with key sizes smaller than 256.

Blowfish Blowfish is a 64-bit block cipher, which means that it encrypts data in chunks or blocks. It is stronger than a stream cipher and has a variable key length between 32 and 448 bits.

MAC (Message Authentication Code) MACs require the sender and receiver to share a secret key.

HMAC (Hashed Message Authentication Code) HMAC was designed to be immune to the multicollision attack. HMAC functions by using a hashing algorithm, such as MD5 or SHA-1, and altering the initial state by use of a symmetric key.

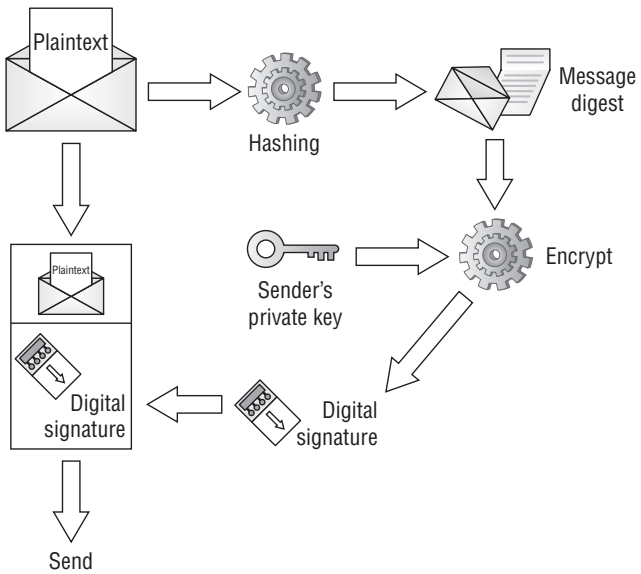
Even if someone can intercept and modify the data, it's of little use if that person does not possess the secret key. There is no easy way for the person to re-create the hashed value without the key.

Digital signatures (see Figure 14.8) are based on public key cryptography and used to verify the authenticity and integrity of a message. A digital signature is created by passing a message's contents through a hashing algorithm. The hashed value is then encrypted with the sender's private key. Upon receiving the message, the recipient decrypts the encrypted sum and then recalculates the expected message hash.

Values should match in order to

- Ensure validity of the message
- Prove that it was sent by the party believed to have sent it
- Prove that only that party has access to the private key

FIGURE 14.8 Digital signature process



Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Cryptography Attacks

Cryptographic attacks are methods of evading the security of a cryptographic system by finding weaknesses in the cipher, protocol, or key management. The following are cryptographic attacks that can be performed by an attacker:

Cipher Text–Only Attack This attack requires the attacker to obtain several messages encrypted using the same encryption algorithm. The key indicators of a cipher text–only attack are the following:

- The attacker does not have the associated plain text.
- The attacker attempts to crack the code by looking for patterns and using statistical analysis.

Known–Plain Text Attack This attack requires the attacker to have the plain text and cipher text of one or more messages. The goal is to discover the key. This attack can be used if you know a portion of the plain text of a message.

Chosen–Plain Text Attack This type of attack is carried out when an attacker has the plain text messages of their choosing encrypted. An attacker can analyze the cipher text output of the encryption.

Chosen–Cipher Text Attack This type of attack is carried out when the attacker can decrypt portions of the cipher text message of their choosing. The attacker can use the decrypted portion of the message to discover the key.

A replay attack occurs when the attacker can intercept cryptographic keys and reuse them at a later date to either encrypt or decrypt messages to which they may not have access.

A brute-force attack involves trying all possible combinations (such as keys or passwords) until the correct solution is identified. Brute-force attacks are usually successful but require time and are usually costly.

Summary

Cryptography has been created to keep secrets from those not authorized to view the information. Cryptography's goal is to keep that information private while also ensuring it can travel across unsecure networks such as the Internet unmolested and unaltered. In many cases, cryptography is just a means of delaying viewing of information for a period of time until the information is no longer useful. Symmetric encryption secret keys are used primarily for performing bulk data encryption whereas asymmetric keys are used for transferring a secret key securely to a system.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Exam Essentials

Define the two types of encryption. Symmetric key and asymmetric key encryption are the two main types of encryption.

Understand the methods used to scramble data during encryption. Substitution and transposition methods are the basis of encryption and are used to scramble data during the encryption process.

Identify the common encryption algorithms. MD5, SHA, RC4, RC5, and Blowfish are the most common encryption algorithms.

Know how public and private keys are created. A public key and a private key are created simultaneously as a key pair and are used to encrypt and decrypt data.

Data encrypted with one member of the key pair can only be decrypted by the other.

Know the definition of cryptography. Cryptography is the process of encrypting data through a mathematical process of scrambling data known as an encryption algorithm.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Review Questions

1. How many keys exist in a public/private key pair?
   - **A.** 1
   - **B.** 2
   - **C.** 3
   - **D.** 4
2. How many keys are needed for symmetric key encryption?
   - **A.** 1
   - **B.** 2
   - **C.** 3
   - **D.** 4
3. Which of the following key lengths would be considered uncrackable? (Choose all that apply.)
   - **A.** 512
   - **B.** 256
   - **C.** 128
   - **D.** 64
4. What algorithm outputs a 128-bit message digest regardless of the length of the input?
   - **A.** SHA
   - **B.** MD5
   - **C.** RC4
   - **D.** RC6
5. What algorithm outputs a 160-bit key with variable-length input?
   - **A.** SHA
   - **B.** MD5
   - **C.** RC4
   - **D.** RC6
6. Which algorithm is used in the digital signature process?
   - **A.** RC4
   - **B.** RC5
   - **C.** Blowfish
   - **D.** MD5

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

7. What is cryptography?
   - **A.** The study of computer science
   - **B.** The study of mathematics
   - **C.** The study of encryption
   - **D.** The creation of encryption algorithms

8. What is the process of changing the order of some characters in an encryption key?
   - **A.** Transposition
   - **B.** Subtraction
   - **C.** Substitution
   - **D.** Transrelation

9. Data encrypted with the server's public key can be decrypted with which key?
   - **A.** The server's public key
   - **B.** The server's private key
   - **C.** The client's public key
   - **D.** The client's private key

10. Which type of encryption is the fastest to use for large amounts of data?
    - **A.** Symmetric
    - **B.** Public
    - **C.** Private
    - **D.** Asymmetric

11. What is the goal of a known–plain text attack?
    - **A.** To read the encrypted data
    - **B.** To gain access to the public key
    - **C.** To discover the encryption key
    - **D.** To validate the sender of the data

12. Which cryptographic attack attempts to crack the code by looking for patterns and using statistical analysis?
    - **A.** Cipher text–only attack
    - **B.** Chosen–plain text attack
    - **C.** Chosen–cipher text attack
    - **D.** Brute-force attack

13. Which two factors are of concern when using brute-force attacks against encryption?
    - **A.** Time
    - **B.** Money
    - **C.** Knowledge of the sender
    - **D.** The ability to capture data

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

14. Which program is useful in ensuring the integrity of a file that has been downloaded from the Internet?
    - **A.** Tripwire
    - **B.** Norton Internet Security
    - **C.** Snort
    - **D.** WinMD5

15. What are some of the common fields in an x.509 certificate? (Choose all that apply.)
    - **A.** Secret Key
    - **B.** Expiration Date
    - **C.** Issuer
    - **D.** Public Key

16. What is the standard format for digital certificates?
    - **A.** x.500
    - **B.** x.509
    - **C.** x.25
    - **D.** XOR

17. What would the cipher text result be of a value of 1 in plain text and 0 in the secret key after an XOR process?
    - **A.** 1
    - **B.** 0

18. What are two components of a PKI?
    - **A.** User passwords
    - **B.** Digital certificates
    - **C.** Encrypted data
    - **D.** CA

19. What element of the CIA triad ensures that the data sent is the same data received?
    - **A.** Confidentiality
    - **B.** Integrity
    - **C.** Authentication

20. What is the purpose of a hash?
    - **A.** To ensure confidentiality when using a public network such as the Internet
    - **B.** To ensure integrity of a transferred file
    - **C.** To ensure only authorized users are accessing a file
    - **D.** To ensure the data is available to authorized users

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.

Answers to Review Questions

1. B. Two keys, a public key and a private key, exist in a key pair.
2. A. The same key is used to encrypt and decrypt the data with symmetric key encryption.
3. A, B. A key length of 256 bits or more is considered uncrackable.
4. B. MD5 outputs a 128-bit digest with variable-length input.
5. A. SHA outputs a 160-bit key with variable-length input.
6. D. MD5 is used in the digital signature process.
7. C. Cryptography is the study of encryption.
8. A. Transposition is the process of changing the order of some characters in an encryption process.
9. B. Data can be decrypted with the other key in the pair—in this case, the server's private key.
10. A. Symmetric key encryption is fast and best to use when you have large amounts of data.
11. C. The goal of a known–plain text attack is to discover the encryption key.
12. A. A cipher text–only attack attempts to crack the encryption using cryptoanalysis.
13. A, B. Time and money are the two biggest concerns when attempting to break encryption using a brute-force method.
14. D. WinMD5 can be used to verify the integrity of a file downloaded from the Internet.
15. C, D. An x.509 certificate includes a field for Issuer and Public Key.
16. B. x.509 is the standard for digital certificates.
17. A. Different values such as 1 and 0 in an XOR process result in a value of 1.
18. B, D. CA (certificate authorities) and digital certificates are two components of a PKI.
19. B. Integrity ensures the data is not modified in transit.
20. B. A hash is a one-way encryption used to validate the integrity of a file.

Chapter 14. Cryptography. CEH® Certified Ethical Hacker Study Guide, ISBN: 9780470525203
Prepared for puneet_kumar@intuit.com, Puneet Kumar
Copyright © 2010 by Wiley Publications Inc.. This download file is made available for personal use only and is subject to the Terms of Service. Any other use requires prior written consent from the copyright owner. Unauthorized use, reproduction and/or distribution are strictly prohibited and violate applicable laws. All rights reserved.