**Chapter 8**

**Information Security**

**A Guide to this Instructor’s Manual:**

We have designed this Instructor’s Manual to supplement and enhance your teaching experience through classroom activities and a cohesive chapter summary.

This document is organized chronologically, using the same headings that you see in the textbook. Under the headings you will find: lecture notes that summarize the section, Teaching Tips, Class Discussion Topics, and Additional Projects and Resources. Pay special attention to teaching tips and activities geared towards quizzing your students and enhancing their critical thinking skills.

In addition to this Instructor’s Manual, our Instructor’s Resources also contain PowerPoint Presentations, Test Banks, and other supplements to aid in your teaching experience.

|  |
| --- |
| **At a Glance** |

**Instructor’s Manual Table of Contents**

* Overview
* Learning Objectives
* Teaching Tips and Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms
* Solutions to End-of-Chapter Exercises

|  |
| --- |
| Lecture Notes |

**Overview**

Chapter 8 introduces the issues of information security in the online world. It discusses methods for controlling access to information using authentication and authorization. It describes common kinds of attacks on a computer’s security, including viruses, worms, Trojan horses, and zombie armies. It describes a range of techniques for encrypting messages, starting from simple Caesar ciphers and other symmetric encryption algorithms and ending with an explanation of RSA public-key encryption. It discusses the importance of security protocols (SSL and TLS) for transmission of sensitive personal information over the web. And it explains the growing importance of computer security for small-scale, embedded systems that are connected to a network.

# **Learning Objectives**

* Explain the difference between authentication and authorization
* Explain the use of a hash function to encrypt passwords on a computer system
* Describe cyber-attacks including viruses, worms, Trojan horses, DoS attacks, and phishing, and explain how they differ from each other
* Describe ways to increase the security of information on your computer and online
* Encrypt and decrypt messages using simple Caesar ciphers and matrix-based block ciphers
* Describe the overall process used by symmetric encryption algorithms such as DES
* Describe the overall process used by RSA public-key encryption
* Explain why web transmission protocols such as SSL and TLS use multiple forms of encryption to secure data transfer over the web
* Explain the importance of computer security for networked embedded systems

# **Teaching Tips**

**8.1 Introduction**

1. Introduce the term **information security**. Talk about basic precautionary steps that can be taken to safeguard physical information devices such as laptops and smartphones. Emphasize that the security of the physical devices, and even of IDs and physical credit cards, pales in comparison with the security risks created by the Internet and the web.

**8.2 Threats and Defenses**

1. Introduce the term **authentication**. Ask students how many different usernames and passwords they use, how many different systems they log into on a regular basis. Make a list of the different types. Note the importance of keeping the file containing passwords from being accessed by an unauthorized person: **encryption** is necessary. Ideal encryption for passwords is easy to apply but hard to undo. A **hash function** works for this. Have students work through the book’s hash function for various strings. Point out that if they use one password for multiple accounts and somebody gets their hands on it, then they’ve managed to get the keys to their personal data kingdom.
2. Talk briefly about the idea of **cyberwarfare** and how it affects society when countries are hacking other countries for information and political gain.
3. Discuss different methods used to break into someone’s account: guessing the password, brute force trials of all possibilities, **password-cracking software**, or **social engineering** (getting the user to hand over the information).
4. Talk about **password managers** and how they can be leveraged to protect all the various passwords you may use. Other elaborate methods to secure accounts include fingerprint or retina scans and one-time password schemes, where a user receives a temporary password sent to a cell phone or similar device. These temporary passwords expire after a few seconds.
5. Discuss the new **dual authentication** methods being employed by some companies, where a one-time code is sent to a specific email address or texted to a cell phone after a login attempt.
6. Introduce the term **authorization**. Each user has permission to access certain information or files and to run certain software. The operating system checks for authorization with **access control lists (permissions)**; the **system administrator** or **superuser** ultimately determines what is authorized for each kind of user.
7. Internet security is more difficult than single-computer security. Introduce the term **malware** for software designed to attack a computer. **Viruses** embed themselves in other software and replicate when the software is run. **Worms** can transmit themselves from one computer to another. A **Trojan horse** is a piece of software that appears to do something useful but that also contains hidden malicious code. Discuss **keystroke loggers** and Trojan horse attacks from visiting websites (**drive-by exploit** or **drive-by download**).
8. Call attention to a newer form of malware called **ransomware**. Discuss the methods it employs. Talk about some of the more high-profile ransomware attacks in the past couple of years.
9. **Denial-of-service (DoS) attacks** direct many browsers to the same URL, effectively clogging that web server. One of the best technical terms ever is **zombie army** (also called **botnets**), which describes innocent infected computers being used to perform DoS attacks. Point out the scale of this criminal activity; the example in the book refers to a botnet involving 12 million computers.
10. Discuss the new, more sophisticated method of DDoS attacks: **reflection and amplification** attacks.
11. **Phishing** attacks involve emails claiming to be sent from legitimate organizations like banks, stores, or ISPs. The perpetrator hopes that the recipient will provide information like username and password, thinking the request is legitimate.
12. Talk about ways to keep data safe. Go over **antivirus software**, **firewall software**, and **antispyware**. Talk about the importance of applying any **security patches** released by companies in a timely fashion.
13. Distinguish **White hats** from **Black hats.**

**Quick Quiz 1**

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is when a computer or online service requests a username and password before permitting access.

Answer: Authorization

1. (True or false) Viruses are often spread through email attachments.

Answer: True

1. What does the term “zombie army” refer to in computer security terms?

Answer: Computers owned by innocent people that are co-opted by viruses or Trojan horse programs to support online criminal activities, such as DDoS attacks.

1. What is an email sent by a hacker pretending to be a legitimate business or entity requesting username and password information called?

Answer: Phishing

1. (True or false) Reflection and amplification is a newer way to protect your data by having a temporary code or password sent to a trusted device after a login attempt.

Answer: False

**8.3 Encryption**

1. Introduce the terms **cryptography**, **encryption**, and **decryption**. **Symmetric encryption algorithms** require the sender and receiver to share a special key with which messages may be encrypted or decrypted. **Asymmetric encryption algorithms** (**public key encryption algorithms**) avoid this problem: one key belonging to person A is made public and may be used to encrypt a message to A. Only A holds a private key, necessary for decrypting a message encrypted with the public key. Only A can decrypt the message.

|  |  |
| --- | --- |
| ***Teaching Tip*** | Have students practice using the different encryption algorithms discussed in the book. You could design a treasure hunt where each clue is encrypted using one of these techniques, with teams of students seeking to find the treasure. |

1. Introduce the term **Caesar cipher** as an example of a **stream cipher**. Note that cryptogram puzzles often found in newspapers use this kind of cipher; the fact that we can break them for fun indicates the problem with this kind of cipher.
2. Introduce the term **block cipher**, and note that each plaintext character contributes to multiple ciphertext characters. Go over examples of the book’s matrix-based block cipher carefully. This is a much more complex idea than a stream cipher.
3. Introduce the term **DES (Data Encryption Standard)**. This algorithm requires a complex sequence of manipulations. Take a simple example and work through the steps of the algorithm, at least one pass, very carefully. Note the similarity of decryption to encryption. Introduce the term **AES (Advanced Encryption Standard)** which is similar in form but uses longer keys in order to be harder to break.
4. Talk about the use of **steganography**, hiding information in plain sight, in terms of technology and computer files. Discuss the al-Qaeda operative who hid information inside a pornographic video.
5. Introduce the term **RSA** (named for Rivest, Shamir, and Adleman), an asymmetric encryption algorithm. RSA is based on the difficulty of finding prime factors for large numbers. Go through an example of how RSA works with great care.
6. Discuss quantum computing and RSA encryption.

|  |  |
| --- | --- |
| ***Teaching Tip*** | Refer students to the following page for a demonstration of RSA encryption: <http://people.eku.edu/styere/Encrypt/RSAdemo.html> |

**Quick Quiz 2**

1. An encryption algorithm that requires the sender and receiver to share a secret key is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Answer: symmetric encryption

1. (True or false) Julius Caesar invented the Caesar cipher.

Answer: True

1. (True or false) DES encryption is based on the difficulty of finding prime factors of large numbers.

Answer: False

1. \_\_\_\_ is the most common public-key encryption algorithm.

Answer: RSA

1. \_\_\_\_\_\_\_\_ is the act of hiding data in other types of files by changing the last bits of the date to match the information being hidden.

Answer: Steganography

**8.4 Web Transmission Security**

1. Introduce the terms **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)**. These standards allow the encryption of transmissions over the web, working between the application and transport layers. These use both RSA and DES encryption: RSA encryption is established but used only to encrypt a DES shared key, and then (less computationally expensive) DES may be used from then on.
2. Talk about **public-key certificates (digital certificate)** and how these play into Internet communications and safety.
3. Talk about how systems **handshake** to setup the information exchange between systems.
4. Discuss the **Virtual Private Network (VPN)** and how it can help keep data safe when in public spaces.

**8.5 Embedded Computing**

1. Introduce the term **embedded computers**. Note the proliferation of embedded computers in everything these days, including furnaces, automobiles, and control systems of every type. The newest trend is to connect these systems to the network to share data and get updates. Cyber-attacks on embedded systems can cause chaos.

**8.6 Conclusion**

1. Computer systems are vulnerable to different types of attacks.
2. The weakest point of computer security is people.
3. Varying types of encryption exist to provide different levels of protection.

**8.7 Summary of Level 3**

1. Hardware described in Chapters 4 and 5 is unusable by the average user.
2. The operating system provides the virtual environment the ease of use for the average user to make use of the hardware in a computer system.
3. This hardware/software combination is vulnerable to attack, and therefore system security and encryption and security is important to safeguard data both locally and on the web.

# **Class Discussion Topics**

1. What kinds of cyber-attacks have you experienced? Have you had a computer that was infected with a virus? Have you been unable to use a site by experiencing a DoS attack or downloaded spyware or a Trojan horse? Have you fallen for a phishing scheme? What do you do to secure your information on the Internet?
2. How many passwords do you use?
3. What are the pros and cons of symmetric versus asymmetric encryption algorithms? What issues must be considered when deciding what kind of encryption to use?
4. Imagine a networked embedded system attached to your air conditioning system. This system permits the power company to raise the thermostat, or cycle the system on and off, when energy demands are high. If every household had such a device, what might be the ramifications of a cyber-attack?
5. Do you believe that “hackers” who do things like expose the identity of rapists are White hats or Black hats? Regardless of the law, do you feel they are being ethical? Are they being moral? Is it right for them to be sentenced to a longer jail term than the individuals they uncovered?

# **Additional Projects**

1. Form into groups, and create a simple Caesar cipher for your group, keeping it secret from other groups. Use your cipher to encrypt a sentence-long message. Then trade messages with another group, and see how long it takes you to break the encryption.
2. Look up information on the uses of public key encryption for sending secure messages and for creating secure electronic “signatures.” Describe how keys are distributed and used for these purposes.
3. As a group, work through the matrix-based block cipher described in the book for encoding a short message. Check your work with another group.

# **Additional Resources**

1. News article about new approaches to authentication: <http://www.networkworld.com/research/2007/060407-multifactor-authentication.html>
2. Article about distributed denial-of-service attacks: <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html>
3. Take an entire MIT course online to learn about system security:

https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm

**Key Terms**

* **AES (Advanced Encryption Standard)**: A symmetric encryption algorithm that is newer than DES and uses a longer secret key.
* **Access control lists (permissions)**: A list of controls that specify exactly what a user is allowed to do with each data file on a system or network.
* **Antispyware**: Software that checks for the presence of a malicious program to capture personal information that has been entered on webpages.
* **Antivirus software**: Software designed to catch any possible virus attacks before they occur or clean up the damage if they do occur.
* **Asymmetric encryption algorithm/public-key encryption algorithm**: An encryption algorithm where the encryption key is made public but the decryption key, which is different, is known only to the receiver.
* **Authentication**: The process of verifying who has the right to gain access to the computer.
* **Authorization**: Governs what an authenticated user of a computer is allowed to do.
* **Block cipher**: Any encryption algorithm that encodes a block of characters together so that each coded character is the result of several plaintext characters.
* **Botnet**: A collection of infected computers under the control of a central site that can direct a DoS attack.
* **Caesar cipher**: An encryption algorithm that shifts each character in the message to another character some fixed distance farther along in the alphabet.
* **Cryptography**: The science of secret writing.
* **Cyberwarfare**: Computer attacks from one country on the computing resources of another country with intent to damage or destroy computer systems or steal sensitive information.
* **Decryption**: The process of reversing the effects of encryption, using an algorithm that converts the encoded text back into the original text.
* **Denial-of-service (DoS) attack**: An attempt to disable a particular website by automatically directing many browsers to that site.
* **DES (Data Encryption Standard)**: A symmetric encryption algorithm developed in the 1970s but still widely used.
* **Drive-by download/drive-by exploit**: The process whereby an infected website downloads a Trojan horse to the computer of a user visiting that site.
* **Dual authentication**: The use of an additional temporary code or password sent to a trusted device to complete a login attempt with a correct username and password.
* **Embedded computer**: A computational device (chip, processor, computer) embedded within another system.
* **Encryption**: The process of using an algorithm to convert information into a representation that cannot be understood or utilized by anyone without the appropriate decryption algorithm.
* **Firewall software**: Software that filters what programs and network communications can access a computer.
* **Hacker**: Originally, someone proficient at tinkering with computers; now, someone who breaks into a computer system for the purpose of doing harm.
* **Handshake**: The exchange of setup information between the client and the server prior to sending real data.
* **Hash function**: An encryption process that is easy to apply but hard to undo.
* **Information security**: The goal of keeping information protected from those who should not have access to it.
* **Keystroke logger**: A hidden program that captures the user’s passwords and credit card numbers as they are typed.
* **Malware**: Malicious software designed to attack a computer.
* **Password-cracking software**: A program that automates a brute-force approach to finding a password for a given user ID by encrypting in turn all words in its dictionary using the known hash function.
* **Password manager software (password vault)**: A central site that securely stores all your passwords in encrypted form.
* **Phishing**: The practice of sending widespread emails in hopes of luring users to visit a fake website, where personal information can be collected.
* **Public-key certificate/digital certificate**: A certificate issued by a trusted third-party certificate authority.
* **Ransomware**: Software usually downloaded through an email attachment that encrypts the user’s files and demands payment for an unlock key.
* **Reflection and amplification**: A more sophisticated type of DDoS attack that fools the attacked system into thinking a DNS query is coming from a legitimate source, causing the system to flood itself with requests and sendouts.
* **Remote Desktop Protocol (RDP)**: The ability for employees to see and utilize another system at another location as though they were sitting at it.
* **RSA**: A public-key encryption algorithm developed at MIT by Ron Rivest, Adi Shamir, and Len Adleman.
* **Security patch**: An update, generally to the operating system, that adds new or improved security measures.
* **Social engineering**: The process of using people to get the information you want.
* **Spam**: Junk email.
* **SSL (Secure Sockets Layer)**: A series of protocols to ensure secure data transmission on the web.
* **Steganography**: The practice of hiding the very existence of a message, now usually within an image on the web.
* **Stream cipher**: Any encryption algorithm that encodes one character at a time.
* **Symmetric encryption algorithm**: An encryption algorithm that requires a secret key shared by the sender and receiver.
* **System administrator**: The person who has access to everything on a computer and who sets up the authorization privileges for all other users.
* **TLS (Transport Layer Security)**: An improved version of SSL.
* **Trojan horse**: A computer program that does some harmless little job but also contains code to perform malicious attacks.
* **Virtual private network (VPN)**: A connection made between a system and a network far away, usually through VPN tunnels, that hides data from the local network the computer is connected to.
* **Virus**: A computer program that embeds itself within another program or file in order to infect a host computer and then spread.
* **Worm**: Similar to a virus but can send copies of itself to other nodes on a computer network without having to be carried by an infected host file.
* **Zombie army**: Another term for a botnet.

**Solutions to End-of-Chapter Exercises**

1. Scenario (a) tells the person attempting to log on the name of the computing system and that there is no valid user name “jones”. Scenario (b) tells the person attempting to logon the name of the computing system but does not reveal which part of the “smith/password” combination is incorrect. Scenario (c) gives no information, not even the name of the computing system, until the correct userID/password is given.

a. Step 1: fido → 6 9 4 15  
 Step 2: 6 + 9 + 4 + 15 = 34  
 Step 3: 34 → 6 (34 = 4 × 7 with 6 left over)  
 Step 4: (6 + 1) × 9 = 63  
 Step 5: 63 → 36 → cf

b. Step 1: blank → 2 12 1 14 11  
 Step 2: 2 + 12 + 1 + 14 + 11 = 40  
 Step 3: 40 → 5 (40 = 5 × 7 with 5 left over)  
 Step 4: (5 + 1) × 9 = 54  
 Step 5: 54 → 45 → de

c. Step 1: ti34pper → 20 9 3 4 16 16 5 18  
 Step 2: 20 + 9 + 3 + 4 + 16 + 16 + 5 + 18 = 91  
 Step 3: 91 → 0 (91 = 13 × 7 with 0 left over)  
 Step 4: (0 + 1) × 9 = 9  
 Step 5: 9 → 9 → i

**3.**  a.u s e r → 21 19 5 18 → 43 39 11 37 → 43039011037

b. It is a bad hashing algorithm because it is completely reversible. Given the above string, it can be separated (because of the 0s) into four individual numbers, which reverses Step 3:

43 39 11 37

For each of these numbers, Step 2 can be reversed by subtracting 1, then dividing by 2:

21 19 5 18

Then reverse Step 1 by translating these numbers back into letters: u s e r

Therefore the original password can be recovered from the encrypted password.

**4.** a. There are 10 possibilities for each digit, so there are 10 × 10 × 10 × 10 = 10,000 possible passcodes.

b. 10,000 seconds, or about 2.78 hours

**5.** The number n of possible characters is 26 + 26 + 10 + 3 = 65, and the maximum length k of the password is 10. The total number of passwords, using the formula given in Section 8.2.1, is 1.36731E+18. At the rate of 10,000,000 tries per second, it would take over 4,000 years to generate and test all potential passwords.

**6.**  0.132353 seconds

**7.** This can be seen by constructing a table showing the number of infected machines at the beginning and end of each hour.

|  |  |  |
| --- | --- | --- |
| Hour | Beginning of hour | End of hour |
| 1 | 1 | (1 × 50) × 10% = 5 = 51 |
| 2 | 5 | (5 × 50) × 10% = 25 = 52 |
| 3 | 25 | (25 × 50) × 10% = 125 = 53 |
| 4 | 125 | (125 × 50) × 10% = 625 = 54 |
| 5 | 625 | (625 × 50) × 10% = 3125 = 55 |

At the end of the fifth hour, 3,125 machines have been infected. At the end of n hours, 5n machines will be infected.

**8.**  Here is the message:

We here at Marriott appreciate your loyalty as a customer. We want to make things more easy for you when you travel, so we have partnered with Hilton and Ritz-Carlton to create a unified rewards program. Now when you stay at any of these fine brand hotels, you will earn award points that can apply to a future stay at any of the three hotels. For you we will quick set this up, just click on the link below to get started:

http://www.Mariott.com

Clues:

1. You should always be suspicious when a company asks you to go to a website and enter personal information.

2. Grammar error #1: " make things more easy for you"

3. Grammar error #2: "we will quick set this up"

4. In the URL: Marriott is misspelled as Mariott

**9.**  Information is available on the Web.

**10**. a. Existing probability of failure per year is 2 events/4 years = 0.5 per year.

Existing risk exposure = ($600 + $12,000) \* 0.5 = $6300.

Risk exposure with backup server = ($600 + $12,000) \*0.2 = $2520

The difference is $6300 - $2520 = $3780, more than the cost of the new server. This would be a cost-effective measure.

b. With the new probability, the risk exposure with backup server =

($600 + $12,000) \*0.3 = $3780.

The difference is $6300 - $3780 = $2520, less than the cost of the new server. This would not be a cost-effective measure.

**11**. MOVE OUT AT DAWN

**12**. The s value is 12 and the decoded message is  
 ALL GAUL IS DIVIDED

**13**. a.  ×  =  (modulo 26)

b. ATTACK

**14**. 100111 ⊕ 110101 = 010010

**15.** a. 1.25hours

b. 0.77 seconds

**16**. 1. n = p\*q = 7\*11 = 77

2. m = (p – 1)\*(q – 1) = 6\*10 = 60

3. Choose e = 13 (e = 13 and m = 60 have no common factors)

4. Then d = 37 because e\*d = 37\*13 = 481 = 8\*60 + 1, so when we compute e\*d  
using wrap-around arithmetic with respect to 60, we get 1.

Another possibility is e = 11, d = 11

**17**. a. We must have d between 0 and m = 8; d = 3 because e\*d = 11\*3 = 33 = 4\*8 + 1.

b. The code for 3 is 311 using wrap-around arithmetic with respect to 15. 311 = 177147 = 11809\*15 + 12 → 12.

c. To decode, compute (12)3 using wrap-around arithmetic with respect to 15. 123 = 1728 = 115\*15 + 3 → 3.

**18.** 256 qubits could simultaneously represent all 256 possible keys.

**Challenge Work**

1. The result when a message is hashed is also called a message digest, which may give students another term to search for.

2. It is doubtful that a student can answer all of these questions about any virus, but some of this information should be available.

3. The plaintext is ONEIFBYLAND.