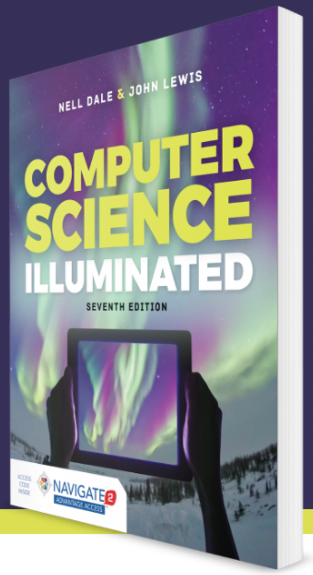


CHAPTER 17
LECTURE OUTLINE

Computer Science Illuminated, Seventh Edition

Nell Dale, PhD; John Lewis, PhD

Computer Security

17.1 Security at All Levels

Information Security

17.2 Preventing Unauthorized Access

Passwords

CAPTCHA

Fingerprint Analysis

17.3 Malicious Code

Antivirus Software

Security Attacks

17.4 Cryptography

17.5 Protecting Your Information Online

Credits

Nell Dell, PhD & John Lewis, PhD
Authors

Jones & Bartlett Learning
Publisher

Eric Pogue
Audio commentary plus slides with the grey backgrounds

Chapter Goals (1 of 2)

- Discuss the CIA triad
- List three types of authentication credentials
- Create secure passwords and assess the security level of others
- Define categories of malware
- List the types of security attacks
- Define cryptography

Chapter Goals (2 of 2)

- Encode and decode messages using various ciphers
- Discuss the challenges of keeping online data secure
- Discuss the security issues related to social media and mobile devices

Information Security

Information Security

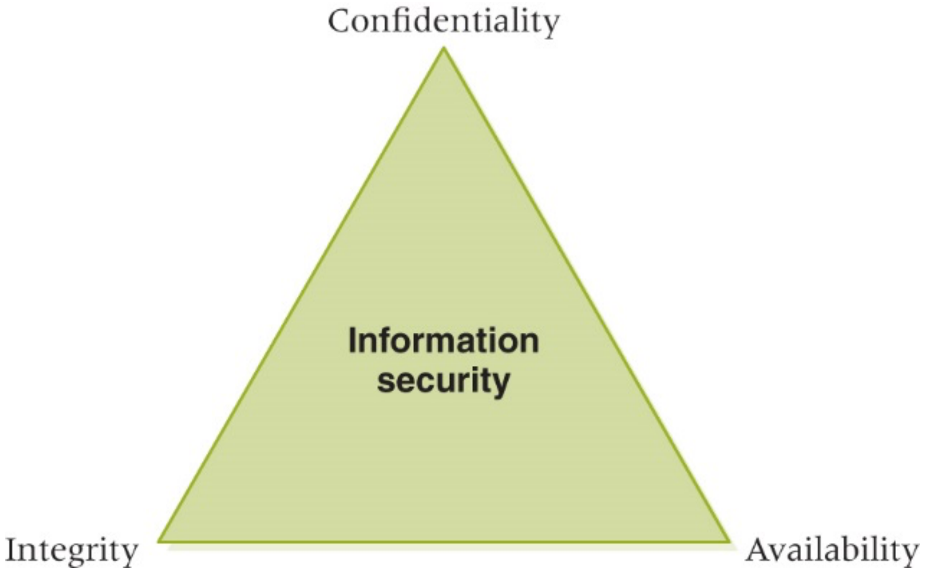
The techniques and policies used to ensure proper access to data

Cyber Security

The ability to protect resources accessible on the Internet

CIA Triad of Information Security

Ensuring that data can be modified only by appropriate mechanisms



The CIA triad of information security

Ensuring that data is protected from unauthorized access

The degree to which authorized users can access information for legitimate purposes

Information Security

Rick Analysis

Determining the nature and likelihood of the risks to key data

Planning for information analysis requires risk analysis

Goal is to minimize vulnerability to threats that put a system at the most risk

Preventing Unauthorized Access (1 of 5)

Authentication Credentials

Information users provide to identify themselves for computer access

- **User knowledge** Name, password, PIN
- **Smart card** A card with an embedded memory chip used for identification
- **Biometrics** Human characteristics such as fingerprints, retina or voice patterns

Preventing Unauthorized Access (2 of 5)

Guidelines for passwords

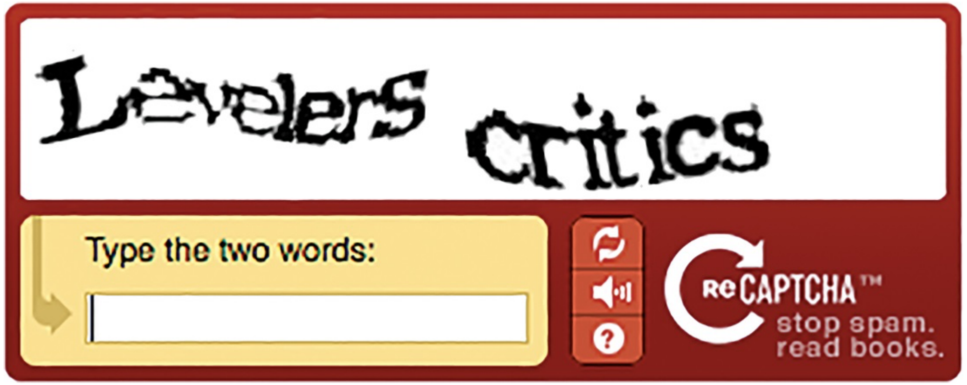
- Easy to remember, hard to guess
- Don’t use family or pet names
- Don’t make it accessible
- Use combination uppercase/lowercase letters, digits, and special characters
- Don’t leave computer when logged in
- Don’t ever tell anyone
- Don’t include in an email
- Don’t use the same password in lots of places

Preventing Unauthorized Access (3 of 5)

Typical Password Criteria

- Contain six or more characters
- Contain at least one uppercase and one lowercase letter
- Contain at least one digit
- Contain at least one special character

Preventing Unauthorized Access (4 of 5)



Courtesy of Google

A CAPTCHA form verification

CAPTCHA

Software that verifies that the user is not another computer

reCAPTCHA

Software that helps digitize books at the same time

Preventing Unauthorized Access (5 of 5)

Fingerprint analysis: A stronger level of verification than username and password

© LongHa2006/Getty images

A fingerprint scanner

What if somebody steals your digitized fingerprint?

Computer Security (1 of 3)

Malicious Code

A computer program that attempts to bypass appropriate authorization and/or perform unauthorized functions

- **Worm** stands alone, targets network resources
- **Trojan horse** disguised as benevolent resource
- **Virus** self-replicating
- **Logic bomb** set up to execute at system event

Antivirus Software

Software installed to detect and remove malicious code

Signature detection recognizes known malware and removes

Heuristics are strategies used to identify general patterns

Computer Security (2 of 3)

Security Attacks

An attack on the computer system itself

Password guessing Obvious

Phishing Trick users into revealing security information

Spoofing Malicious user masquerades as authorized user

Back door Unauthorized access to anyone who knows it exists

Computer Security (3 of 3)

Buffer overflow Defect that could cause a system to crash and leave the user with heightened privileges

Denial-of-service Attack that prevents authorized user from accessing the system

Man-in-the-middle Network communication is intercepted in an attempt to obtain key data

Have you ever experienced one of these?

Cryptography (1 of 4)

Cryptography

The field of study related to encoded information (comes from Greek word for "secret writing")

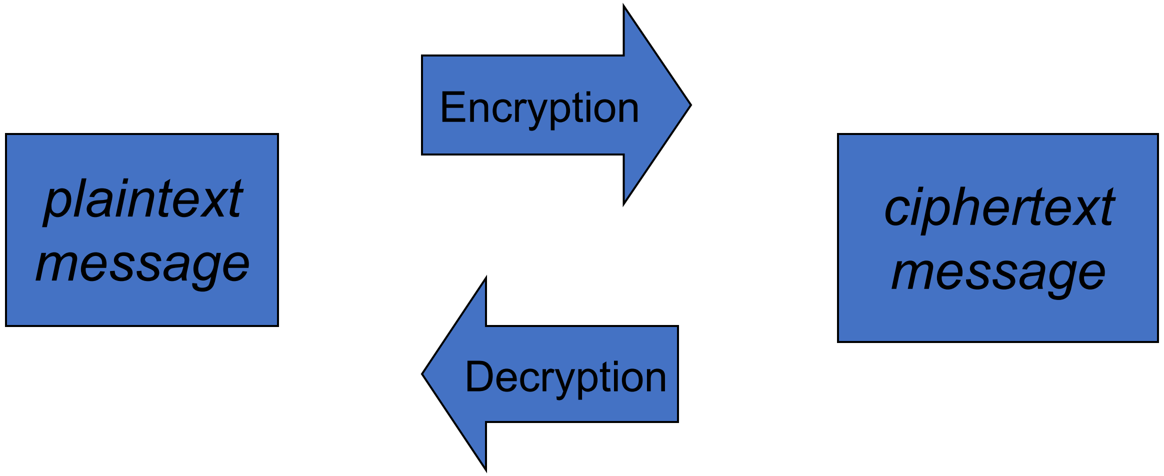
Encryption

The process of converting plaintext into ciphertext

Decryption

The process of converting ciphertext into plaintext

Cryptography (2 of 4)



Encrypted(Information) cannot be read

Decrypted(Encrypted(Information)) can be

Cryptography (3 of 4)

Cipher

An algorithm used to encrypt and decrypt text

Key

The set of parameters that guide a cipher

Neither is any good without the other

Cryptography (4 of 4)

Substitution Cipher

A cipher that substitutes one character with another

Caesar Cipher

A substitution cipher that shifts characters a certain number of positions in the alphabet

Transposition Ciphers

A cipher that rearranges the order of existing characters in a message in a certain way (e.g., a route cipher)

Substitution 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
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

Substitute the letters in the second row for the letters in the top row to encrypt a message

Encrypt(COMPUTER) gives FRPSXWHU

Substitute the letters in the first row for the letters in the second row to decrypt a message

Decrypt(Encrypt(COMPUTER)) gives COMPUTER

Why is this called the Caesar cipher?
What is the key?

Transposition Cipher

T O D A Y

+ I S + M

O N D A Y

Write the letters in a row of five, using '+' as a blank. Encrypt by starting spiraling inward from the top left moving counter clockwise

Encrypt(TODAY IS MONDAY) gives T+ONDAYMYADOIS+

Decrypt by recreating the grid and reading the letters across the row

The key are the dimensions of the grid and the route used to encrypt the data

Cryptanalysis

Cryptanalysis

The process of decrypting a message without knowing the cipher or the key used to encrypt it

Substitution and transposition ciphers are easy for modern computers to break

To protect information, more sophisticated schemes are needed

Public/Private Keys (1 of 2)

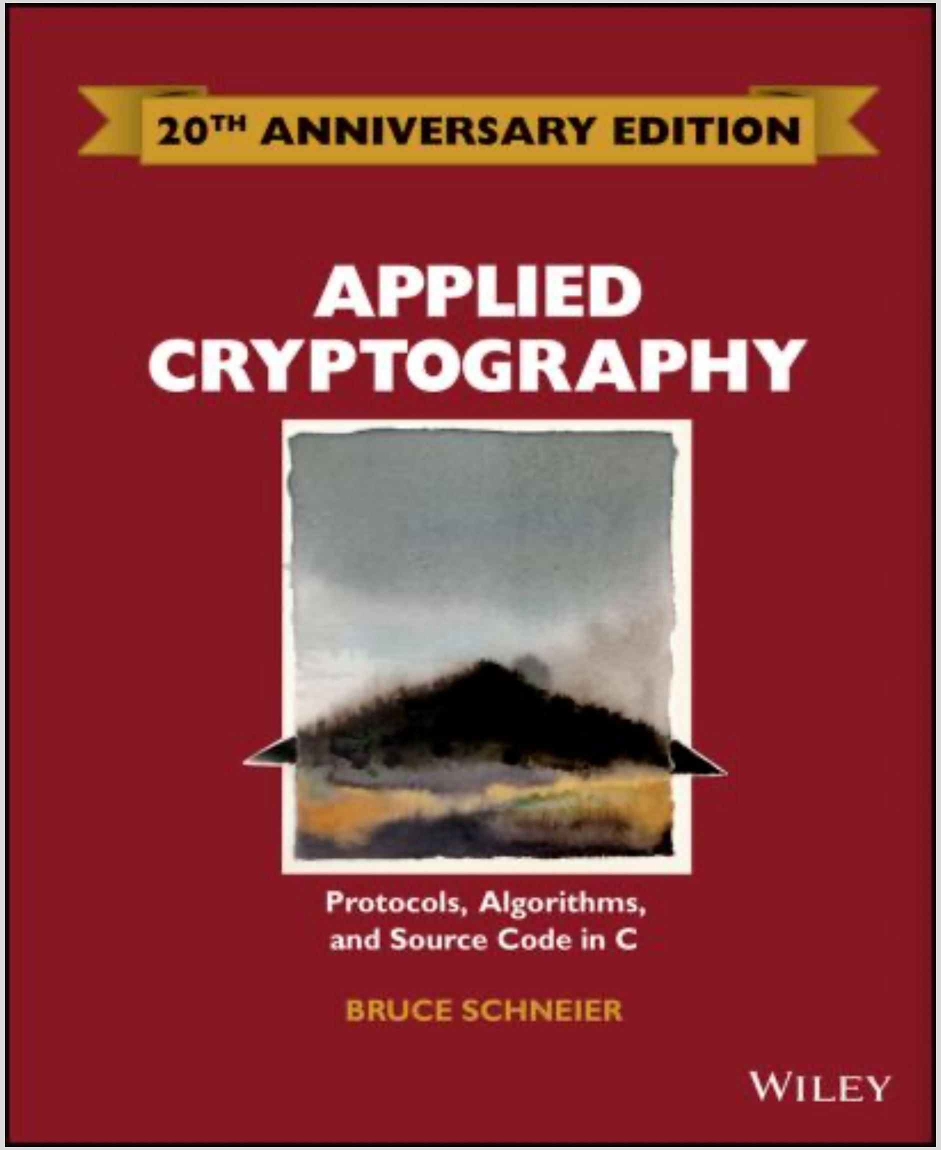
Public-Key Cryptography

An approach in which each user has two related keys, one public and one private

One's public key is distributed freely

A person encrypts an outgoing message, using the receiver's public key.

Only the receiver's private key can decrypt the message



20TH ANNIVERSARY EDITION

APPLIED CRYPTOGRAPHY

Protocols, Algorithms,
and Source Code in C

BRUCE SCHNEIER

WILEY

Public/Private Keys (2 of 2)

Digital Signature

Data that are appended to a message, made from the message itself and the sender's private key, to ensure the authenticity of the message

Digital Certificate

A representation of a sender's authenticated public key used to minimize malicious forgeries

Protecting Online Information

Why are smart people dumb about protecting online information?

- The Internet creates a false sense of anonymity
- People make assumptions about how securely their information is being treated
- People don’t think about the ramifications of sharing information

Security and Portable Devices

Smartphones, tablets, and laptops combined with GPS capabilities can pose ethical problems

- Apple iPhone and Google log and transmit data about users
- Law enforcement makes use of this data in criminal investigations
- U.S. Customs and Border Protection asserted the authority to seize and copy information in portable electronic devices for any reason

Final Comments

Chapter 17 Lecture