Chapter 17
Information Science

Chapter Objectives

Check off these skills when you feel that you have mastered them.

- ☐ Know what a binary code is.
- ☐ Use the diagram method to determine or verify a code word, given the message.
- ☐ Use the diagram method to decode a received message.
- ☐ Be able to compute check digits for code words given the parity-check sums for the code.
- ☐ Be able to determine the distance between two *n*-tuples of 0's and 1's.
- ☐ Be able to determine the weight of a code word and the minimum weight of the nonzero code words in a code (for binary codes, the minimum weight is the same as the minimum distance between code words).
- ☐ Know what nearest-neighbor decoding is and be able to use it for decoding messages received in the Hamming code of Table 17.2.
- ☐ Be able to encode and decode messages that have symbols (such as letters of the alphabet) expressed in binary form.
- ☐ Be able to make observations regarding frequently (or infrequently) occurring letters.
- ☐ Be able to decode using a Huffman code and be able to create a Huffman code, given a table of probabilities.
- ☐ Be able to encode and decode messages using the Caesar and Vigenère ciphers.
- ☐ Be able to add binary strings.
- ☐ Be able to perform calculations using modular arithmetic.
- ☐ Understand how the RSA public key encryption scheme works.
- ☐ Be able to complete a truth table given 2 or 3 statements and the connectives NOT, OR, and AND.
- ☐ Be able to determine if two statements are logically equivalent.

Guided Reading

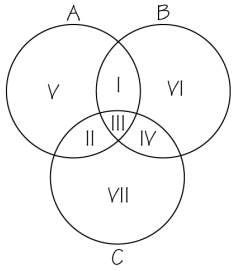
Introduction

In this chapter we consider some sophisticated techniques to detect and correct errors in digitally transmitted messages. We also take a look at methods that have been developed for the compression of data and for protection of the confidentiality of our messages. The Internet was originally used only by a few organizations as a source of information, but use of the Internet has become far more widespread. Now the Internet is used for shopping, entertainment, games, and much more. Web search efficiency is of importance with such wide spread use.

Section 17.1 Binary Codes

Key idea

Most computerized data are stored and transmitted as sequences of 0's and 1's. We can store a data string of length 4 in regions I through IV, respectively.



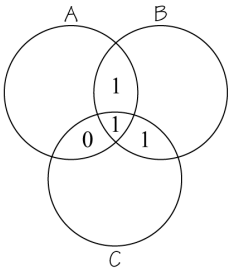
Regions V, VI, and VII have appended digits so that the sum of the regions for each circle has **even parity**. The encoded messages are called **code words**. This scheme is helpful to detect and even correct errors.

Example A

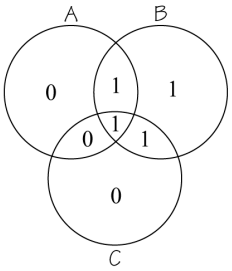
Store the data string 1011 along with its appended digits correctly in a three-circle diagram. What is the code word?

Solution

Original data string



Coded data string



The code word is 1011010.

Question 1

If a code word was received as 0100011, what region (if any) would be changed to decode the message using the diagram method?

Answer

Region III

Section 17.2 Encoding with Parity-Check Sums

🗝 Key idea

If a string of digits $a_1\ a_2\ a_3\ a_4$ is a message, then we can create a code word in a **binary linear code** by adding check digits that are the **parity-check sums** $a_1 + a_2 + a_3$, $a_1 + a_3 + a_4$, and $a_2 + a_3 + a_4$.

𝒢 Example B

What is the code word for the message 1100?

Solution

$a_1 + a_2 + a_3 = 2$, even parity; so the first check digit is 0. Both $a_1 + a_3 + a_4$ and $a_2 + a_3 + a_4 = 1$, odd parity; so the last two check digits are 1. The code word is therefore, 1100011.

🗝 Key idea

Since there may be errors in the coding process or transmission, we use the **nearest-neighbor decoding method** to find the code word with the shortest distance (number of positions in which the strings differ) from the received message. Use Table 17.1 on page 620.

𝒢 Example C

Using the nearest-neighbor method, decode these two code words.

a) 1110110
b) 0110010

Solution

a) The distance between the strings is 1, the error is in the sixth digit. 1110110 should be 1110100.
b) The distance is 0, there is no error. The message is a valid code word.

🗝 Key idea

The weight of a binary code is the minimum number of 1's that occur among all nonzero code words of that code.

🗝 Key idea

In a **variable-length code**, we can use **data compression** to make the shortest code words correspond to the most frequently occurring strings. Morse code is an example.

🗝 Key idea

In encoding a sequence of letters with a binary code (or decoding the binary code), we need an assignment of letters and code.

𝒢 Example D

Use $A \to 0,\ B \to 10,\ C \to 110,\ D \to 1110,\ E \to 11110,\ F \to 111110,\ G \to 1111111$ to decode the following.

$$01110111101111111111111011011100$$

Solution

Noticing the location of the zeros, 01110111101111111111111011011100 can be written as 0, 1110, 11110, 1111111,111110, 110, 1110, 0. Thus we have, *ADEGFCDA*.

Key idea

Huffman coding assigns to letters of the alphabet strings of variable size depending on the frequency a letter occurs or an assigned probability. To do this one needs to create a **code tree** (binary tree) performing the following steps.

- List the letters in increasing order top to bottom in terms of their probabilities. Note: The sum of the probabilities will be 1.
- The two letters that have the lowest probability of occurring get grouped together. Their probabilities are summed and the letter that has the smallest probability of occurring appears on the left. Rearrange the letters (two are grouped together), if necessary, in terms of their probabilities of occurring. From here on out a group of letters can consist of more than one letter.
- Continue this process with the new list until all letters appear in a string and the probability is 1.
- The letters/combination of letters are now spread out into a tree, working backwards. Figure 17.7 on page 633 demonstrates this with *EC* having probability 0.425 placed with a 0 on the top branch and *FDBA* having probability 0.575 placed with a 1 on the bottom branch.
- Read the variable string code for the letters right to left.

Question 2

Use a Huffman tree code to assign a binary code given the following.

A	B	C	D	E	F	G
0.105	0.235	0.100	0.115	0.195	0.107	0.143

Answer

$A = 001$, $B = 10$, $C = 000$, $D = 011$, $E = 111$, $F = 010$, $G = 110$.

Section 17.3 Cryptography

Key idea

Encryption of stored and transmitted data protects its security. For example, passwords are stored in encrypted form in computers.

Key idea

The so-called **Caesar cipher** is a cryptosystem that assigns a letter of the alphabet to another letter of the alphabet by shifting each letter of the alphabet by a fixed algorithm. Since there is a limited number of letters of the alphabet, there is a limited number of possible shifts.

Key idea

Modular arithmetic can be used in encrypting information. The notation $a \bmod n$ is read as a modulo n. a and n are both positive integers. $a \bmod n$ is the remainder when a is divided by n.

Example E

Calculate the following.

a) $41 \bmod 26$

b) $112 \bmod 11$

c) $7 \bmod 12$

d) $8 \bmod 8$

Solution

a) $41 \bmod 26 = 15$ because $41 = 1 \cdot 26 + 15$.

b) $112 \bmod 11 = 2$ because $112 = 10 \cdot 11 + 2$.

c) $7 \bmod 12 = 7$ because $7 = 0 \cdot 12 + 7$.

d) $8 \bmod 8 = 0$ because $8 = 1 \cdot 8 + 0$.

🗝 Key idea

The **Vigenère cipher** requires a key word that will first shift each letter of the word to be encoded. Each letter of the word to be encoded is identified by a position 0 – 25 (A is located in position 0, not 1). The code word then shifts each letter and that result is evaluated modulo 26.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Location	0	1	2	3	4	5	6	7	8	9	10	11	12
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Location	13	14	15	16	17	18	19	20	21	22	23	24	25

Example F

Use the Vigenère cipher with the keyword PEELING to encrypt the message I'M NOT FEELING WELL. Note: The apostrophe is not encrypted.

Solution

P is in the position 15; E is in position 4; L is in position 11; I is in position 8, N is in position 13, and G is in position 6.

Original	Location			Encrypted
I	8	15	$(8+15) \bmod 26 = 23 \bmod 26 = 23$	X
M	12	4	$(12+4) \bmod 26 = 16 \bmod 26 = 16$	Q
N	13	4	$(13+4) \bmod 26 = 17 \bmod 26 = 17$	R
O	14	11	$(14+11) \bmod 26 = 25 \bmod 26 = 25$	Z
T	19	8	$(19+8) \bmod 26 = 27 \bmod 26 = 1$	B
F	5	13	$(5+13) \bmod 26 = 18 \bmod 26 = 18$	S
E	4	6	$(4+6) \bmod 26 = 10 \bmod 26 = 10$	K
E	4	15	$(4+15) \bmod 26 = 19 \bmod 26 = 19$	T
L	11	4	$(11+4) \bmod 26 = 15 \bmod 26 = 15$	P
I	8	4	$(8+4) \bmod 26 = 12 \bmod 26 = 12$	M
N	13	11	$(13+11) \bmod 26 = 24 \bmod 26 = 24$	Y
G	6	8	$(6+8) \bmod 26 = 14 \bmod 26 = 14$	O
W	22	13	$(22+13) \bmod 26 = 35 \bmod 26 = 9$	J
E	4	6	$(4+6) \bmod 26 = 10 \bmod 26 = 10$	K
L	11	15	$(11+15) \bmod 26 = 26 \bmod 26 = 0$	A
L	11	4	$(11+4) \bmod 26 = 15 \bmod 26 = 15$	P

The encrypted message would be XQ RZB SKTPMYO JKAP.

Question 3

Given that CUTE was used as a key word for the Vigenère cipher to encrypt OUML KM CSA, what is the decrypted message?

Answer

Math is joy.

🗝 Key idea

In a **Cryptogram** one letter stands for another. By examining the frequency that a letter occurs, one can try to decipher it.

🗝 Key idea

Cable television companies verify your key as a valid customer before unscrambling the signal. They use a method of matching strings by "addition": 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0. Two strings match if they "add" to a string of 0's.

Example G

If your **key** is k = 10011101 and the transmitted message is $p + k$ = 01101100, what is the password p that will unscramble your signal?

Solution

Add the strings 10011101 + 01101100 to get 11110001.

$$\begin{array}{r} 10011101 \\ +01101100 \\ \hline 11110001 \end{array}$$

🗝 Key idea

The **multiplication property for modular arithmetic** is as follows.

$$(ab) \bmod n = \big((a \bmod n)(b \bmod n)\big) \bmod n$$

This property allows for simpler calculations.

Example H

Use the multiplication property for modular arithmetic to simply $\left(11^2 \cdot 12\right) \bmod 5$.

Solution

$$\begin{aligned} \left(11^2 \cdot 12\right) \bmod 5 &= \left[\left(11^2 \bmod 5\right)\left(12 \bmod 5\right)\right] \bmod 5 \\ &= \left[\left(11 \bmod 5\right)^2 (2)\right] \bmod 5 \\ &= \left[\left(1^2 \bmod 5\right)(2)\right] \bmod 5 \\ &= \left[(1 \bmod 5)(2)\right] \bmod 5 \\ &= \left[1(2)\right] \bmod 5 \\ &= 2 \bmod 5 \\ &= 2 \end{aligned}$$

Key idea

RSA public key encryption involves a procedure involving prime numbers and modular arithmetic. The procedure for sending and receiving messages is outlined on pages 642 – 643 of your text. In this form of encryption, letters start with 01 and a space is 00.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Location	01	02	03	04	05	08	07	08	09	10	11	12	13
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Location	14	15	16	17	18	19	20	21	22	23	24	25	26

Example I

Use the RSA scheme with $p = 7,\ q = 11,$ and $r = 7$ to decode the received numbers 31, 01 and 48.

Solution

1. Since $p = 7$ and $q = 11,\ n = pq = 7 \cdot 11 = 77.$
2. Since $p - 1 = 7 - 1 = 6$ and $q - 1 = 11 - 1 = 10,$ m will be the least common multiple of 6 and 10, namely 30.
3. We need to choose r such that it has no common divisors with 30. Thus, r can be 7. This confirms that $r = 7$ is a valid choice.
4. We need to find s.

$$r^2 \bmod m = 7^2 \bmod 30 = 49 \bmod 30 = 19$$
$$r^3 \bmod m = 7^3 \bmod 30 = 343 \bmod 30 = (11 \cdot 30 + 13) \bmod 30 = 13$$
$$r^4 \bmod m = 7^4 \bmod 30 = 2401 \bmod 30 = (80 \cdot 30 + 1) \bmod 30 = 1$$

Thus $t = 4.$

Since $s = r^{t-1} \bmod m,$ where $r = 7,\ m = 30,$ and $t = 4,$ we have the following.

$$s = 7^{4-1} \bmod 30 = 7^3 \bmod 30 = 13$$

5. Since $31^{13} \bmod 77 = \left[\left(31^4\right)^2 \cdot 31^5 \right] \bmod 77 = \left[\left(\left(31^4\right) \bmod 77 \right)^2 \cdot 31^5 \bmod 77 \right] \bmod 77$

$$= \left(60^2 \cdot 12\right) \bmod 77 = 43200 \bmod 77 = 3,\ R_1 = 3.$$

Since $1^{13} \bmod 77 = 1 \bmod 77 = 1,\ R_2 = 1.$

Since $48^{13} \bmod 77 = \left[\left(48^4\right)^2 \cdot 48^5 \right] \bmod 77 = \left[\left(\left(48^4\right) \bmod 77 \right)^2 \cdot 48^5 \bmod 77 \right] \bmod 77$

$$= \left(36^2 \cdot 34\right) \bmod 77 = 44064 \bmod 77 = 20,\ R_3 = 20.$$

Thus, the message is CAT.

Question 4

Use the RSA scheme with $p = 13,\ q = 11,$ and $r = 7$ to encrypt the message DOG.

Answer

Thus, the numbers sent are 82, 115, 6.

Section 17.4 Web Searches and Mathematical Logic

🗝 Key idea

Information on the Internet is stored on computers all around the world in the form of documents called Web pages. To find a particular source of information, web search engines are used to filter through web pages worldwide. These search engines use systematic search techniques called algorithms to gather information. When a search engine conducts a search, it must present the results in some sort of logical order. Many search engines rank each Web page according to features such as frequency with which the key word appears on the page or by the number of other pages that link to each page that is found.

🗝 Key idea

An expression in **Boolean logic** is simply a statement that is either true or false. Many search engines allow users to construct searches using Boolean logic.

🗝 Key idea

A **truth table** lists the values for an expression for all possible combinations of the Boolean variables P and Q. The letter T is used to indicate that an expression is true, and the letter F indicates that an expression is false.

🗝 Key idea

The **connectives** AND, OR, and NOT can be used to construct complex Boolean expressions.

- The expression NOT P is called the **negation** of P. If P is true then NOT P is false, and if P is false then NOT P is true. The standard mathematical notation for this is $\neg P$. The truth table is as follows.

P	$\neg P$
T	F
F	T

- The expression P AND Q is called the **conjunction** of P and Q. This expression is true when both P and Q are true and is false otherwise. The standard mathematical notation for this is $P \wedge Q$. The truth table is as follows.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

- The expression P OR Q is called the **disjunction** of P and Q. This expression is true if either P or Q (or both) are true and is false otherwise. The standard mathematical notation for this is $P \vee Q$. The truth table is as follows.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

🗝 Key idea

If two expressions have the same value (true or false) for each possible assignment of the Boolean variables, they are said to be **logically equivalent**.

Example J

Is the expression $P \vee (\neg Q \wedge R)$ logically equivalent to $(P \vee \neg Q) \wedge (P \vee R)$?

Solution

First we construct the truth table for $P \vee (\neg Q \wedge R)$.

P	Q	R	$\neg Q$	$\neg Q \wedge R$	$P \vee (\neg Q \wedge R)$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	F	T
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	F	T	F	F

Next we construct the truth table for $(P \vee \neg Q) \wedge (P \vee R)$.

P	Q	R	$\neg Q$	$P \vee \neg Q$	$P \vee R$	$(P \vee \neg Q) \wedge (P \vee R)$
T	T	T	F	T	T	T
T	T	F	F	T	T	T
T	F	T	T	T	T	T
T	F	F	T	T	T	T
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	T	T	T	T
F	F	F	T	T	F	F

Since the last columns of the two truth tables are identical, the expression $P \vee (\neg Q \wedge R)$ is logically equivalent to $(P \vee \neg Q) \wedge (P \vee R)$. .

Question 5

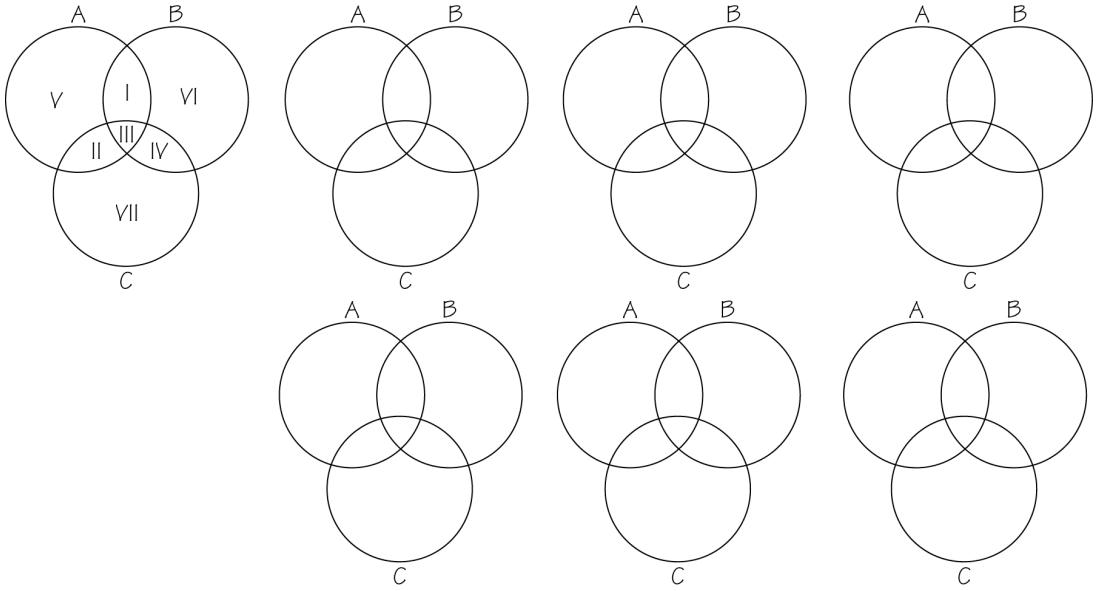
Is the expression $P \wedge (\neg Q \vee \neg R)$ logically equivalent to $(P \wedge \neg Q) \vee (P \wedge \neg R)$?

Answer

Yes

Homework Help

Exercises 1 – 6
Carefully read Section 17.1 before responding to these exercises. The following diagrams may be helpful.



Exercises 7 – 8
Carefully read Section 17.2 before responding to these exercises. The following table may be helpful for Exercise 7.

	$a_2 + a_3$	c_1	$a_1 + a_3$	c_2	$a_1 + a_2$	c_3	Code word
000							
100							
010							
001							
110							
101							
011							
111							

Exercises 9 – 10
Carefully read Section 17.2 before responding to these exercises. The following table may be helpful for Exercise 9.

	$a_2 + a_3 + a_4$	c_1	$a_2 + a_4$	c_2	$a_1 + a_2 + a_3$	c_3	Code word
0000							
1000							
0100							
0010							
0001							
1100							
1010							
1001							
0110							
0101							
0011							
1110							
1101							
1011							
0111							
1111							

Exercise 11
Carefully read Section 17.2 before responding to this exercise. The following table may be helpful.

	$a_1 + a_2$	c_1	$a_2 + a_3$	c_2	$a_1 + a_3$	c_3	Code word
000							
100							
010							
001							
110							
101							
011							
111							

Exercise 12
Carefully read Section 17.2 before responding to this exercise. The following table may be helpful.

	Weight	Append	Code word
0000000			
0001011			
0010111			
0100101			
1000110			
1100011			
1010001			
1001101			
0110010			
0101110			
0011100			
1110100			
1101000			
1011010			
0111001			
1111111			

Exercise 13
Carefully read Section 17.2 before responding to this exercise. The following table may be helpful.

	Weight	Append	Code word
0000000			
0001011			
0010111			
0100101			
1000110			
1100011			
1010001			
1001101			
0110010			
0101110			
0011100			
1110100			
1101000			
1011010			
0111001			
1111111			

Exercises 14 – 16
Carefully read Section 17.2 before responding to these exercises. The following table may be helpful

Exercises 17 – 19
Carefully read Section 17.2 before responding to these exercises. The following tables may be helpful for Exercises 17 and 18.

	$a_1 + a_2$	$c_1 = (a_1 + a_2) \bmod 3$	$2a_1 + a_2$	$c_2 = (2a_1 + a_2) \bmod 3$	Code word
00					
10					
20					
01					
02					
11					
22					
21					
12					

Code word	1211 differs by

Exercises 21 – 24
Carefully read Section 17.2 before responding to these exercises. Pay special attention to Examples 1 and 2 on pages 630 – 631.

Exercises 25 – 28
Carefully read Section 17.2 before responding to these exercises. The following copy of the Morse code should be helpful for Exercises 25 – 27. In Exercise 28, answers will vary.

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

Exercises 29 – 30
Carefully read Section 17.2 before responding to these exercises. The following tables should be helpful.

Exercise 29

2015	2015
2057 – 2015	

Exercise 30

1207	1207
1207 + 373	

Exercises 31 – 33
Carefully read Section 17.2 before responding to these exercises. Pay special attention to Huffman coding on pages 631 – 634.

Exercises 34 – 37
Carefully read Section 17.3 before responding to these exercises. Pay special attention to modular arithmetic and the Caesar cipher on pages 634 – 636.

Exercises 38 – 40
Carefully read Section 17.3 before responding to these exercises. Pay special attention to Example 3 on pages 636 – 637. The following tables may be helpful.

For Exercise 38

Original	Location			Encrypted
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	

For Exercise 39

Encrypted	Location				Decrypted
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		
			$= \quad \bmod 26 = (\quad)\bmod 26$		

Continued on next page

For Exercise 40

Original	Location			Encrypted
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	
			$(\quad)\bmod 26 = \quad \bmod 26 =$	

Exercises 41 – 47
Carefully read Section 17.3 before responding to these exercises. Pay special attention to pages 637 – 639.

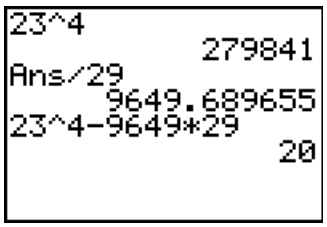
Exercise 48 – 50, 58
Visit the Web addresses indicated in these exercise.

Exercises 51 – 52
Carefully read Section 17.3 before responding to these exercises. Pay special attention to Example 4 on page 640.

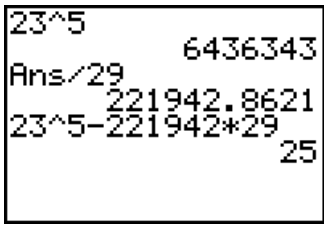
Exercises 53 – 57

Carefully read Section 17.3 before responding to these exercises. Pay special attention to the procedure outlined on pages 642 – 643. A calculator is needed to do modular arithmetic with large values. For example $23^{13} \bmod 29 = \left[\left(23^4\right)^2 \cdot 23^5\right] \bmod 29 = \left[\left(\left(23^4\right) \bmod 29\right)^2 \cdot 23^5 \bmod 29\right] \bmod 29$

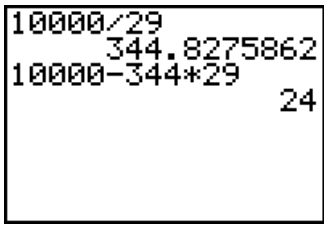
$23^4 \bmod 29 = 20$



$23^5 \bmod 29$



$23^{13} \bmod 29 = \left(20^2 \cdot 25\right) \bmod 29 = 10000 \bmod 29 = 24$



Exercises 59 – 67

Carefully read Section 17.4 before responding to these exercises. For exercises that require creating truth tables, the following should be helpful.

P	*Q*	*R*	
T	T	T	
T	T	F	
T	F	T	
T	F	F	
F	T	T	
F	T	F	
F	F	T	
F	F	F	

Do You Know the Terms?

Cut out the following 22 flashcards to test yourself on Review Vocabulary. You can also find these flashcards at http://www.whfreeman.com/fapp7e.

Chapter 17 **Information Science** **Binary linear code**	**Chapter 17** **Information Science** **Boolean Logic**
Chapter 17 **Information Science** **Caesar cipher**	**Chapter 17** **Information Science** **Cryptogram**
Chapter 17 **Information Science** **Cryptography**	**Chapter 17** **Information Science** **Data compression**
Chapter 17 **Information Science** **Decoding**	**Chapter 17** **Information Science** **Distance between two strings**

Logic attributed to that uses operations such as $\wedge, \vee$, and $\neg$ to connect statements.	**A code consisting of words composed of 0's and 1's obtained by using parity-check sums to append check digits to messages.**
A sentence (or message) that has been encrypted.	**A cryptosystem used by Julius Caesar whereby each letter is shifted the same amount.**
The process of encoding data so that the most frequently occurring data are represented by the fewest symbols.	**The study of how to make and break secret codes.**
The distance between two strings of equal length is the number of positions in which they differ.	**The process of translating received data into code words.**

Chapter 17 **Information Science** **Encryption**	**Chapter 17** **Information Science** **Even parity**
Chapter 17 **Information Science** **Key**	**Chapter 17** **Information Science** **Key word**
Chapter 17 **Information Science** **Logically equivalent**	**Chapter 17** **Information Science** **Modular arithmetic**
Chapter 17 **Information Science** **Nearest-neighbor decoding**	**Chapter 17** **Information Science** **Odd parity**

Even integers are said to have even parity.	**The process of encoding data to protect against unauthorized interpretation.**
A word used to determine the amount of shifting for each letter while encoding a message.	**A string used to encode and decode data.**
Addition and multiplication involving modulo n.	**Two expressions are said to be logically equivalent if they have the same values for all possible values of their Boolean variables.**
Odd integers are said to have odd parity.	**A method that decodes a received message as the code word that agrees with the message in the most positions.**

Chapter 17 **Information Science** **Parity-check sums**	**Chapter 17** **Information Science** **RSA public key encryption scheme**
Chapter 17 **Information Science** **Truth table**	**Chapter 17** **Information Science** **Variable-length code**
Chapter 17 **Information Science** **Vignenère code**	**Chapter 17** **Information Science** **Weight of a binary code**

A method of encoding that permits each person to announce publicly the means by which secret messages are to be sent to him or her.	**Sums of digits whose parities determine the check digits.**
A code in which the number of symbols for each code word may vary.	**A tabular representation of an expression in which the variables and the intermediate expressions appear in columns and the last column contains the expression being evaluated.**
The minimum number of 1's that occur among all nonzero code words of a code.	**A cryptosystem that utilizes a key word to determine how much each letter is shifted.**

Practice Quiz

1. If you use the circular diagram method to encode the message 1010, what is the encoded message?

a. 1010001

b. 1010010

c. 1101000

2. Suppose the message 1111100 is received and decoded using the nearest-neighbor method. What message is recovered?

a. 1111

b. 1110

c. 0111

3. What is the distance between received words 1111100 and 1101101?

a. 5

b. 4

c. 2

4. For the code C = $\{0000, 1010, 0101, 1111\}$, how many errors would have to occur during the transmission for a received word to possibly be encoded incorrectly?

a. 1

b. 2

c. 3

5. Use the encoding scheme $A \to 0,\ B \to 10,\ C \to 11$ to decode the sequence 0110011.

a. ABBAC

b. ACBAC

c. ACAAC

6. What is the sum of the binary sequences 1001101 and 1100011?

a. 1101111

b. 0101110

c. 0110000

7. Using modular arithmetic, $3^6 \bmod 20$

a. 3.

b. 9.

c. 19.

8. For the RSA scheme with $p = 11$ and $q = 17$, which of the following could be chosen as a value for *r*?

a. 5

b. 6

c. 9

9. For the RSA scheme with $m = 5$ and $r = 8,$ what is the value of s?

a. 2

b. 3

c. 5

10. Are $\neg(P \vee \neg Q)$ and $\neg P \vee \neg Q$ logically equivalent?

a. no

b. yes

c. can't tell

Word Search

Refer to page 652 of your text to obtain the Review Vocabulary. There are 22 hidden vocabulary words/expressions in the word search below. This represents all vocabulary. It should be noted that spaces and hyphens are removed as well as accents.

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

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____