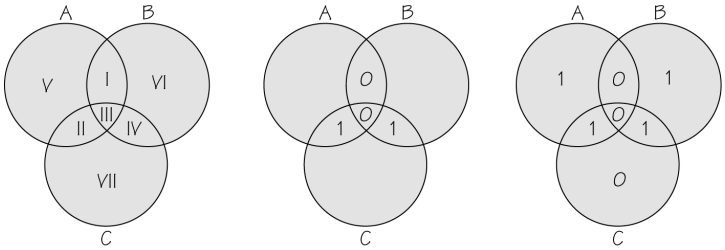
Chapter 17
Information Science

Solutions

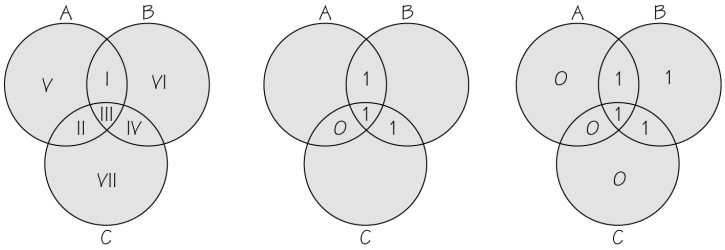
Exercises:

1. For 0101:



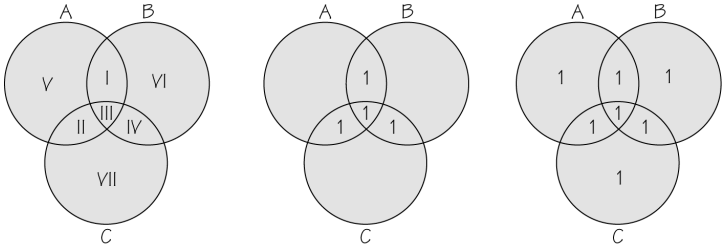
The code word given by regions I, II, III, IV, V, VI, VII is 0101110.

For 1011:



The code word given by regions I, II, III, IV, V, VI, VII is 1011010.

For 1111:

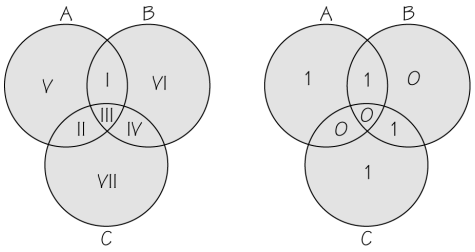


The code word given by regions I, II, III, IV, V, VI, VII is 1111111.

3. (a) When you compare 1**1011011** and 1**0100110**, they differ by 6 digits. Thus, the distance is 6.

(b) When you compare **0**111**10**100 and **1**111**01**100, they differ by 3 digits. Thus, the distance is 3.

5. There would be no change to 1001101 since the total number of 1's in each circle is even.



7. Consider the following table.

	a_2+a_3	c_1	a_1+a_3	c_2	a_1+a_2	c_3	Code word
000	0	**0**	0	**0**	0	**0**	**000000**
100	0	**0**	1	**1**	1	**1**	**100011**
010	1	**1**	0	**0**	1	**1**	**010101**
001	1	**1**	1	**1**	0	**0**	**001110**
110	1	**1**	1	**1**	2	**0**	**110110**
101	1	**1**	2	**0**	1	**1**	**101101**
011	2	**0**	1	**1**	1	**1**	**011011**
111	2	**0**	2	**0**	2	**0**	**111000**

Thus, the binary linear code is 000000, 100011, 010101, 001110, 110110, 101101, 011011, 111000.

9. Consider the following table.

	$a_2+a_3+a_4$	c_1	a_2+a_4	c_2	$a_1+a_2+a_3$	c_3	Code word
0000	0	**0**	0	**0**	0	**0**	**0000000**
1000	0	**0**	0	**0**	1	**1**	**1000001**
0100	1	**1**	1	**1**	1	**1**	**0100111**
0010	1	**1**	0	**0**	1	**1**	**0010101**
0001	1	**1**	1	**1**	0	**0**	**0001110**
1100	1	**1**	1	**1**	2	**0**	**1100110**
1010	1	**1**	0	**0**	2	**0**	**1010100**
1001	1	**1**	1	**1**	1	**1**	**1001111**
0110	2	**0**	1	**1**	2	**0**	**0110010**
0101	2	**0**	2	**0**	1	**1**	**0101001**
0011	2	**0**	1	**1**	1	**1**	**0011011**
1110	2	**0**	1	**1**	3	**1**	**1110011**
1101	2	**0**	2	**0**	2	**0**	**1101000**
1011	2	**0**	1	**1**	2	**0**	**1011010**
0111	3	**1**	2	**0**	2	**0**	**0111100**
1111	3	**1**	2	**0**	3	**1**	**1111101**

Thus, the binary linear code is 0000000, 1000001, 0100111, 0010101, 0001110, 1100110, 1010100, 1001111, 0110010, 0101001, 0011011, 1110011, 1101000, 1011010, 0111100, 1111101. No, since 1000001 has weight 2.

11. Consider the following table.

	$a_1 + a_2$	c_1	$a_2 + a_3$	c_2	$a_1 + a_3$	c_3	Code word
000	0	**0**	0	**0**	0	**0**	**000000**
100	1	**1**	0	**0**	1	**1**	**100101**
010	1	**1**	1	**1**	0	**0**	**010110**
001	0	**0**	1	**1**	1	**1**	**001011**
110	2	**0**	1	**1**	1	**1**	**110011**
101	1	**1**	1	**1**	2	**0**	**101110**
011	1	**1**	2	**0**	1	**1**	**011101**
111	2	**0**	2	**0**	2	**0**	**111000**

Thus, the binary linear code is 000000, 100101, 010110, 001011, 110011, 101110, 011101, 111000. 001001 is decoded as 001011; 011000 is decoded as 111000; 000110 is decoded as 010110; 100001 is decoded as 100101.

13. Consider the following table.

	Weight	Append	Code word
0000000	0	**0**	**00000000**
0001011	3	**1**	**00010111**
0010111	4	**0**	**00101110**
0100101	3	**1**	**01001011**
1000110	3	**1**	**10001101**
1100011	4	**0**	**11000110**
1010001	3	**1**	**10100011**
1001101	4	**0**	**10011010**
0110010	3	**1**	**01100101**
0101110	4	**0**	**01011100**
0011100	3	**1**	**00111001**
1110100	4	**0**	**11101000**
1101000	3	**1**	**11010001**
1011010	4	**0**	**10110100**
0111001	4	**0**	**01110010**
1111111	7	**1**	**11111111**

The extended code is 00000000, 00010111, 00101110, 01001011, 10001101, 11000110, 10100011, 10011010, 01100101, 01011100, 00111001, 11101000, 11010001, 10110100, 01110010, 11111111. The code will detect any three errors or correct any single error.

15. There are $2^5 = 32$ possible messages of length 5. There are $2^8 = 256$ possible received words.

17. Consider the following table.

	$a_1 + a_2$	$c_1 = (a_1 + a_2) \bmod 3$	$2a_1 + a_2$	$c_2 = (2a_1 + a_2) \bmod 3$	Code word
00	0	**0**	0	**0**	**0000**
10	1	**1**	2	**2**	**1012**
20	2	**2**	4	**1**	**2021**
01	1	**1**	1	**1**	**0111**
02	2	**2**	2	**2**	**0222**
11	2	**2**	3	**0**	**1120**
22	4	**1**	6	**0**	**2210**
21	3	**0**	5	**2**	**2102**
12	3	**0**	4	**1**	**1201**

Thus, the ternary code is 0000, 1012, 2021, 0111, 0222, 1120, 2210, 2102, 1201.

19. There are $3^4 = 81$ possible messages of length 5. There are $3^6 = 729$ possible received words.

21. 001100001111000 can be written as 0, 0, 110, 0, 0, 0, 111, 10, 0, 0. Thus we have, AATAAAGCAA.

23. 1111, 0, 10, 0, 0, 1110, 0, 10, 10 would be written as 111101000111001010. 001000110011110111010 can be written as 0, 0, 10, 0, 0, 110, 0, 1111, 0, 1110, 10. Thus we have *AABAACAEADB*.

25. *t*, *n*, and *r* would be the most frequently occurring consonants. *e* would be the most frequently occurring vowel.

27. In the Morse code, a space is needed to determine where each code word ends. In a fixed-length code of length k, a word ends after each k digits.

29. Given the following:

2015	2015
$2057 - 2015$	42
$2079 - 2057$	22
$2060 - 2079$	-19
$2050 - 2060$	-10
$2053 - 2050$	3
$2065 - 2053$	12
$2030 - 2065$	-35
$2025 - 2030$	-5
$2002 - 2025$	-23

the compressed numbers are 2015 42 22 -19 -10 3 12 -35 -5 -23; We go from 49 characters to 34 characters, a reduction of $\frac{49-34}{49} = \frac{15}{49} \approx 30.6\%$.

31. 11100100001001110110011010 can be written as 1110, 01, 00, 00, 10, 01, 110, 110, 01, 10, 10. Thus, the message is decoded to be *BCEEFCDDCFF*.

33. *B* is the least likely letter, *J* is the second least likely, and *G* is the third least likely letter.

35. RETREAT would be encrypted as UHWUHDW. DGYDQFH would be decoded as ADVANCE.

37. One can take a position, such as 0 and determine that it takes 13 iterations to arrive at 0 again.

$$(0+8) \bmod 26 = 8 \bmod 26 = 8$$
$$(8+8) \bmod 26 = 16 \bmod 26 = 16$$
$$(16+8) \bmod 26 = 24 \bmod 26 = 24$$
$$(24+8) \bmod 26 = 32 \bmod 26 = 6$$
$$(6+8) \bmod 26 = 14 \bmod 26 = 14$$
$$(14+8) \bmod 26 = 22 \bmod 26 = 22$$
$$(22+8) \bmod 26 = 30 \bmod 26 = 4$$
$$(4+8) \bmod 26 = 12 \bmod 26 = 12$$
$$(12+8) \bmod 26 = 20 \bmod 26 = 20$$
$$(20+8) \bmod 26 = 28 \bmod 26 = 2$$
$$(2+8) \bmod 26 = 10 \bmod 26 = 10$$
$$(10+8) \bmod 26 = 18 \bmod 26 = 18$$
$$(18+8) \bmod 26 = 26 \bmod 26 = 0$$

39. Given the key word BEATLES, we note that B is in the position 1; E is in position 4; A is in position 0; T is in position 19; L is in position 11; S is in position 18.

Encrypted	Location				Decrypted
S	18	1	$18 = 18 \bmod 26 = (17+1) \bmod 26$	17	R
S	18	4	$18 = 18 \bmod 26 = (14+4) \bmod 26$	14	O
L	11	0	$11 = 11 \bmod 26 = (11+0) \bmod 26$	11	L
E	4	19	$4 = 30 \bmod 26 = (11+19) \bmod 26$	11	L
T	19	11	$19 = 19 \bmod 26 = (8+11) \bmod 26$	8	I
R	17	4	$17 = 17 \bmod 26 = (13+4) \bmod 26$	13	N
Y	24	18	$24 = 24 \bmod 26 = (6+18) \bmod 26$	6	G
T	19	1	$19 = 19 \bmod 26 = (18+1) \bmod 26$	18	S
X	23	4	$23 = 23 \bmod 26 = (19+4) \bmod 26$	19	T
O	14	0	$14 = 14 \bmod 26 = (14+0) \bmod 26$	14	O
G	6	19	$6 = 32 \bmod 26 = (13+19) \bmod 26$	13	N
P	15	11	$15 = 15 \bmod 26 = (4+11) \bmod 26$	4	E
W	22	4	$22 = 22 \bmod 26 = (18+4) \bmod 26$	18	S

The original message was ROLLING STONES.

41. I'll.

43. To start, X would be an encrypted A or I. Similarly, G would be an encrypted A or I. The original statement is "I am a man."

45. could've or would've.

47. and

49. Oh, I love your magazine. Especially the "Enrich Your Word Power" section. I think it's really, really, really good.

51. (a)
$$\begin{array}{r} 10111011 \\ +\ 01111011 \\ \hline 11000000 \end{array}$$

(b)
$$\begin{array}{r} 11101000 \\ +\ 01110001 \\ \hline 10011001 \end{array}$$

53. 1. VIP converts to 220916.

2. We will send 22, 09, and 16 individually.

3. Since $p = 5$ and $q = 17$, $n = pq = 5 \cdot 17 = 85$.
Since $\text{GCF}(22, 85) = 1$, $\text{GCF}(9, 85) = 1$, and $\text{GCF}(16, 85) = 1$, we can proceed. (GCF stands for *greatest common factor*.) Thus, $M_1 = 22$, $M_2 = 09$, and $M_3 = 16$.

4. Since $R_i = M_i^r \bmod n$ and $r = 3$, we have the following.

$$R_1 = 22^3 \bmod 85 = (2 \cdot 11)^3 \bmod 85 = \left[\left(2^3 \cdot 11\right) \cdot 11^2\right] \bmod 85$$
$$= \left[\left[\left(2^3 \cdot 11\right) \bmod 85\right]\left[11^2 \bmod 85\right]\right] \bmod 85$$
$$= \left[(88 \bmod 85)(121 \bmod 85)\right] \bmod 85 = (3 \cdot 36) \bmod 85 = 108 \bmod 85 = 23$$

$$R_2 = 9^3 \bmod 85 = \left(3^2\right)^3 \bmod 85 = 3^6 \bmod 85 = \left[\left(3^5 \bmod 85\right)(3 \bmod 85)\right] \bmod 85$$
$$= \left[(243 \bmod 85)(3 \bmod 85)\right] \bmod 85 = (73 \cdot 3) \bmod 85 = 219 \bmod 85 = 49$$

$$R_3 = 16^3 \bmod 85 = \left(2^4\right)^3 \bmod 85 = 2^{12} \bmod 85 = \left[\left(2^7 \bmod 85\right)\left(2^5 \bmod 85\right)\right] \bmod 85$$
$$= \left[(128 \bmod 85)(32 \bmod 85)\right] \bmod 85 = (43 \cdot 32) \bmod 85 = (43 \cdot 2 \cdot 16) \bmod 85$$
$$= \left[(43 \cdot 2) \cdot 16\right] \bmod 85 = \left[(86 \bmod 85)(16 \bmod 85)\right] \bmod 85$$
$$= \left[1 \cdot (16 \bmod 85)\right] \bmod 85 = (16 \bmod 85) = 16$$

Thus, the numbers sent are 23, 49, 16.

55. 1. Since $p = 5$ and $q = 17$, $n = pq = 5 \cdot 17 = 85$.

2. Since $p - 1 = 5 - 1 = 4$ and $q - 1 = 17 - 1 = 16$, m will be the least common multiple of 4 and 16, namely 16.

3. We need to choose r such that it has no common divisors with 16. Thus, r can be 5. This confirms that $r = 5$ is a valid choice.

4. We need to find s such that $rs = 1 \bmod m$.

$$r^2 \bmod m = 5^2 \bmod 16 = 25 \bmod 16 = 9$$
$$r^3 \bmod m = 5^3 \bmod 16 = 125 \bmod 16 = 13$$
$$r^4 \bmod m = 5^4 \bmod 16 = 625 \bmod 16 = 1$$

Thus $t = 4$.

Since $s = r^{t-1} \bmod m$, where $r = 5$ and $t = 4$, we have the following.

$$s = 5^{4-1} \bmod 16 = 5^3 \bmod 16 = 125 \bmod 16 = 13$$

57. N converts to 14 and O converts to 15, but 14 and 77 have a greatest common divisor of 7. On the other hand, using blocks of length 4, NO converts to 1415 and the greatest common divisor of 77 and 1415 is 1.

59. As the following shows, since the entries in the column for the variable P are exactly the same as the entries in the column for $P \vee (P \wedge Q)$, the two expressions are logically equivalent.

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

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

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

Next we construct the truth table for $\neg P \vee \neg Q$

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

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

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

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

Continued on next page

63. continued

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

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

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

65. The truth table for $\neg P \vee Q$ is as follows.

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

Because the last column of this truth table is identical for the one for $P \to Q$, we conclude that the two expressions are logically equivalent.

67. Let *P* denote "it snows" and let *Q* denote "there is school." Then the statement "If it snows, there will be no school" can be expressed as $P \to \neg Q$. Similarly, the statement "it is not the case that it snows and there is school" can be expressed as $\neg(P \wedge Q)$. We now construct the truth tables for each of these expressions. A truth table for $P \to \neg Q$ is as follows.

P	Q	$\neg Q$	$P \to \neg Q$
T	T	F	F
T	F	T	T
F	T	F	T
F	F	T	T

A truth table for $\neg(P \wedge Q)$ is as follows.

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

Because the two tables have identical last columns, the two expressions are logically equivalent.