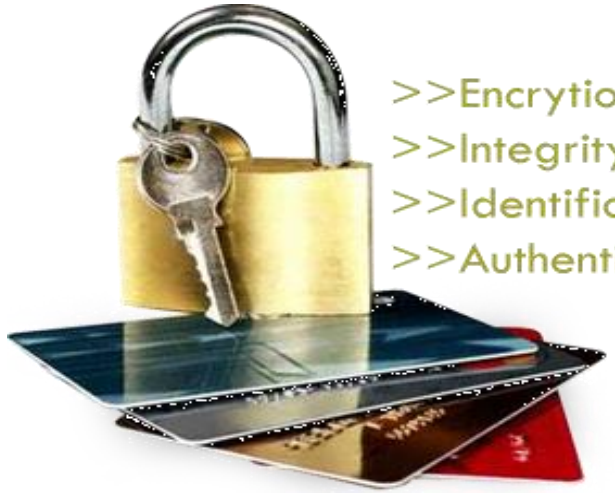
Information and System Security

Book Exercises



>>Encrytion
>>Integrity
>>Identification
>>Authentication

VIT-AP UNIVERSITY

Exercises

EXERCISES

1.6 Which security service(s) are guaranteed when using each of the following methods to send mail at the post office?

a. Regular mail
b. Regular mail with delivery confirmation
c. Regular mail with delivery and recipient signature
d. Certified mail
e. Insured mail
f. Registered mail

1.7 Define the type of security attack in each of the following cases:

a. A student breaks into a professor's office to obtain a copy of the next day's test.
b. A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.
c. A student sends hundreds of e-mails per day to another student using a phony return e-mail address.

Exercises

1.8 Which security mechanism(s) are provided in each of the following cases?

a. A school demands student identification and a password to let students log into the school server.

b. A school server disconnects a student if she is logged into the system for more than two hours.

c. A professor refuses to send students their grades by e-mail unless they provide student identification they were preassigned by the professor.

d. A bank requires the customer's signature for a withdrawal.

1.9 Which technique (cryptography or steganography) is used in each of the following cases for confidentiality?

a. A student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts it in a ball-point pen, and passes the pen to another student.

b. To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement.

c. A company uses special ink on its checks to prevent forgeries.

d. A graduate student uses watermarks to protect her thesis, which is posted on her website.

1.10 What type of security mechanism(s) are provided when a person signs a form he has filled out to apply for a credit card?

Exercises

EXERCISES

2.11 Which of the following relations are true and which are false?

$5 \mid 26 \quad 3 \mid 123 \quad 27 + 127 \quad 15 + 21 \quad 23 \mid 196 \quad 8 \mid 5$

2.12 Using the Euclidean algorithm, find the greatest common divisor of the following pairs of integers.

a. 88 and 220 b. 300 and 42 c. 24 and 320 d. 401 and 700

2.13 Solve the following.

a. Given gcd (a, b) = 24, find gcd (a, b, 16).
b. Given gcd (a, b, c) = 12, find gcd (a, b, c, 16)
c. Find gcd (200, 180, and 450).
d. Find gcd (200, 180, 450, 610).

2.14 Assume that n is a non-negative integer.

a. Find gcd $(2n + 1, n)$.
b. Using the result of part a, find gcd (201, 100), gcd (81, 40), and gcd (501, 250).

2.15 Assume that n is a non-negative integer.

a. Find gcd $(3n + 1, 2n + 1)$.
b. Using the result of part a, find gcd (301, 201) and gcd (121, 81).

Exercises

2.16 Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.

a. 4 and 7

b. 291 and 42

c. 84 and 320

d. 400 and 60

2.17 Find the results of the following operations.

a. 22 mod 7

b. 140 mod 10

c. –78 mod 13

d. 0 mod 15

2.18 Perform the following operations using reduction first.

a. (273 + 147) mod 10

b. (4223 + 17323) mod 10

c. (148 + 14432) mod 12

d. (2467 + 461) mod 12

2.19 Perform the following operations using reduction first.

a. (125 × 45) mod 10

b. (424 × 32) mod 10

c. (144 × 34) mod 12

d. (221 × 23) mod 22

Exercises

2.20 Use the properties of the mod operator to prove the following:

a. The remainder of any integer when divided by 10 is the rightmost digit.

b. The remainder of any integer when divided by 100 is the integer made of the two rightmost digits.

c. The remainder of any integer when divided by 1000 is the integer made of the three rightmost digits.

2.21 We have been told in arithmetic that the remainder of an integer divided by 5 is the same as the remainder of division of the rightmost digit by 5. Use the properties of the mod operator to prove this claim.

2.22 We have been told in arithmetic that the remainder of an integer divided by 2 is the same as the remainder of division of the rightmost digit by 2. Use the properties of the mod operator to prove this claim.

2.23 We have been told in arithmetic that the remainder of an integer divided by 4 is the same as the remainder of division of the two rightmost digits by 4. Use the properties of the mod operator to prove this claim.

2.24 We have been told in arithmetic that the remainder of an integer divided by 8 is the same as the remainder of division of the rightmost three digits by 8. Use the properties of the mod operator to prove this claim.

2.25 We have been told in arithmetic that the remainder of an integer divided by 9 is the same as the remainder of division of the sum of its decimal digits by 9. In other words, the remainder of dividing 6371 by 9 is the same as dividing 17 by 9 because $6 + 3 + 7 + 1 = 17$. Use the properties of the mod operator to prove this claim.

Exercises

2.26 The following shows the remainders of powers of 10 when divided by 7. We can prove that the pattern will be repeated for higher powers.

$10^0 \bmod 7 = 1$ $10^1 \bmod 7 = 3$ $10^2 \bmod 7 = 2$

$10^3 \bmod 7 = -1$ $10^4 \bmod 7 = -3$ $10^5 \bmod 7 = -2$

Using the above information, find the remainder of an integer when divided by 7. Test your method with 631453672.

2.27 The following shows the remainders of powers of 10 when divided by 11. We can prove that the pattern will be repeated for higher powers.

$10^0 \bmod 11 = 1$ $10^1 \bmod 11 = -1$ $10^2 \bmod 11 = 1$ $10^3 \bmod 11 = -1$

Using the above information, find the remainder of an integer when divided by 11. Test your method with 631453672.

2.28 The following shows the remainders of powers of 10 when divided by 13. We can prove that the pattern will be repeated for higher powers.

$10^0 \bmod 13 = 1$ $10^1 \bmod 13 = -3$ $10^2 \bmod 13 = -4$

$10^3 \bmod 13 = -1$ $10^4 \bmod 13 = 3$ $10^5 \bmod 13 = 4$

Using the above information, find the remainder of an integer when divided by 13. Test your method with 631453672.

Exercises

2.29 Let us assign numeric values to the uppercase alphabet (A = 0, B = 1, . . . Z = 25). We can now do modular arithmetic on the system using modulo 26.

a. What is (A + N) mod 26 in this system?
b. What is (A + 6) mod 26 in this system?
c. What is (Y – 5) mod 26 in this system?
d. What is (C –10) mod 26 in this system?

2.30 List all additive inverse pairs in modulus 20.

2.31 List all multiplicative inverse pairs in modulus 20.

2.32 Find the multiplicative inverse of each of the following integers in $\mathbf{Z}_{180}$ using the extended Euclidean algorithm.

a. 38
b. 7
c. 132
d. 24

2.33 Find the particular and the general solutions to the following linear Diophantine equations.

a. $25x + 10y = 15$
b. $19x + 13y = 20$
c. $14x + 21y = 77$
d. $40x + 16y = 88$

2.34 Show that there are no solutions to the following linear Diophantine equations:

a. $15x + 12y = 13$
b. $18x + 30y = 20$
c. $15x + 25y = 69$
d. $40x + 30y = 98$

Exercises

2.35 A post office sells only 39-cent and 15-cent stamps. Find the number of stamps a customer needs to buy to put \$2.70 postage on a package. Find a few solutions.

2.36 Find all solutions to each of the following linear equations:

a. $3x \equiv 4 \pmod 5$

b. $4x \equiv 4 \pmod 6$

c. $9x \equiv 12 \pmod 7$

d. $256x \equiv 442 \pmod{60}$

2.37 Find all solutions to each of the following linear equations:

a. $3x + 5 \equiv 4 \pmod 5$

b. $4x + 6 \equiv 4 \pmod 6$

c. $9x + 4 \equiv 12 \pmod 7$

d. $232x + 42 \equiv 248 \pmod{50}$

2.38 Find $(\mathbf{A} \times \mathbf{B}) \bmod 16$ using the matrices in Fig. 2.28.

$$\underset{\mathbf{A}}{\begin{bmatrix} 3 & 7 & 10 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}} \qquad \underset{\mathbf{A}}{\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 5 & 2 & 4 \end{bmatrix}}$$

Fig. 2.28 *Matrices for Exercise 38*

Exercises

2.39 In Fig. 2.29, find the determinant and the multiplicative inverse of each residue matrix over $\mathbf{Z}_{10}$.

$$\mathbf{A} = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix} \qquad \mathbf{C} = \begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}$$

Fig. 2.29 *Matrices for Exercise 39*

2.40 Find all solutions to the following sets of linear equations:

a. $3x + 5y \equiv 4 \pmod 5$
$2x + y \equiv 3 \pmod 5$

b. $3x + 2y \equiv 5 \pmod 7$
$4x + 6y \equiv 4 \pmod 7$

c. $7x + 3y \equiv 3 \pmod 7$
$4x + 2y \equiv 5 \pmod 7$

d. $2x + 3y \equiv 5 \pmod 8$
$x + 6y \equiv 3 \pmod 8$

Exercises

3.11 A small private club has only 100 members. Answer the following questions:

a. How many secret keys are needed if all members of the club need to send secret messages to each other?

b. How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.

c. How many secret keys are needed if the president decides that the two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.

3.12 Some archeologists found a new script written in an unknown language. The archeologists later found a small tablet at the same place that contains a sentence in the same language with the translation in Greek. Using the tablet, they were able to read the original script. What type of attack did the archeologists use?

3.13 Alice can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message two times, each time with a different key. Is she right? Defend you answer.

Exercises

3.14 Alice has a long message to send. She is using the monoalphabetic substitution cipher. She thinks that if she compresses the message, it may protect the text from single-letter frequency attack by Eve. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend your answer.

3.15 Alice often needs to encipher plaintext made of both letters (a to z) and digits (0 to 9).

a. If she uses an additive cipher, what is the key domain? What is the modulus?

b. If she uses a multiplication cipher, what is the key domain? What is the modulus?

c. If she uses an affine cipher, what is the key domain? What is the modules?

3.16 Suppose that spaces, periods, and question marks are added to the plaintext to increase the key domain of simple ciphers.

a. What is the key domain if an additive cipher is used?

b. What is the key domain if a multiplicative cipher is used?

c. What is the key domain if an affine cipher is used?

Exercises

3.17 Alice and Bob have decided to ignore Kerckhoff's principle and hide the type of the cipher they are using.

a. How can Eve decide whether a substitution or a transposition cipher was used?

b. If Eve knows that the cipher is a substitution cipher, how can she decide whether it was an additive, multiplicative, or affine cipher?

c. If Eve knows that the cipher is a transposition, how can she find the size of the section (m)?

3.18 In each of the following ciphers, what is the maximum number of characters that will be changed in the ciphertext if only a single character is changed in the plaintext?

a. Additive

b. Multiplicative

c. Affine

d. Vigenere

e. Auto-key

f. One-time pad

g. Rotor

h. Enigma

Exercises

3.19 In each of the following ciphers, what is the maximum number of characters that will be changed in the ciphertext if only one character is changed in plaintext?

a. Single transposition
b. Double transposition
c. Playfair

3.20 For each of the following ciphers, say whether it is a stream cipher or block cipher. Defend your answers.

a. Playfair
b. Auto-key
c. One-time pad
d. Rotor
e. Enigma

3.21 Encrypt the message "this is an exercise" using one of the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.

a. Additive cipher with key = 20
b. Multiplicative cipher with key = 15
c. Affine cipher with key = (15, 20)

Exercises

3.22 Encrypt the message "the house is being sold tonight" using one of the following ciphers. Ignore the space between words. Decrypt the message to get the plaintext:

a. Vigenere cipher with key: "dollars"

b. Autokey cipher with key = 7

c. Playfair cipher with the key created in the text (see Fig. 3.13)

3.23 Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is full of surprises".

3.24 Use the Playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.

3.25 Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key:

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

Exercises

3.26 John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is a shift cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a cave with "XVIEWYWI" engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here? What is the plaintext?

3.27 Eve secretly gets access to Alice's computer and using her cipher types "abcdefghij". The screen shows "CABDEHFGIJ". If Eve knows that Alice is using a keyed transposition cipher, answer the following questions:

a. What type of attack is Eve launching?

b. What is the size of the permutation key?

3.28 Use a brute-force attack to decipher the following message enciphered by Alice using an additive cipher. Suppose that Alice always uses a key that is close to her birthday, which is on the 13th of the month:

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

Exercises

3.29 Use a brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plaintext "ab" is enciphered to "GL".

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

3.30 Use a one-letter frequency attack to decipher the following message. Assume that you know it is enciphered using monoalphabetic substitution cipher.

ONHOVEJHWOBEVGWOCBWHNUGBLHGBGR

3.31 Assume that punctuation marks (periods, question marks, and spaces) are added to the encryption alphabet of a Hill cipher, then a 2×2 key matrix in Z_{29} can be used for encryption and decryption.

a. Find the total number of possible matrices.

b. It has been proved that the total number of invertible matrices is $(N^2 - 1)(N^2 - N)$, where N is the number of alphabet size. Find the key domain of a Hill cipher using this alphabet.

Exercises

3.32 Use a single-letter frequency attack to break the following ciphertext. You know that it has been created with an additive cipher

OTWEWNGWCBPQABIZVQAPMLJGZWTTQVOBQUMAPMIDGZCAB
EQVBMZLZIXMLAXZQVOQVLMMXAVWEIVLLIZSNZWAB
JQZLWNLMTQOPBVIUMLGWCBPAEQNBTGTMNBBPMVMAB
ITIAKWCTLVBBQUMQBEPQTMQBEIAQVUGBZCAB

3.33 Use a Kasiski test and single-frequency attack to break the following ciphertext. You know that it has been created with a Vigenere cipher

MPYIGOBSRMIDBSYRDIKATXAILFDFKXTPPSNTTJIGTHDELT
TXAIREIHSVOBSMLUCFIOEPZIWACRFXICUVXVTOPXDLWPENDHPTSI
DDBXWWTZPHNSOCLOUMSNRCCVUUXZHHNWSVXAUHIK
LXTIMOICHTYPBHMHXGXHOLWPEWWWWDALOCTSQZELT

3.34 The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key.

Exercises

3.35 Show the matrix representation of the transposition-cipher encryption key with the key (3, 2, 6, 1, 5, 4). Find the matrix representation of the decryption key.

3.36 The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFNOPIKLB" are given. You know that the algorithm is a Hill cipher, but you don't know the size of the key. Find the key matrix.

3.37 Hill ciphers and multiplicative ciphers are very similar. Hill ciphers are block ciphers using multiplication of matrices; multiplicative ciphers are stream ciphers using multiplication of scalars.

a. Define a block cipher that is similar to an additive cipher using the addition of matrices.

b. Define a block cipher that is similar to an affine cipher using the multiplication and addition of matrices.

3.38 Let us define a new stream cipher. The cipher is affine, but the keys depend on the position of the character in the plaintext. If the plaintext character to be encrypted is in position i, we can find the keys as follow:

a. The multiplicative key is the (i mod 12)th element in $\mathbf{Z}_{26}^*$.

b. The additive key is the (i mod 26)th element in $\mathbf{Z}_{26}$.

Exercises

3.39 Suppose that for a Hill cipher, the plaintext is a multiplicative identity matrix (**I**). Find the relationship between the key and ciphertext. Use the result of your finding to launch a chosen-plaintext attack on the Hill cipher.

3.40 Atbash was a popular cipher among Biblical writers. In Atbash, "A" is encrypted as "Z", "B" is encrypted as "Y", and so on. Similarly, "Z" is encrypted as "A", "Y" is encrypted as "B", and so on. Suppose that the alphabet is divided into two halves and the letters in the first half are encrypted as the letters in the second and vice versa. Find the type of cipher and key. Encipher the message "an exercise" using the Atbash cipher.

3.41 In a Polybius cipher, each letter is enciphered as two integers. The key is a 5×5 matrix of characters as in a Playfair cipher. The plaintext is the character in the matrix, the ciphertext is the two integers (each between 1 and 5) representing row and column numbers. Encipher the message "An exercise" using the Polybius cipher with the following key:

	1	2	3	4	5
1	z	q	p	f	e
2	y	r	o	g	d
3	x	s	n	h	c
4	w	t	m	i / j	b
5	v	u	l	k	a

Exercises

5.13 A transposition block has 10 inputs and 10 outputs. What is the order of the permutation group? What is the key size?

5.14 A substitution block has 10 inputs and 10 outputs. What is the order of the permutation group? What is the key size?

5.15
a. Show the result of 3-bit circular left shift on word $(10011011)_2$.
b. Show the result of 3-bit circular right shift on the word resulting from Part a.
c. Compare the result of Part b with the original word in Part a.

5.16
a. Swap the word $(10011011)_2$.
b. Swap the word resulting from Part a.
c. Compare the result of Part a and Part b to show that swapping is a self-invertible operation.

5.17 Find the result of the following operations:

a. $(01001101) \oplus (01001101)$
b. $(01001101) \oplus (10110010)$
c. $(01001101) \oplus (00000000)$
d. $(01001101) \oplus (11111111)$

Exercises

5.18 a. Decode the word 010 using a 3×8 decoder.

b. Encode the word 00100000 using a 8×3 encoder.

5.19 A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits size of the padding and the number of blocks.

5.20 Show the table for the straight D-box in Fig. 5.4.

5.21 Show the table for the compression D-box in Fig. 5.4.

5.22 Show the table for the expansion D-box in Fig. 5.4.

5.23 Show the D-box defined by the following table:

8	1	2	3	4	5	6	7

5.24 Determine whether the D-box with the following table is a straight D-box, a compression D-box expansion D-box.

1	1	2	3	4	4

5.25 Determine whether the D-box with the following table is a straight D-box, a compression D-box, or an expansion D-box.

1	3	5	6	7

Exercises

5.26 Determine whether the D-box with the following permutation table is a straight D-box, a compression D-box, or an expansion D-box.

1	2	3	4	5	6

5.27 The input/output relation in a 2×2 S-box is shown by the following table. Show the table for the inverse S-box.

		Input: right bit	
		0	1
Input: left bit	0	01	11
	1	10	00

5.31 The maximum period length of an LFSR is 32. How many bits does the shift register have?

5.32 A 6×2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusive-ors the even-numbered bits to get the right bit of the output. If the input is 110010, what is the output? If the input is 101101, what is the output?

5.33 The leftmost bit of a 4×3 S-box rotates the other three bits. If the leftmost bit is 0, the three other bits are rotated to the right one bit. If the leftmost bit is 1, the three other bits are rotated to the left one bit. If the input is 1011, what is the output? If the input is 0110, what is the output?