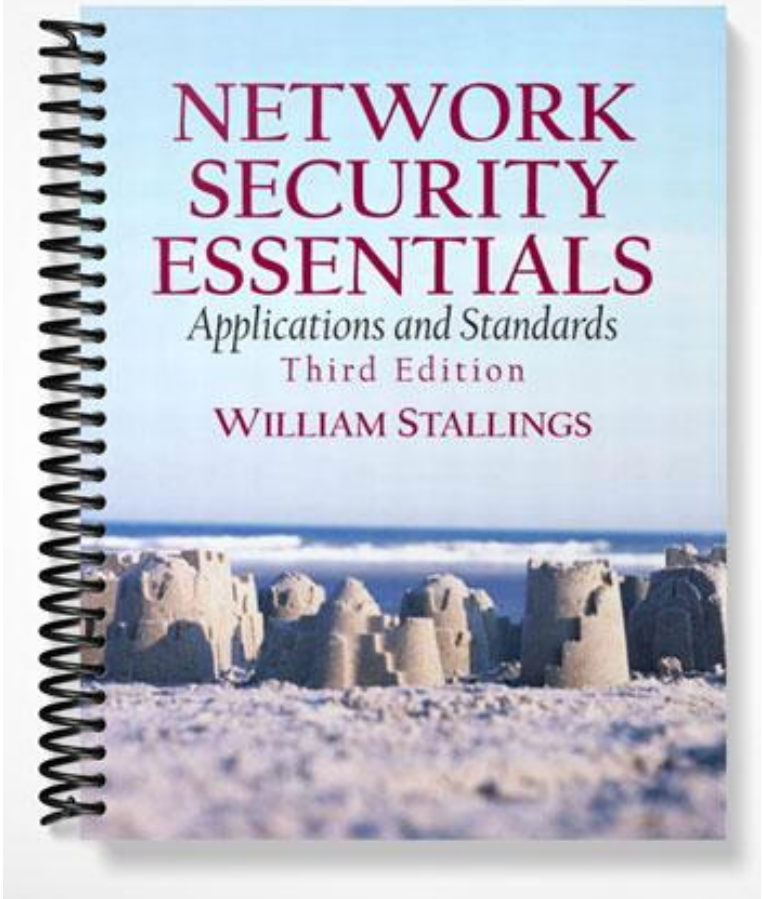
SOLUTIONS MANUAL



SOLUTIONS MANUAL

NETWORK SECURITY ESSENTIALS
THIRD EDITION

WILLIAM STALLINGS

NOTICE

This manual contains solutions to all of the review questions and homework problems in *Network Security Essentials, Third Edition*. If you spot an error in a solution or in the wording of a problem, I would greatly appreciate it if you would forward the information via email to ws@shore.net. An errata sheet for this manual, if needed, is available at ftp://shell.shore.net/members/w/s/ws/S.

W.S.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

ANSWERS TO QUESTIONS

1.1 The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

1.2 **Passive attacks** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active attacks** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

1.3 **Passive attacks:** release of message contents and traffic analysis. **Active attacks:** masquerade, replay, modification of messages, and denial of service.

1.4 **Authentication:** The assurance that the communicating entity is the one that it claims to be.
Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
Data confidentiality: The protection of data from unauthorized disclosure.
Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

1.5 See Table 1.3.

Answers to Problems

1.1	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

1.2	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

CHAPTER 2
SYMMETRIC ENCRYPTION AND MESSAGE CONFIDENTIALITY

ANSWERS TO QUESTIONS

2.1 Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

2.2 Permutation and substitution.

2.3 One secret key.

2.4 A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

2.5 Cryptanalysis and brute force.

2.6 In some modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

2.7 With triple encryption, a plaintext block is encrypted by passing it through an encryption algorithm; the result is then passed through the same encryption algorithm again; the result of the second encryption is passed through the same encryption algorithm a third time. Typically, the second stage uses the decryption algorithm rather than the encryption algorithm.

2.8 There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

2.9 With **link encryption**, each vulnerable communications link is equipped on both ends with an encryption device. With **end-to-end encryption**, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data; the data in encrypted form are then transmitted unaltered across the network to the destination terminal or host.

2.10 For two parties A and B, key distribution can be achieved in a number of ways, as follows:

1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.