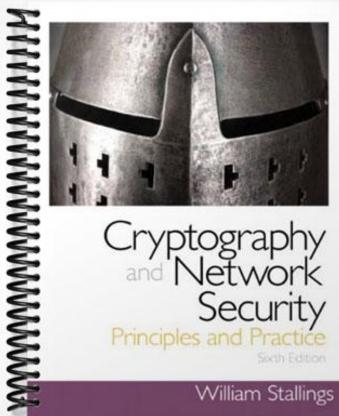
TEST BANK

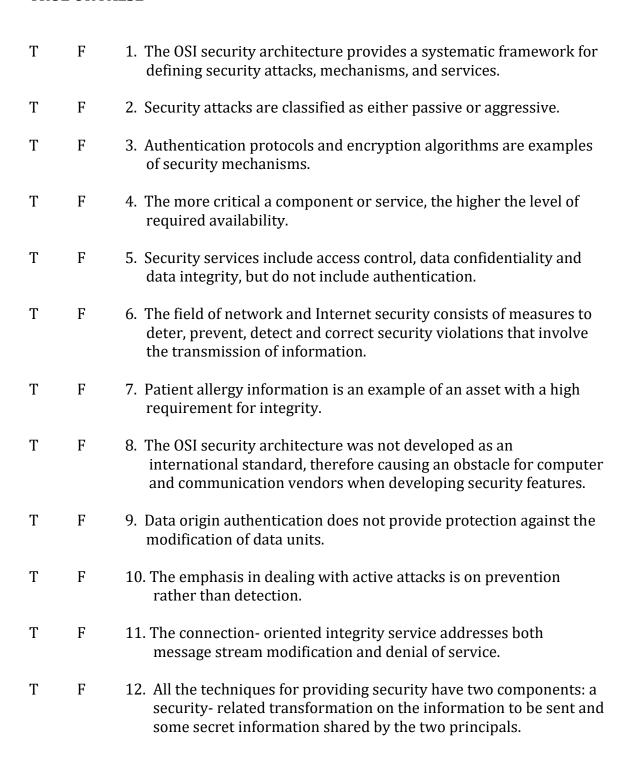


Cryptography
and Network
Security Principles and Practice

William Stallings

CHAPTER 1: OVERVIEW

TRUE OR FALSE



Т		F	13. Information access threats intercept or modify data on behalf of users who should not have access to that data.		
Т		F	14. The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts.		
Т		F	15. Symmetric encryption is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.		
ΜĮ	JLT	IPLE C	НОІСЕ		
	1.		is the most common method uses encryption keys and hash function ures.		
			A) Symmetric encryption	B) Data integrity algorithms	
			C) Asymmetric encryption	D) Authentication protocols	
2. A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the messa				_	
			A) integrity	B) encryption	
			C) analysis	D) masquerade	
3 involves the passive capture of a data unit and retransmission to produce an unauthorized effect.				_	
			A) Disruption	B) Replay	
			C) Service denial	D) Masquerade	

Cryptography and Network Security: Principles and Practice, 6^{th} Edition, by William Stallings

Cryptography and Network Security: Principles and Practice, 6^{th} Edition, by William Stallings

4.	The three concepts that form what is often referred to as the CIA triad are These three concepts embody the fundamental security objectives for both data and for information and computing services.						
	A) confidentiality, integrity and availability						
	B) communication, integrity and authentication C) confidentiality, integrity, access control						
	D) communication, information and authenticity						
5.	A loss of is the unauthor	rized disclosure of information.					
	A) authenticity	B) confidentiality					
	C) reliability	D) integrity					
6.	. Verifying that users are who they say they are and that each input arriving the system came from a trusted source is						
	A) authenticity	B) credibility					
	C) accountability	D) integrity					
7. A level breach of security could cause a significant degra mission capability to an extent and duration that the organization perform its primary functions, but the effectiveness of the function significantly reduced.		nd duration that the organization is able to					
	A) catastrophic	B) moderate					
	C) low	D) high					
8.	A is any action that compromises the security of information owned by an organization.						
	A) security attack	B) security service					
	C) security alert	D) security mechanism					

Cryptography and Network Security: Principles and Practice, 6th Edition, by William Stallings

9. A takes place when one entity pretends to be a different e		ntity pretends to be a different entity.	
		A) replay	B) masquerade
		C) service denial	D) passive attack
10 is the protection of transmi		is the protection of trans	smitted data from passive attacks.
		A) Access control	B) Data control
		C) Nonrepudiation	D) Confidentiality
11. A(n) service is one that protects a system to ensure its availabil and addresses the security concerns raised by denial- of- service attacks.			
		A) replay	B) availability
		C) masquerade	D) integrity
12 threats exploit service flaws in computers to inhibit use by legitimate users.		aws in computers to inhibit use by	
		A) Information access	B) Reliability
		C) Passive	D) Service
13. A(n) is a potential for violation of security, which exis a circumstance, capability, action or event that could bread cause harm.			
		A) threat	B) attack
		C) risk	D) attack vector
14.	_	rotection of the information t flows is	chat might be derived from observation of
	A) con	nectionless confidentiality	B) connection confidentiality
	C) trai	ffic- flow confidentiality	D) selective- field confidentiality

Cryptography and Network Security: Principles and Practice, 6th Edition, by William Stallings

15. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery is a(n)			
A) security audit trail	B) digital signature		
C) encipherment	D) authentication exchange		
SHORT ANSWER			
1. A is any process, or a device incorp designed to detect, prevent, or recover from a seencryption algorithms, digital signatures and au	ecurity attack. Examples are		
2. An attack attempts to alter system r	resources or affect their operation.		
3. "The protection afforded to an automated inf the applicable objectives of preserving the integ of information system resources" is the definition	rity, availability and confidentiality		
4. A loss of is the disruption of access to information system.	to or use of information or an		
5. Irreversible mechanisms include ha authentication codes, which are used in digital sauthentication applications.			
6. In the United States, the release of student gr	rade information is regulated by the		
7. A loss of is the unauthorized modific	ation or destruction of information.		
8. A attack attempts to learn or make u but does not affect system resources.	se of information from the system		
9. The service is concerned with assur from the source that it claims to be from. This seconnection is not interfered with in such a way one of the two legitimate parties for the purpose reception.	ervice must also assure that the that a third party can masquerade as		

Cryptography and Network Security: Principles and Practice, 6^{th} Edition, by William Stallings				
10. Two specific authentication services defined in X.800 are peer entity authentication and authentication.				
11. In the context of network security, is the ability to limit and control the access to host systems and applications via communications links.				
12 prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message and when a message is received, the sender can prove that the alleged receiver in fact received the message.				
13. Viruses and worms are two examples of attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network.				
14. An is an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.				
15 is the use of a trusted third party to assure certain properties of a data exchange.				