STELLA MARIS COLLEGE (AUTONOMOUS), CHENNAI - 600 086
(For candidates admitted during the academic year 2023 – 2024)

B. C. A. DEGREE EXAMINATION, APRIL 2026
SIXTH SEMESTER

COURSE : MAJOR CORE
PAPER : SECURITY CONCEPTS
SUBJECT CODE : 23CS/MC/SC65
TIME : 3 HOURS **MAX. MARKS: 100**

Q. No.	SECTION A (20 x 1 =20 marks)	CO	KL
1) i.	A _____ is a malicious program that appears legitimate but performs hidden harmful actions.	CO1	K1
ii)	In stack smashing, the attacker typically overwrites the saved _____ and return address.		
iii)	The _____ protocol consists of a series of messages exchanged by client and server.		
iv)	————is a DoS attack where an attacker sends a large number of UDP packets to a random port on a target system.		
v)	Several file names associated with a single inode is called a _____ link.		
vi)	_____SSL is a general-purpose service implemented as a set of protocols that rely on TCP.		
vii)	_____ access control allows users to grant permission to specific other user IDs to access their files.		
viii)	A digital signature is created by encrypting the message digest using the sender's _____ key.		
ix)	_____ access control allows users to grant permission to specific other user IDs to access their files.		
x)	The hashed-password method has the advantage that passwords are not stored in _____.		

...2

2) i.	A firewall is primarily used to _____ A. generate passwords B. filter traffic between networks C. encrypt messages D. replace antivirus	CO2	K2
ii.	_____ function in C is unsafe because it does not check input length. A. fgets() B. gets() C. strncpy() D. scanf()		
iii.	The main purpose of spyware is to _____ A. replicate itself across networks B. secretly collect user information C. block network traffic D. overwrite the return address		
iv.	_____ is used to manage and diagnose the network. A. UDP B. ICMP C. DoS D. RBAC		
v.	Traditional UNIX access control is an example of _____ A. MAC B. DAC C. RBAC D. ABAC		
vi.	A trusted third-party authority responsible for issuing public key certificate is called _____. A. service provider B. administrator C. certificate authority D. key user		
vii.	_____algorithm uses a 128-bit block size and key sizes of 128/192/256 bits. A. DES B. 3DES C. AES D. RSA		
viii.	The CIA triad consists of_____ A) confidentiality, integrity, availability B) control, inspection, access C) confidentiality, inspection, authorization D) control, integrity, authentication		
ix.	_____ cipher uses a 5×5 matrix of letters. A) Caesar B) Playfair C) DES D) AES		
x.	Salt is used in password hashing to _____ A) encrypt passwords B) increase storage size C) prevent dictionary attacks D) compress passwords		

Q. No.	SECTION B (4 x 5 =20 marks)	CO	KL
3	Apply the CIA triad with suitable real-world examples and explain. **(OR)** Apply the working of SSL/TLS protocol and its role in securing Internet communication.	CO3	K3
4	Show how a buffer overflow attack occurs with a suitable example. **(OR)** Make use of a suitable scenario and explain how phishing attack works.	CO3	K3
5	Analyse how different security threats and vulnerabilities impact system assets **(OR)** Analyse the concept of access control and describe the differences between Discretionary Access Control (DAC) and Role-Based Access Control (RBAC).	CO4	K4
6	Analyse how a SQL injection attack manipulates application input to alter database queries. Illustrate with a suitable example. **(OR)** Compare the different methods of Message Authentication using one way hash function with appropriate diagrams.	CO4	K4
Q. No.	**SECTION C (5 x 12 = 60marks)**	**CO**	**KL**
7	Recall the concepts of Caesar Cipher and Playfair Cipher and outline their working with appropriate examples. **(OR)** Define packet filtering firewall. List the packet header fields used in filtering rules and state how they are used to allow or deny network traffic.	CO1	K1
8	Interpret how malware, virus and worms impact on computer systems. **(OR)** Explain the history and components of a Symmetric Encryption System with a neat diagram.	CO2	K2
9	Apply suitable authentication techniques for securing an online banking system and justify your selection. **(OR)** Use appropriate cryptographic techniques to secure data transmission in an online banking system. Justify.	CO3	K3
10	Examine the effectiveness of different firewall types in protecting a network from cyber threats. **(OR)** Analyse the causes and consequences of buffer overflow attacks and recommend appropriate prevention techniques.	CO4	K4
11	Explain a secure communication model using SSL/TLS and HTTPS protocols for an e-commerce application. **(OR)** Assess how user authentication is achieved through token-based authentication and biometric authentication.	CO5	K5

****