

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 90455

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2025.

Fifth/Sixth Semester

Computer Science and Engineering

CCS 354 – NETWORK SECURITY

(Common to Computer Science and Engineering (Artificial Intelligence and Machine Learning)/Computer and Communication Engineering/
Artificial Intelligence and Data Science/Information Technology)

(Regulations 2021)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Outline a hash function with an example.
2. Define authentication.
3. What is a public key?
4. Write a note on Kerberos.
5. Outline the need for access control.
6. What is secure sockets layer protocol?
7. Write a note on pretty good privacy.
8. What is DomainKeys Identified Mail?
9. Define an intrusion detection system.
10. What is a block chain?

PART B — (5 × 13 = 65 marks)

11. (a) Present an outline of the basic principles of public-key cryptosystems.

Or

- (b) What is digital signature? How does digital signature encryption work?
Outline with a diagram and an example.

12. (a) Outline X.509 authentication service with a diagram.

Or

- (b) Outline symmetric encryption and asymmetric encryption with an example.

13. (a) What is IP security? Why IP security is important? How does IP security work? Outline with an example.

Or

- (b) What is Web security? How the Web can be secured? Outline.

14. (a) What is S/MIME? How does S/MIME work? Outline.

Or

- (b) How to ensure mobile devices remain secure and prevent unauthorized access to corporate data? Outline.

15. (a) What is a firewall? Outline the types of firewalls.

Or

- (b) Present an outline of Cloud Security and IoT security.

PART C — (1 × 15 = 15 marks)

16. (a) Present a framework for a secure public-key cryptosystem.

Or

- (b) Present a framework for an intrusion detection system.