(2 Hours) **Total Marks: 50**

Note:
- **Question number Q1 is compulsory**
- **Attempt any two questions out of Q2 to Q5**

			Marks	Course Outcome CO	Bloom's Level BL
Q1	**Answer the following**				
	a.	Discuss various security services defined in information security.	**[05]**	CO1	BL2
	b.	Explain any two operating system tools that can be used to implement security functions	**[05]**	CO4	BL2
	c.	Find the Greatest Common Divisor (GCD) of the numbers 285 and 741 using the Euclidean algorithm.	**[05]**	CO2	BL4
	d.	What is Firewall?	**[05]**	CO3	BL2
Q2	**a.**	Evaluate the concept of mutual authentication and explain how reflection attacks can compromise it. How can such attacks be prevented?	**[08]**	CO2	BL4
	b.	Explain the approaches used for intrusion detection, focusing on statistical anomaly detection and rule-based detection.	**[07]**	CO3	BL2
Q3	**a.**	Explain the concept of database access control.	**[08]**	CO4	BL2
	b.	Analyze and compare MD5 and SHA-512 in terms of structure, strength, and vulnerability to attacks	**[07]**	CO2	BL4
Q4	**a.**	Explain the working of IPsec in ensuring secure communication over the Internet.	**[08]**	CO3	BL2
	b.	Break down the digital certificate creation process.	**[07]**	CO2	BL4
Q5	**a.**	Break down the steps involved in RSA encryption and decryption. In an RSA system, the public key of a given user is e = 103, n = 143. What is the private key?	**[08]**	CO2	BL4
	b.	Describe how PGP provide email security.	**[07]**	CO3	BL2

****