

5 Years Integrated MCA, Utkal University

End Semester Examination, March 2021

Semester: 9<sup>th</sup>  
Full Mark:70

Sub: IS (9.4)  
Time: 3Hours

Answer all Questions

1	a)	Write short note on active attack.	4
	b)	Discuss the different security services in detail.	7
	c)	Using playfair cipher, convert the Plain text “Hide Money” to Cipher text with the key “TUTORIALS”.	3
		OR	
	d)	Discuss the process of AES in detail.	11
	e)	Explain the process of key discarding process of DES.	3
2	a)	What is asymmetric key cryptography? Discuss the RSA algorithm in detail with a suitable example.	7
	b)	What is MAC.? How it is different from message digest.	7
		OR	
	c)	Write short note on digital signature.	7
	d)	What is message digest? Explain the MD5 message digest algorithm in detail.	7
3	a)	What is PGP? What are the cryptographic functions supported by PGP. Discuss the working mechanism	10
	b)	Describe VPN.	4
		OR	
	c)	What is SMTP? Why SMTP can't work with non-text data. Explain the working mechanism of SMTP.	7
	d)	Discuss the detail processes of S/MIME.	7
4		Discuss the SET process in detail along with the list of participants. How does the SET protect the payment information from merchant?	14
		OR	
		What is SSL? Discuss the handshake protocol in detail.	14

5	a)	What is firewall? Explain the different types of firewall with the limitations of firewall.	10
	b)	Write short note on network address translation.	4
		OR	
	c)	Discuss the different modes of operations and components of ESP.	10
	d)	What is security association? How it is established in IPsec.	4