	Enrollment No:		Exam Seat No:		_		
	(C.U.SHAH I	UNIVERSITY				
	Winter Examination-2018 Subject Name: Cryptography and Network Security						
	Subject Code: 4TE06CNS1		Branch: B.Tech (CE)				
	Semester: 6	Date: 24/10/2018	Time: 02:30 To 05:30	Marks: 70			
	Instructions: Use of Programmable calculator & any other electronic instrument is prohibited. Instructions written on main answer book are strictly to be obeyed. Draw neat diagrams and figures (if necessary) at right places. Assume suitable data if needed. 						
Q-1	 a) What are th b) Define Sect c) List out Pas d) Write differ e) What is Ave f) What are th g) Define Hash h) What type of i) Define Viru j) What is med k) List Transport l) How many 	sive Attack. ence between Symmetricalanche Effect? e different modes of Open Function. of information can be sects. ant by Intruder? osition Techniques. Keys are used in 3DES? receive data as "aby" and anograhy.	c key and Asymmetric Key.		(14)		
Q-2	a) Explain Net	questions work Security Model wi yfair with suitable examp	<u>-</u>		(14) (07) (07)		
Q-3	a) Explain RS keys and ge	_	_	nd private	(14) (07) (07)		
Q-4	a) Write Eucli	d's algorithm and give su	uitable example. Ciphers that follow Feistel Struc	cture.	(14) (07) (07)		



Q-5		Attempt all questions	(14)
	a)	Write the digital signature standard algorithm.	(07)
	b)	Explain diffie Hellman key exchange algorithm with suitable examples.	(07)
Q-6		Attempt all questions	(14)
	a)	Explain SHA1 algorithm.	(07)
	b)	What is Transport mode and Tunnel mode? Explain about the scope of AH and ESP in these modes?	(07)
		ESF in these modes?	
Q-7		Attempt all questions	(14)
	a)	Write about Kerberos and x.509 authentication services.	(07)
	b)	Explain the four protocols defined by Secure Socket Layer.	(07)
Q-8		Attempt all questions	(14)
-	a)	Explain Data Encryption Standard with diagram.	(07)
	b)	What is Firewall? Explain different types of firewall.	(07)

