Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2019

Course: Network Security and Cryptography **Semester: VI**
Program: B.Tech CS with Cyber Law **Time 03 hrs.**
Course Code: CSEG 423 **Max. Marks: 100**
Instructions: Answer ALL the Questions

SECTION A

S. No.		**Marks**	**CO**
Q 1	Differentiate between Active attacks and Passive Attacks	**4**	**CO2**
Q 2	Mention the strengths and weakness of DES algorithm	**4**	**CO1,CO4**
Q 3	What is Kerberos? What are the uses?	**4**	**CO2**
Q 4	Use the Vigenere cipher with keyword “HEALTH” to encipher the message “LIFE IS FULL OF SURPRISES”	**4**	**CO1**
Q 5	List the properties of hashing functions?	**4**	**CO2**

SECTION B

Q 6	List the four tasks that are performed in each round of AES Cipher? Explain	**10**	**CO4**
Q 7	Explain in detail Feistel Block Cipher structure with neat sketch.	**10**	**CO1**
Q 8	Explain the Bell-Lapadula (BLP) and Harrison-Ruzzo-Ullman (HRU) model	**10**	**CO5**
Q 9	Briefly, explain Encapsulating IP Security Payload? Or Explain about the trust mechanism and certificates used by PGP and S/MIME	**10**	**CO3**

SECTION-C

Q 10	Explain the authentication procedures defined by X.509 certificate. Illustrate the concept of ‘certificate chain’ for verification of digital signature on X.509 certificate. What are the main features of Kerberos Version 5? Or Briefly, explain the different message authentication functions with neat diagrams?	**20**	**CO3**
Q 11	i) In a medical information system that controls access to patient records and prescriptions: • doctors may read and write patient records and prescriptions; • Nurses may read and write prescriptions only but should learn nothing about the contents of patient records. How can you capture this policy in a lattice model that prevents information flow from patient records to prescriptions? In your opinion, which security model is most appropriate for this policy? ii) Apply the RSA algorithm, for given e=13 and n=100 encrypt and decrypt the message “HOW ARE YOU” using 00 to 25 for letters A to Z and 26 for space.	**10+10**	**CO5, CO2**

Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: Network Security and Cryptography **Semester: VI**
Program: B.Tech CS with Cyber Law **Time 03 hrs.**
Course Code: CSEG 423 **Max. Marks: 100**

Instructions: Answer ALL the Questions

S. No.		Marks	CO
	SECTION A		
Q 1	List and briefly define categories of passive and active security attacks.	**4**	**CO2**
Q 2	Distinguish between mono alphabetic and poly alphabetic cipher?	**4**	**CO3, CO1**
Q 3	Distinguish between message integrity and message authentication	**4**	**CO2**
Q 4	Use the Vigenere cipher with keyword “WEALTH” to encipher the message “LIFE IS FULL OF SURPRISES”	**4**	**CO1**
Q 5	What are the requirements of the cryptographic hash functions?	**4**	**CO2**
	SECTION B		
Q 6	Explain in detail Feistel Block Cipher structure with neat sketch.	**10**	**CO1**
Q 7	Discuss any four Substitution Technique and list their merits and demerits.	**10**	**CO1**
Q 8	Illustrate in detail about the message authentication code and its requirements.	**10**	**CO2**
Q 9	Briefly, explain Encapsulating IP Security Payload? Or Explain about the trust mechanism and certificates used by PGP and S/MIME	**10**	**CO3**
	SECTION-C		
Q 10	Explain the authentication procedures defined by X.509 certificate. Illustrate the concept of ‘certificate chain’ for verification of digital signature on X.509 certificate. What are the main features of Kerberos Version 5? Or Briefly, explain the different message authentication functions with neat diagrams?	**20**	**CO3**
Q 11	i)In a medical information system that controls access to patient records and prescriptions: • doctors may read and write patient records and prescriptions; • Nurses may read and write prescriptions only but should learn nothing about the contents of patient records. How can you capture this policy in a lattice model that prevents information flow from patient records to prescriptions? In your opinion, which security model is most appropriate for this policy? ii)Apply the RSA algorithm, for given e=13 and n=100 encrypt and decrypt the message “HOW ARE YOU” using 00 to 25 for letters A to Z and 26 for space.	**10+10**	**CO5, CO2**