


<b>Name:</b>	 <b>UPES</b> UNIVERSITY WITH A PURPOSE
<b>Enrolment No:</b>	

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**  
**Online End Semester Examination, June 2021**

<b>Course: Introduction to cryptography</b> <b>Program: Common paper minor-II</b> <b>Course Code: MRBL 0202</b>	<b>Semester: IV</b> <b>Time : 03 hrs</b> <b>Max. Marks: 100</b>
---	---

**SECTION A**

- 1. Each Question will carry 5 Marks**  
**2. Instruction: Complete the statement / Select the correct answer(s)**

S. No.	Question	CO				
Q 1	(a) Cryptanalysis aims to comprise -----, ----- and ----- (b) Technical attacks target the ----- Side channel attacks target the -----	<b>CO 1</b>				
Q 2	Mention 05 mathematical attacks in cryptanalysis -----, -----, -----, ----- and -----	<b>CO 1</b>				
Q 3	Mention 05 possible causes for social engineering attack in cryptanalysis -----, -----, -----, ----- and -----	<b>CO 1</b>				
Q 4	Substitution Cipher means ----- Caesar cipher means -----	<b>CO 2</b>				
Q 5	With the help of following key generate the Cipher text for “ UPES conducts online exams” in Mono alphabetic cipher method <table border="1" style="width: 100%; margin-top: 5px;"> <tr> <td style="width: 30%;">alphabet</td> <td>ABCDEFGHIJKLMN OPQRSTUVWXYZ</td> </tr> <tr> <td>Key</td> <td>DKVQFIBJWPESCXHTMYAUOLRGZN</td> </tr> </table>	alphabet	ABCDEFGHIJKLMN OPQRSTUVWXYZ	Key	DKVQFIBJWPESCXHTMYAUOLRGZN	<b>CO 3</b>
alphabet	ABCDEFGHIJKLMN OPQRSTUVWXYZ					
Key	DKVQFIBJWPESCXHTMYAUOLRGZN					
Q 6	In RSA algorithm To encrypt a message m, the sender obtains ----- and computes -----	<b>CO 3</b>				

**SECTION B**

- 1. Each question will carry 10 marks**  
**2. Instruction: Write short / brief notes**

Q 7	Explain the importance of hash functions in cryptographic processes	<b>CO 2</b>
Q 8	Compare the following terms (a) Codes Vs Ciphers (b) Transposition Vs Substitution (c) Monoalphabetic Vs Polyalphabetic	<b>CO 3</b>
Q 9	Describe the Public key infrastructure and requirements of Public- key certificate	<b>CO 2</b>
Q 10	Explain pseudo code analysis with an example	<b>CO 3</b>
Q 11	Explain clearly block cipher and DES	<b>CO 2</b>

**Section C**

**1. Each Question carries 20 Marks.**

**2. Instruction: Write long answer.**

Q 12	(a) Explain the types of cryptanalytic attacks (b) Describe asymmetric cryptography (c) Define RSA and explain the encryption and decryption with an example	<b>CO 3</b>
------	--	-------------