Pandit Deendayal Energy University, Gandhinagar
School of Technology
Internal Examination 2

B. Tech. (ICT) **Semester – V**
Date: 29/10/2021 **Time: 03.00 PM to04:30 PM**
Course Name : Information Security **Course Code : 20IC310T**
Max. Marks: 30

Instructions :

- Submit legible hand written assignment on foolscap A4 size pages as single pdf- named with your roll no. and name.
- Write your name, roll no., subject name and code at top of the assignment.
- Assume suitable data wherever essential and mention it clearly.
- Writing appropriate units, nomenclature, and drawing neat sketches/schematics wherever required is an integral part of the answer.
- Submit assignment online through Teams only.
- Each question is of 10 marks
- Only handwritten answers allowed.

No	Question	Mark	CO
1	Compare CFB(Cipher FeedBack) and OFB (Output FeedBack) system. (2 marks per difference)	10	CO1
2	Let's consider that Alice and Bob carries out the Diffie-Hellman Key Exchange with prime number p=17 and primitive root g=3 a) Suppose Alice chooses private key X=8 and Bob chooses private key Y=10. Show the computations performed by both Alice and Bob to determine the shared secret key. (1 mark for answer, 4 marks for justification). b) If Alice and Bob has compute the public keys 14 and 4 respectively then what is Alice's private key X and Bob's private key Y. (1 mark for answer, 4 marks for justification).	10	CO4
3	Discuss the following with respect to RSA in COVID-19 related applications. • Discuss on the advantages with an example (3 marks) • Discuss on the disadvantages with an example (3 marks) • Discuss on security analysis with an example (4 marks)	10	CO6