GURUDAS COLLEGE
INTERNAL EXAMINATION,2020
COMPUTER SCIENCE (HONOURS)
SEMESTER IV
PAPER SEC B-1
THEORY

F.M : 40

GROUP A

Answer any 4(four) questions

1. What is MAC algorithm? How is security of MAC function express? 5+5

2. Explain MD5 algorithm. 10

3. Explain DES function with proper diagram. Why we use XOR function in DES? 6+4
4. Explain Authentication header protocol in Transport mode of IP security. 5+2+3

   What is IP security? Write down the goals of IP security

5. Write down the differences 2.5x2

   i. Tunnel and Transport mode
   ii. AH and ESP protocol

   Briefly define a Group, Ring, Field. 5

6. Find integers x such that 10
   $5x \equiv 4 \pmod 3$
   $7x \equiv 6 \pmod 5$
   $9x \equiv 8 \pmod 7$

GROUP B
INTERNAL ASSESSMENT
F.M:10

1. Find the multiplicative inverse of each nonzero element in Z_5. 5

2. Use Fermat's Little Theorem to compute $3^{302} \bmod 5$, $3^{302} \bmod 7$ and $3^{302} \bmod 11$. Use your results and the Chinese remainder theorem to find $3^{302} \bmod 385$ 5

Send the Scanned answer scripts to the following mail id:
csexam.cmsa3@gmail.com