Total No. of Printed Pages—15

**3 SEM TDC GEMT (CBCS) GE 3 (A/B/C)**

**2020**

( Held in April–May, 2021 )

MATHEMATICS

( Generic Elective )

Paper : GE–3

*Full Marks* : 80
*Pass Marks* : 32

*Time* : 3 hours

*The figures in the margin indicate full marks for the questions*

Paper : GE–3A

**( Real Analysis )**

**1.** *(a)* Define finite set. 1

*(b)* Determine the set $A$ of $x$ $R$ such that $|2x \quad 3| \quad 7$. 2

*(c)* Prove that the set N×N is denumerable, where $N$ is the set of natural numbers. 3





*(d)* An upper bound $U$ of a non-empty set $S$ in $R$ is the supremum of $S$ if and only if for every 0, there exists an $S$ $S$, prove that $U$ $S$ . 4

*Or*

Let $S$ be a non-empty subset of $R$ and $S$ is bounded above. For $a$ $R$, define the set $a$ $S$ $\{a \quad s : s \quad S\}$. Prove that $\sup(a \quad S) \quad a \quad \sup S$.

**2.** *(a)* Write the statement of Bolzano-Weierstrass theorem for a set. 1

*(b)* If $x$ $R$ (set of real numbers), then there exists $n_x$ $N$. Prove that $x \quad n_x$. 4

*Or*

If $S \quad \frac{1}{n} : n \quad R$ , then prove that inf $S$ 0.

*(c)* Prove that the set $R$ of real numbers is not countable. 5

*Or*

Let there exists a positive real number $x$. Then prove that $x^2 \quad 2$.

**3.** *(a)* Define real sequence. 1

*(b)* Write the sequence formula for the following terms : 1

$$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \cdots$$

*(c)* Prove that a convergent sequence of real numbers is bounded. 3

*(d)* Use general principle of Cauchy's criterion for convergence to show that $\{S_n\}$ is not convergent, where

$$S_n \quad \frac{1}{1} \quad \frac{1}{2} \quad \frac{1}{3} \quad \frac{1}{4} \quad \cdots \quad \frac{1}{n}$$ 5

*Or*

Show that the sequence $\{S_n\}$, where $S_n \quad 1 \quad \frac{1}{n}^{n}$ is convergent and that limit of $1 \quad \frac{1}{n}^{n}$ lies between 2 and 3.

**4.** *(a)* Write the squeeze theorem. 2

*(b)* If $X \quad \{x_n\}$ is a convergent sequence of real numbers, then prove that $X$ is a Cauchy sequence. 3





*Or*

Use the definition of the limit of a sequence to establish the following limit :

$$\lim_{n} \frac{3n \quad 1}{2n \quad 5} \quad \frac{3}{2}$$

*(c)* Let $\{x_n\}$ be the sequence of real numbers defined by $x_1 \quad 1$, $x_{n \ 1} \quad \sqrt{2x_n}$, for $n \quad N$. Show that $\{x_n\}$ converges and find its limit. 5

*Or*

Let $x_1 \quad 8$ and $x_{n \ 1} \quad \frac{x_n}{2} \quad 2$, for $n \quad N$. Show that $\{x_n\}$ is bounded and monotone. Find the limit.

**5.** *(a)* What is called positive series? 1

*(b)* Write the condition for convergence of infinite geometric series

$$1 \quad r \quad r^2 \quad \cdots \quad r^n \quad \cdots \text{ to}$$ 1

*(c)* State the conditions of D'Alembert's ratio test for convergence of an infinite series. 2

*(d)* Prove that a positive term infinite series

$$\frac{1}{1^P} \quad \frac{1}{2^P} \quad \frac{1}{3^P} \quad \cdots \quad \frac{1}{n^P} \quad \cdots \text{ to}$$

is convergent if $P$ 1. 3

*(e)* Show that

$$\frac{1}{n^2}$$

is absolutely convergent. 3

**6.** Test the convergence of any *two* of the following : 5×2=10

*(a)* $\sum_{n=1} \frac{\cos n}{n^2}$

*(b)* $\frac{1}{1^P} \quad \frac{1}{2^P} \quad \frac{1}{3^P} \quad \frac{1}{4^P} \quad \cdots$, for $P$ 0

*(c)* $\sum_{n=1} \frac{n^{n^2}}{(n \quad 1)^{n^2}}$

*(d)* $\sum_{n=1} \frac{2n \quad 1}{n!}$





**7.** *(a)* Define sequence of functions. 1

*(b)* Prove that

$$\lim_n \frac{x}{n} \quad 0$$

for $x$ $R$, $n$ $N$, where

$$f_n(x) \quad \frac{x}{n}$$ 2

*(c)* Show that the sequence of function $\{f_n\}$, where

$$f_n(x) \quad \frac{1}{x \quad n}$$

is uniformly convergent in any interval $[0, K]$, $K$ 0. 3

*(d)* Let $\{f_n\}$ be a sequence of functions such that

$$\lim_n f_n(x) \quad f(x), \; x \quad [a, b]$$

and let $M_n$ $\sup |f_n(x) \quad f(x)|$. Then prove that $f_n$ $f$ uniformly convergent on $[a, b]$ if and only if $M_n$ 0 as $n$ . 4

*Or*

Test the uniform convergence of the sequence $\{f_n\}$, where

$$f_n(x) \quad \frac{nx}{1 \quad n^2x^2}$$

for all real $x$.

**8.** *(a)* Define power series. 1

*(b)* Find the radius of convergence of the following (any *one*) : 4

*(i)* $\frac{(n!)^2}{(2n)!}x^n$

*(ii)* $\frac{n^n}{n!}x^n$

*(c)* Show that the series for which

$$f_n(x) \quad \frac{1}{1 \quad nx}$$

can be integrated term by term in [0, 1] although it is not uniformly convergent. 5

*Or*

For all $n \quad N$

$$L \quad \lim_n \left| \frac{a_{n \ 1}}{a_n} \right|$$

exists finitely or infinitely, then prove that the radius of convergence of the series

$$R \quad \frac{1}{L}$$





Paper : GE–3B

**( Cryptography and Network Security )**

**1.** *(a)* *(i)* Write the full form of the abbreviation SHA. 1

*(ii)* What is MD5? 1

*(iii)* Write the name(s) of the discoverer(s) of public-key encryption. 1

*(iv)* What is the principal objective for developing public-key infrastructure? 1

*(b)* *(i)* Why do there involve two separate keys in public-key cryptosystem? 2

*(ii)* How does a message authentication or digital signature mechanism work? 2

**2.** Answer any *three* of the following : 3×3=9

*(a)* What are plaintext and ciphertext in public-key encryption?

*(b)* What is a cryptographic hash function and how does it work in message authentication?

*(c)* What are the requirements for a digital signature?

*(d)* What are CA (certification authority) and RA (registration authority) in the PKIX model?

**3.** Describe the RSA algorithm. 7

*Or*

Write a short note on secured hash algorithm.

**4.** *(a)* *(i)* For what purpose, port scanning is done? 1

*(ii)* What is the full form of the abbreviation ICMP? 1

*(iii)* What do you mean by buffer overflow? 1

*(b)* Answer any *two* of the following : 2×2=4

*(i)* Why does a SYN-flood occur?

*(ii)* What is smurf attack?

*(iii)* What is the role of Authentication Header (AH) in IP security documents?

**5.** *(a)* How does a teardrop attack work? 3

*(b)* What is Security Association (SA) in IP security policy and what are the parameters that identify SA? 4





**6.** Answer any *two* of the following : 5×2=10

*(a)* Define the various parameters of a security association in a security association data base entry.

*(b)* What is Virtual Private Network (VPN) and how does it work?

*(c)* Give a brief description of Encapsulating Security Payload (ESP) format.

**7.** *(a)* *(i)* What is secured electronic transaction? 1

*(ii)* What is a firewall? 1

*(iii)* What is a router? 1

*(b)* Answer any *two* of the following : 2×2=4

*(i)* What services does the SSL record protocol provide for SSL connection?

*(ii)* What are the three fields that have in an SSL handshake protocol message?

*(iii)* What are the key elements of the model of network management that are used for SNMP?

**8.** *(a)* Give a brief explanation on the purpose of use of proxy-firewall. 3

*(b)* Write about the access policy of SNMPv1. 3

**9.** Answer any *three* of the following : 4×3=12

*(a)* Explain the key features of SET (secured electronic transaction).

*(b)* What are four general techniques that firewalls use to control access and enforce the site's security policy, and how do they work?

*(c)* What are the roles of SMI (structure of management information) and MIB (management information base) in network management?

*(d)* What is packet-filtering router and how does it work?

**10.** What is bastion host? Write the characteristics of a Bastion host. 1+6=7

*Or*

What is SNMPv3? Write about the Protocol Data Units (PDUs) defined in SNMPv3. 7





Paper : GE–3C

**( Information Security )**

**1.** Answer the following : 1×8=8

*(a)* State any two modes of operation of block cipher.

*(b)* State one difference between threats and attack.

*(c)* What is a hash function in cryptography?

*(d)* How does digital signature differ from authentication protocol?

*(e)* List the three classes of intruders.

*(f)* State one difference between statistical anomaly detection and rule-based detection.

*(g)* State one merit of Diffie-Hellman key-exchange algorithm.

*(h)* Define orange book.

**2.** Answer the following : 2×8=16

*(a)* List the parameters (block size, key size and no. of rounds) for three AES versions.

*(b)* Why is trap door one-way function used?

*(c)* Calculate the cipher text for the following using one time pad cipher :

PLAIN TEXT = ROCK & KEYWORD = BOTS

*(d)* Specify the components of encryption algorithm.

*(e)* Draw the block diagram of MD5 message digest algorithm.

*(f)* Write the steps involved in the simplified form of the SSL/TLS protocol.

*(g)* Explain how the integrity of message is ensured without source authentication.

*(h)* Why is ECC better than RSA? However why is it not widely used? Explain.





**3.** How is hash function algorithm designed? Explain their features and properties. 5+5=10

**4.** Answer the following :

*(a)* Describe in detail the key generation in AES algorithm and its expansion format. 6

*(b)* Describe triple DES and its applications. 5

*Or*

*(c)* Explain briefly about Diffie-Hellman key-exchange algorithm.

*(d)* Solve using playfair cipher method, encryption of the word 'semester result' with the keyword 'examination'. 10

*(e)* Describe digital signature algorithm and show how signing and verification is done using DSS. 5

**5.** Answer any *two* of the following : 10×2=20

*(a)* Explain the different security mechanism involved in a intrusion detection system.

*(b)* Analyze various types of virus and its counter measures.

*(c)* Explain the different aspects of security with examples.

★ ★ ★