2106E0176

Candidate's Seat No :_____

M.Tech. (N. & C.) (Sem.-2) (Old) Examination

Network Analysis and Design

Time : 3-00 Hours] **June 2019** **[Max. Marks : 100**

SECTION-I

Q-1

[A] Describe the user requirements. [18]

[B] As a network engineer, your customer is a hospital that wants to upgrade their LAN. Develop a questionnaire to gather requirements from users, hospital management and staff.

[C] Explain dependencies between performance mechanisms.

Q-2

[A] Differentiate between fundamental requirement and feature. [16]

[B] Describe application types.

[C] How capacity requirements can be developed? How data rates are estimated?

[D] Explain distributed computing flow model.

OR

Q-2

[A] Which phrases and keywords are used to categorize the requirement? [16]

[B] Explain individual flow and composite flow.

[C] Differentiate interactive bulk and interactive burst application.

[D] Explain the process of identifying and developing flow.

Q-3 Attempt any four

[A] How requirements can be tracked and managed? [16]

[B] How RMA requirements can be developed?

[C] Explain network management mechanism.

[D] What does performance component architecture describe?

[E] Explain Access/Distribution/Core architectural model

SECTION - 2

Q-4

[A] A component architecture is a description of how and where each network function is applied within that network. Besides addressing/routing, network management, performance, and security, list 3 other possible component architectures for a network. What does each component architecture describe? Show each function, capability, and give 2 examples of mechanisms. [18]

[B] Explain variable length subnetting with example.

[C] Write the process of identifying and classifying routing boundaries.

Q-5

[A] Write following for class B address. [16]
Network addresses, natural mask, number of network addresses, number of device addresses.

[B] Explain route filtering and route aggregation.

[C] What is the difference between service level agreement and policies?

[D] What are service characteristics? How they are useful?

OR

P.T.O.

Q-5 [16]

[A] Write following for class C address.
Network addresses, natural mask, number of network addresses, number of device addresses.

[B] Explain private addressing and NAT.

[C] Describe instrumentation mechanism.

[D] How architectural models can help in determining where security mechanisms can be applied in the network.

Q-6 Attempt any four. [16]

[A] Consider class B network. While working on subnet mask explain 2 bit, 3 bit mask.

[B] "Network Management can be viewed as a structure consisting of multiple layers". Justify.

[C] Describe monitoring mechanism.

[D] Explain Design Traceability.

[E] What is tactical and strategic planning?

2/7

2406E0183

Candidate's Seat No : _____

M.Tech. (N. & C.) (Sem.-2) Examination

Networking-2

June 2019

Time : 3-00 Hours] [Max. Marks : 100

SECTION - I

Q1 **Answer / Explain the following in brief: (Give examples wherever necessary) :** [20]

a. What is ARP cache revalidation?
b. The IP Address 108.23.121.114 belongs to _____ class.
c. What is logical address ?
d. Calculate the Subnet mask for a Class 'B' address and 8 subnets.
e. State the role of ICMP.
f. How do you send multimedia in e-mail? State the protocol used.
g. State the well known port number of POP and IMAP.
h. What do you understand by active open and passive open?
i. State any two different commands used by the Operating systems to manage or display network configurations.
j. What is tail drop in routers?

Q2 **Answer the following in Detail: (Any 3) :** [18]

a. Write a Short Note on Telnet NVT and Option Negotiation giving an example.
b. Explain the working of FTP in detail.
c. List the protocols used for Email Communications, explain each one of them in brief.
d. Discuss the protocols that use TCP as a service.
e. Write a detailed note on IP header.

Q3 **Answer the following in brief (Any 3):** [12]

a. Discuss the role of IETF and IEEE with reference to computer networking.
b. Discuss whether the protocols for wired and wireless networks need to be different or not.
c. Discuss any one software that can help analyze network.
d. Write a short note on IP forwarding algorithm.
e. What is the role of DNS? Discuss different types of resolution techniques.

P. T. O.

SECTION - II

Q4 **Answer / Explain the following in brief: (Give examples wherever necessary):** **[20]**

a. Explain the concept of packet encapsulation.
b. What is tunneling? When is it used?
c. State strict source routing.
d. Why is round trip time necessary in networking?
e. Discuss the use of random time in DHCP.
f. What is the difference between HTTP and HTTPs?
g. What is the role of TFTP? When is it used?
h. When does TCP retransmit the data?
i. What is sorcerer's apprentice bug?
j. Why does router modify the header of all packets passing through it?

Q5 **Answer the following in Detail: (Any 3) :** **[18]**

a. Discuss the TCP Flags and their use.
b. Explain the following features of HTTP (a) Support for Caching (b) Support for negotiation.
c. Write a detailed note on VPN.
d. List the protocols that require checksum calculation. Justify each protocol.
e. For the following CIDR Notation, calculate (a) First Address (b) Last Address (c) CIDR Subnet Mask (d) No. of IPs in the given block
IP address: 108.21.99.06 / 21

Q6 **Answer the following in brief (Any 3):** **[12]**

a. Discuss the role of VPN.
b. Differentiate between classful and classless addressing.
c. Discuss any one software that can be used to simulate networking.
d. What is pseudo-header in UDP? Why is it used?
e. Discuss the concept of 'Additive Increase & Multiplicative Decrease' in TCP.

2506E0190

Candidate's Seat No :_____

M.Tech. (N. & C.) (Sem.-2) Examination

Networ Security

June 2019

Time : 3-00 Hours] **[Max. Marks : 100**

SECTION-I

Q1 Answer the followings in brief: **[20]**

a. How is encoding different from encryption?
b. Explain the term 'deterrence'.
c. How is Network Security different from Information Security?
d. What do you understand by 'Visual Event Monitoring'?
e. Explain the role of hashing algorithms in network security?
f. How do we enforce non-repudiation?
g. State the role of CERT.
h. Differentiate between virus and worms.
i. What do you understand by 'forensic analysis'?
j. Discuss how outlived design leads to vulnerabilities?

Q2 Answer the followings in detail (Any 3): **[15]**

a. Discuss any 5 different security standards in brief.
b. Discuss briefly various human factors that generate security vulnerability.
c. List different security techniques mapped with layers of OSI.
d. List and explain in brief types of viruses.
e. Explain the need & process of building security policy.

Q3 Answer the followings in brief (Any 5): **[15]**

a. What is CIA triad?
b. Discuss the role of IETF.
c. Explain briefly any 3 malwares.
d. What is social engineering? How does it obstruct security?
e. Explain the access control matrix and its elements.
f. What is role-based access control?
g. What do you understand by anomaly detection in IDS?

SECTION-II

Q4 Answer the followings in brief: **[20]**

a. Given an example of DoS attack.
b. What do you understand by penetration testing?
c. What is the use of audit trials?
d. Explain the role of security administration team.
e. What is ACL?
f. Explain biometric based administration.
g. Differentiate between coarse grained Vs. fine grained authorization.
h. Differentiate between stateful Vs. stateless firewall.
i. What is SSH?
j. What is the role of IPv6?

P.T.O.

E190-2

Q5 **Answer the followings in detail (Any 3):** [15]

a. Explain the architecture of IDS.
b. List and briefly explain the modules of NIPS.
c. Discuss the architecture of Kerberos.
d. Write a short note on SET.
e. Explain the role and working of TACAS+.

Q6 **Answer the followings in brief (Any 5):** [15]

a. List and explain types of authorization systems.
b. Discuss packet inspection firewalls in brief.
c. List firewall services mapped to network layers.
d. Explain NAT.
e. Explain VPN.
f. What is DMZ? Why is its placement important?
g. What is the role of PAP and CHAP?

2606E0195

Candidate's Seat No :_____

M.Tech. (N. & C.) (Sem.-2) Examination

Networ Analysis and Design

Time : 3-00 Hours] **June 2019** **[Max. Marks : 100**

SECTION-I

Q-1

[A] Write the difference between general thresholds and environment specific threshold. State the difference between threshold and limit. What are the general thresholds and limits for Interaction delay, Human response time and Network propagation delay [18]

[B] Define flows. Write the common flow characteristics. What are one part, two part and multi part flow specifications?

[C] Explain the fields in the template for the requirements specification. Document the requirement specification for establishing LAN at hospital.

Q-2

[A] What are the initial conditions for gathering and listing requirements? [16]

[B] Describe the requirements of devices that the network will support.

[C] (i) What is the broadcast address of the network 192.168.21.64/28?
(ii) What valid host range is the IP address 172.18.56.247/22 a part of?

[D] Explain topological architecture models.

OR

Q-2

[A] Explain the three performance characteristics –capacity, delay and RMA. [16]

[B] (i) What is the broadcast address of the network 172.22.26.0 255.255.255.0?
(ii) What is the first valid host on the subnetwork that the node 172.23.110.31/23 belong to?

[C] State the information Flows Between Network Analysis, Architecture, and Design?

[D] Describe the need of hierarchy and diversity in network.

Q-3 Attempt any four

[A] Categorize each of the following requirements as core/fundamental, feature or informational. [16]

a. Network must support fast Ethernet and Gigabit Ethernet interfaces for all devices on the network.
b. Network backbone should be upgradable in capacity to 10 Gb/s within two years of deployment.
c. Finance department requires firewall protection to the server.
d. Existing network consists of 10BaseT Ethernet and FDDI segments.

[B] State the purpose of service metric. Also explain in detail service metrics.

[C] What is the network address and subnet mask for class A,B,C,D type addresses?

[D] Describe one – one application each which requires best effort and guaranteed performance.

[E] State and explain general user requirements.

SECTION - 2

Q-4

[A] Describe the role of routing in networking. Write the comparison between RIP(routing information protocol) and OSPF(open shortest path first). [18]

P. T. O.

[B] Explain the following.

(i) Interactions between performance and addressing/routing.
(ii) Interactions between performance and network management.
(iii) Interactions between performance and security

[C] What is reference architecture? Describe process model for component architecture approach.

[16]

Q-5

[A] State the difference between subnetting and supernetting?
[B] Explain functional architecture model.
[C] What is in band and out of band management? What are the trade offs?
[D] Differentiate between Accept specifics/deny all and Accept all/deny specifics policy.

OR

[16]

Q-5

[A] Explain the functionality of SNMP(simple network management protocol)
[B] What are architectural consideration for fault and configuration management?
[C] For networking, explain centralized and distributed management.
[D] What is the difference between first order, second order and third order product?

[16]

Q-6 Attempt any four.

[A] What is the threat analysis? List 3 assets and threat belonging to them.
[B] For what purpose network address is? Explain local, global, private, public, temporary or persistent.
[C] Define security policies and procedures. What should be included in policies and procedures?
[D] How network blueprint is created?
[E] How Vendor, equipment and service provider evaluation is done?

/12

2406E0184

Candidate's Seat No :_____

M.Tech. (Web. Tech.) (Sem.-2) Examination

Web Application Development-2

June 2019

Time : 3-00 Hours] [Max. Marks : 100

Note : (1) Write both the sections in the separate answer books.

(2) Figures to the right indicate full marks.

(3) Write answers in point form.

SECTION-I

Q.1 Answer the following (Any three) **[18]**

(a) What are the features of Django Framework?

(b) Explain comparison operations in Django with an example.

(c) Explain built-in Django filters.

(d) Write short note on Django's MVT architecture.

Q.2 Answer the following (Any five) **[20]**

(a) Explain the use of Django project files - urls.py, views.py, models.py, settings.py.

(b) Discuss advantages and disadvantages of Jinja Framework.

(c) What are the attributes and methods available in a view method's requests reference?

(d) Explain usage of Django template tags - include, extends, block, load.

(e) Explain csrf_token and form.cleaned_data with an example.

(f) What helper methods Django forms provide for simplifying the output form fields?

Q.3 Do as directed **[12]**

(a) Fill in the blanks:

i. _____ tag is used to integrate resources such as css, images, javascript, etc.

ii. _____ method is used to perform form validation on each form field.

(b) Identify whether the statement is true or false and provide explanation:

i. Values declared after a vertical bar | are called tags.

P. T. O.

ii. The {# #} syntax can be used for a single line comment on Django templates.

(c) What is the use of {% cycle %} and {{block.super}} ?

SECTION-II

Q.4 Answer the following (Any three) [18]

(a) Write short note on Django Forms with an example.

(b) What are Django Models ? How they can be created ?

(c) Explain loops in Jinja Framework.

(d) List out various Django form field attributes accessible in templates.

Q.5 Answer the following (Any five) [24]

(a) How to create reusable templates in Django?

(b) How to handle Django form errors?

(c) What are the steps to send a mail in Django via Gmail account ?

(d) Explain types of Django user classes.

(e) Explain any four datatypes of a Django Model.

(f) How to create a single record with save() or create() in Django Models?

Q.6 Do as directed [08]

(a) Identify three incorrect syntax errors in the following Django code, correct it, and display the output:

- ***views.py***

```
nameList = ["Xavier", "John", "Zac", "Dwayne", "Drake"]
```

- ***page.html***

```
{% for name as nameList %}
<p>{{ forloop.countner }} { ame }</p>
{% for %}
```

(b) What does the following URL patterns represent in Django?

- \d+
- \D+
- [-\w]+
- [A-Z]{2}

2506E0191 Candidate's Seat No :_____

M.Tech. (Web. Tech.) (Sem.-2) Examination

Web Server Management

Time : 3-00 Hours] **June 2019** **[Max. Marks : 100**

Part – I

Small Questions **[Total Marks 50]**

Question – 1

Following command / commands is / are used to start apache in rpm / yum installation.
Select one or more answer from below.

a) apachectl start httpd
b) httpd start
c) systemctl start httpd
d) service httpd start

Question – 2

The following lines prevent .htaccess and .htpasswd files from being viewed by Web clients.

```
<Files ~ "^\.ht">
   Order allow,deny
   Deny from all
   Satisfy all
</Files>
```

True / False

Question – 3

With reference to below apache configuration directive

```
Alias /docs /var/web
```

The URL http://www.example.com/docs/dir/file.html will be served from /var/web/dir/file.html

True / False

Question – 4

Write a Redirect rule to redirect "/docs/" directory to http://new.example.com/docs/

Question – 5

Default apache web server DocumentRoot value is

_____.

P.T.O

E191 - 2

Question – 6

How to get the list of all "process ID" of all running apache processes ?

1) pgrep apache
2) pgrep httpd
3) ps -el | grep apache
4) grep httpd
5) apachectl -l

Question – 7

You should avoid using .htaccess files completely if you have access to httpd main server config file. Using .htaccess files slows down your Apache server. Any directive that you can include in a .htaccess file is better set in a Directory block, as it will have the same effect with better performance.

True / False

Question – 8

To make the server accept connections on both port 80 and port 8000 for (ipv4) following configuration parameters can be used. (select one or more options)

a)Listen 80
Listen 8000

b)Listen 192.0.2.1:80
Listen 192.0.2.5:8000

c)Listen 80 & 8000

d)Listen [2001:db8::a00:20ff:fea7:ccea]:80

Question – 9

Is it possible to provide HTTP and HTTPS from the same server? If yes please list the default ports.

Question – 10

If you plan to use .htaccess files, you will need to have a server configuration that permits putting authentication directives in these files. This is done with the _____ directive.

Select from below: (choose multiple if possible)

a) AllowOverride AuthConfig
b) htpasswd
c) AuthType Basic
d) AuthUserFile /usr/local/apache/passwd/passwords

E191-3

Question – 11

What does below rewrite configuration means? (very short)

```
RewriteEngine On
RewriteRule ^about$ about.html [NC]
```

Question – 12

What are the types of virtual hosts ?

Question – 13

What is meaning of "Listen" in httpd.conf file ?

Question – 14

On newly installed apache on Redhat based distribution, what happened if index.html not exist?

1) Error message will be displayed
2) Blank page displayed
3) Default html page will be displayed from welcome.conf
4) Apache will not start

Question – 15

To install https functionality
select one or more

1) install https package
2) install mod_ssl package and restart the http service
3) install mod_secure and restart the http service
4) Just restart https service.

Question 16

To install apache on redhat based system following can be used (select one or more)

1) yum install httpd
2) yum install apache
3) rpm -ivh httpd-*.rpm
4) yum install apache2

Question – 17

List Apache Important configuration file name?

Question – 18

What do you mean by a valid ServerName directive?

P.T.O

E191-4

Question – 19

the URL http://example.com/~hardik/file.html will be translated to the file path

1) /home/hardik/public_html/file.html
2) /var/www/html/hardik/public_html/file.html
3) /var/www/hardik/public_html/file.html
4) /home/hardik/file.html

Question – 20

Apache mod_ssl or https **self signed certificate** are more secure than CA sign certificate.

True / False

Question – 21

With use of .htaccess file apache server need to be restart to apply the new changes in .htaccess file.

True / False

Question – 22

Is it possible to run multiple instances of apache in one server? Explain why

True / False

Question – 23

How to know if a web server is running?

Question – 24

What is the main difference between <Location> and <Directory> sections?

Question – 25

The default apache DocumentRoot in Redhat base distribution is

1) /var/www/html
2) /var/html
3) /www-htdocs
4) /var/www/virtual/html

Also explain what is **DocumentRoot**

E191-5

MI. Tech (Sem-II) Examination
Web Server Management

Part – II
(Attempt any 10 , Total Marks 50)

Question -1

Write userdir with explanation, how it works, it configuration and use.?

Question – 2

If you have only one IP address, but you want to host two web sites on your server. What will you do?

Question – 3

Please explain "server-status", host access (allow-deny) with reference to below configuration

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from 192.168.0.0/24 10.0.0.0/8
</Location>
```

Question - 4

Please explain in detail "virtual hosting" with example and configuration.

Question - 5

Please explain http authentication with reference to below configuration

```
NameVirtualHost 192.168.0.4:80
<VirtualHost 192.168.0.4:80>
    ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot /var/www/virtual/station4.example.com/html
    ServerName station4.example.com
    ErrorLog logs/station4.example.com-error_log
    CustomLog logs/station4.example.com-access_log common
        <Directory /var/www/virtual/station4.example.com/html/emc>
                AuthName "Authorised only for allowed users"
                AuthUserFile "/etc/httpd/conf/station4.passwd"
                AuthType Basic
                Require user1 user2
        </Directory>
        <Directory /var/www/virtual/station4.example.com/html/protected>
                AuthName "Authorised only for allowed users"
                AuthUserFile "/etc/httpd/conf/station4.passwd"
                AuthType Basic
                Require valid-user
        </Directory>
</VirtualHost>
```

P.T.O

E191-6

Question – 6

Write a short note on mod_ssl / https module. Discuss self sign certificate and certificate signed by third party or CA. Please draw a diagram for both scenario.

Question – 7

How can we Serve content out of directory other than the DocumentRoot directory, with example.?

Question – 8

Explain Aliases, Redirecting, and Rewriting rules.?

Question – 9

Discuss various factor to achieve excellent security.

Question – 10

How Does Apache Web Server works, and how many types of Web Servers are there.?

Question – 11

Explain apache logging

LogLevel warn

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

LogFormat "%{Referer}i -> %U" referer

LogFormat "%{User-agent}i" agent

CustomLog logs/access_log combined

2606E196

Candidate's Seat No :_____

M.Tech. (Web. Tech.) (Sem.-2) Examination

Web Security

June 2019

Time : 3-00 Hours] **[Max. Marks : 100**

SECTION-I

Q-1

[A] How cross domain data can be captured? [18]

[B] How HTTP authenticates users?

[C] Write the steps involved in reflected XSS attack.

Q-2

[A] Explain the fields in HTTP request method. [16]

[B] Explain format of URL.

[C] How server and user's browser handle cookie?

[D] Assuming the error code generation and given source code, how cross site scripting attack can occur?

http://mdsec.net/error/5/Error.ashx?message=Sorry%2c+an+error+occurred

Sorry, an error occurred.

OR

Q-2

[A] Explain the fields in HTTP response method. [16]

[B] What is the meaning of following status code?

1. 301 Moved Permanently
2. 400 Bad Request

[C] In case of mail injection attack, which part of mail is affected?

[D] "A key focus of research in the past decade has been client-side vulnerabilities", Justify.

Q-3 Attempt any two

[A] List various attacks against web application. [16]

[B] In case of security of web applications, which factors have combined to exacerbate the problem?

[C] How XSS attack can be prevented?

SECTION - 2

Q-4

[A] Explain SQL and NOSQL injection. [18]

[B] Describe the design flaws in authentication.

[C] How local privacy is preserved? What type of attacks occur?

Q-5

[A] Write the steps involved in a DOM-based XSS attack [16]

[B] In which type of application, stored XSS vulnerability is common?

[C] Given the XML code, how XML injection is done?

[D] Explain LDAP injection.

OR

Q-5

[A] Describe various approaches for reviewing the code. [16]

[B] Explain the path traversal attack.

P.T.O.

[C] For what purpose LDAP is used?
[D] How an attacker can exploit a stored XSS vulnerability to perform the session hijacking attack?

Q-6 Attempt any two. [16]
[A] Describe Implementation flaws in authentication.
[B] Analyze Java and .NET platform. Which is more vulnerable?
[C] Describe the signatures of common vulnerabilities.

2606E196

Candidate's Seat No :_____

M.Tech. (Web. Tech.) (Sem.-2) Examination

Web Security

June 2019

Time : 3-00 Hours] **[Max. Marks : 100**

SECTION-I

Q-1 [18]

[A] How cross domain data can be captured?

[B] How HTTP authenticates users?

[C] Write the steps involved in reflected XSS attack.

Q-2 [16]

[A] Explain the fields in HTTP request method.

[B] Explain format of URL.

[C] How server and user's browser handle cookie?

[D] Assuming the error code generation and given source code, how cross site scripting attack can occur?

http://mdsec.net/error/5/Error.ashx?message=Sorry%2c+an+error+occurred

Sorry, an error occurred.

OR

Q-2 [16]

[A] Explain the fields in HTTP response method.

[B] What is the meaning of following status code?

1. 301 Moved Permanently
2. 400 Bad Request

[C] In case of mail injection attack, which part of mail is affected?

[D] "A key focus of research in the past decade has been client-side vulnerabilities", Justify.

Q-3 Attempt any two [16]

[A] List various attacks against web application.

[B] In case of security of web applications, which factors have combined to exacerbate the problem?

[C] How XSS attack can be prevented?

SECTION - 2

Q-4 [18]

[A] Explain SQL and NOSQL injection.

[B] Describe the design flaws in authentication.

[C] How local privacy is preserved? What type of attacks occur?

Q-5 [16]

[A] Write the steps involved in a DOM-based XSS attack

[B] In which type of application, stored XSS vulnerability is common?

[C] Given the XML code, how XML injection is done?

[D] Explain LDAP injection.

OR

Q-5 [16]

[A] Describe various approaches for reviewing the code.

[B] Explain the path traversal attack.

P. T. O.

[C] For what purpose LDAP is used?
[D] How an attacker can exploit a stored XSS vulnerability to perform the session hijacking attack?

Q-6 Attempt any two. [16]
[A] Describe Implementation flaws in authentication.
[B] Analyze Java and .NET platform. Which is more vulnerable?
[C] Describe the signatures of common vulnerabilities.

2 /7

2006E0169

Candidate's Seat No :_____

M.Tech. (N. & C.) (Sem.-2) (Old) Examination
Wireless Networking and Mobile Computing
June 2019

Time : 3-00 Hours] **[Max. Marks : 100**

SECTION I

Q1. (a) Define the following: [10]

i. Frequency
ii. MAC address
iii. WTA
iv. Encapsulation
v. Cellular IP

Q1. (b) Explain various steps for mobile terminating call in GSM. Define IMSI, MSRN and TMSI number [8]

Q2. Justify the following statements: [16]

i. Data rate of optical band is greater than radio band
ii. Orthogonal FDMA reduce interference
iii. TCP is reliable protocol
iv. MIMO is appropriate for multipath propagation

OR

Q2. Give reasons: [16]

i. Hidden terminal problem reduces throughput
ii. Rainbow is formed during presence of clouds
iii. Active members in Bluetooth have 3-bit address
iv. Small cell sizes are appropriate in densely populated areas

Q3. Explain various signal propagation effects [16]

OR

Q3. Explain various multiple access techniques Write down the advantages and limitations of each [16]

P. T. O.

E169-2

SECTION II

Q4.(a)	Explain security mechanisms used in IEEE 802.11	[10]
Q4. (b)	Explain Bluetooth architecture	[8]
Q5.	Explain why Standard TCP fails in wireless scenario. Explain the I-TCP,a variant of TCP optimized for wireless scenario.	[16

OR

Q5.	Explain GSM architecture in detail.	[16]
Q6.	Explain Direct sequence spread spectrum with example.	[16]

OR

Q6. Explain different stages of Mobile-IP architecture as

i. Need
ii. Discovery
iii. Registration
iv. Tunnelling

2006E0170

Candidate's Seat No :_____

M.Tech. (N. & C. + Web. Tech.) (Sem.-2) Examination

Foundation of Cryptography

Time : 3-00 Hours] **June 2019** **[Max. Marks : 100**

NOTE : (1) Write both the sections in the separate answer books
(2) Figures to the right indicate full marks.
(3) Make necessary assumptions wherever necessary.

SECTION-I

Q.1 **Define the following (Any three)** [18]

1 Caesar cipher
2 Homophonic encoding
3 Public key cryptosystems
4 Playfair cipher
5 Perfect secrecy

Q.2 (a) Explain role of hash function in data integrity.
(b) Explain following modes of operation on block ciphers. (16)
1. Cipher block chaining mode
2. Counter mode

OR

Q.2 (a) Explain CBC-MAC
(b) Explain key life cycle in detail. (16)

Q.3 **Describe any two of the following.** (16)

(a) Explain Data Encryption standard in detail. Explain its expansion to triple DES.

OR

(a) Explain ElGamal cryptosystems.

SECTION-II

Q.4 **Define the following (Any three)** [18]

1 Identity based encryption
2 Pseudo random numbers
3 One time pads
4 Key storage in software vs hardware
5 Zero-knowledge mechanisms in entity authentication

Q.5 (a) What security services are provided by digital signatures?
(b) Explain digital signature creation using RSA. [16]

OR

Q.5 (a) Explain Deterministic vs. non deterministic generators of random numbers.
(b) Explain one-way password protection system. [16]

Q.6 **Explain the following (Any two)**

(a) Explain any 4 cryptographic protocols. [16]

OR

(a) Explain public key management models.

2106E0177

Candidate's Seat No :_____

M.Tech. (N.C. & Web. Tech.) (Sem.-2) Examination

Data Analytics

June 2019

Time : 3-00 Hours] **[Max. Marks : 100**

Instructions:

1. Figures to the right indicate full marks
2. Each section should be written in a separate answer book
3. Be precise and to the point in your answer

SECTION-I

1. Answer the following: (Any 10) **[20]**

i. What is Data Analytics? List some of its challenges.

ii. What is Stratified Sampling technique?

iii. Give an example of a Regression problem specifying the predictors and the response variables.

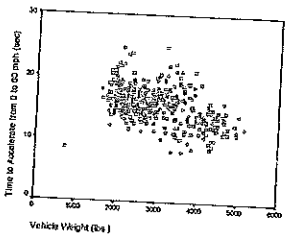
iv. What is a good value of error tolerance? And what is bad value?

v. From the given equations, what is the equation for the regression of Y on X? Why?
$Y = 4 + 2x$ OR $Y = X$ OR $Y = 2 + X$ OR $Z_X = Z_Y$

vi. What do you understand by Multivariate Analysis of Variance?

vii. What sort of statistical test of this hypothesis would you perform on the following?
"People who have high scores on the computer self-efficacy test will have low scores on the aging anxiety test"

viii. The pattern in the chart represents which type of Correlation? Why?



ix. Define Support and Confidence.

x. What is the best way to test the success of the Discriminant function in classifying new cases in Discriminant Analysis?

xi. What do you understand by Cross-Validation?

2. Attempt the following questions: (Any 5) **[20]**

A. Given a one-dimensional dataset {1,5,8,10,2}. Use Euclidean Distance to establish hierarchical grouping relationship and draw the Dendrogram.

B. Given a set of paired data (X,Y):

a) If Y is independent of X, then what value of a correlation coefficient would you expect?

b) If Y is linearly dependent on X, then what value of a correlation coefficient would you expect?

c) How could Y be closely dependent upon X yet $r \approx 0$?

C. Suppose you have the following data with one real-value input variable & one real-value output variable. What is leave-one out cross validation mean square error in case of linear regression (Y = bX+c)?

X (Independent Variable)	Y (Dependent Variable)
0	2
2	2
3	1

D. A researcher wishes to test the idea that shows size and mathematical ability are correlated; that is, people with larger feet have higher mathematical skills. To test this he conducts a study of an entire town of 2000 persons measuring their shoe size and administering a math test. He finds that there is a significant correlation between shoe size and math skills with people with larger feet having higher math skills.
What might be an important problem with this approach?

E. A student is asked to test the hypotheses for a mean where $\mu = 20$ and $\sigma = 10$ using $\alpha = 0.05$. After

P. T. O.

sampling she obtains: n = 100, X = 18

a) What is wrong with the following as a written solution?

$\sigma_X = 10/10 = 1.0000.$

$(18-20)/1 = 2 = 0.0228.$

b) Write it correctly.

c) What is your conclusion?

F. A researcher polled a number of people to determine their pie preferences and found the following frequencies:

	Apple	Berry	Cherry	Peach	Pumpkin
Male	12	10	15	9	12
Female	26	20	9	15	24

The null hypothesis is: there is no difference in the preferences for these pies, $\alpha = 0.05$.

a) What is the expected frequency for male and apple (just the single cell)?

b) What is the appropriate value for degrees of freedom?

c) What is the critical value for Chi-square?

d) The value of Chi-square obtained is 7.378. What is your conclusion regarding the null hypothesis?

3. Answer the following: (Any 1) **[10]**

A. Describe the Logistic Regression model for two classes and derive its expression for posterior probability that a given pattern x having p attributes is in class k, k=1,2.

B. Elaborate in detail about any two modern Data Analytics tools with examples.

SECTION-II

4. Do as Directed: (Any 2) **[20]**

A. What is Bayes Theorem? Consider an example training dataset with 1500 records and 3 classes Parrot, Dog and Fish. The Predictor features set consists of 4 features as: Swim, Wings, Green Color, Dangerous Teeth. Apply Naïve Bayes classifier for testing an animal to be a parrot, dog or fish assuming n number of records belonging to each class.

B. Carry out KNN algorithm on the following example:

Height (in cm)	158	158	158	158	158	163	163	160	160	160	160	160	160	160	160	160	160
Weight (in kg)	58	58	58	58	58	58	58	64	64	64	64	64	64	64	64	64	64
T-Shirt Size	M	M	M	M	M	M	M	L	L	L	L	L	L	L	L	L	L

C. In how many ways a Decision Tree can be formed? Explain the methods.

5. Attempt the following: **[20]**

A. What is Dimensionality Reduction? Discuss any one technique. [06]

B. Self-Organizing Maps exhibit "Winner-take-all" behavior. Justify. [04]

C. **Compare:** [06]

a) Supervised Vs. Unsupervised Learning

b) KNN Vs. K-Means Clustering

D. Why are Histograms considered to be one of the best Data Visualization tool? Explain with the help of an example. [04]

6. Answer the following: (Any 1) **[10]**

A. What are Support Vector Machines? What is the importance of Kernal in SVM? Explain the objective function of SVM.

B. What do you understand by Clustering Tendency? How would you assess the Clustering Tendency of a method? How do you validate the method?

****