CBCS SCHEME

USN □□□□□□□□□□ 15EC835

Eighth Semester B.E. Degree Examination, July/August 2021

Network and Cyber Security

Time: 3 hrs. Max. Marks: 80

Note: ***Answer any FIVE full questions.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

1 a. Describe the steps of SSL record protocol provides two services for SSL connections. **(08 Marks)**

b. Describe the different step involved in exchange of message from client and server in handshake protocol. **(08 Marks)**

2 a. Discuss the pseudorandom function in TLS. **(08 Marks)**

b. Discuss sequence of step involved during message exchange in user authentication protocols of SSH. **(08 Marks)**

3 a. Discuss the confidentiality and authentication in PGP cryptographic function. **(10 Marks)**

b. Define the five header fields in MIME. **(06 Marks)**

4 a. Illustrate the key component of the internet mail architecture with neat diagram. **(10 Marks)**

b. Discuss the five header fields in MIME. **(06 Marks)**

5 a. Describe the various IP security document categorized roadmap. **(06 Marks)**

b. Describe the IP security policy applied to each IP packet that transits from a source to a destination. **(10 Marks)**

6 a. With neat diagram, describe various fields in ESP packet format. **(08 Marks)**

b. With neat diagram, describe various fields in IKE header format. **(08 Marks)**

7 a. What are the significance of policy driven security certifications do net address the threat. **(08 Marks)**

b. Describe the list of specialized skills that should be available on demand in IT security. **(08 Marks)**

8 a. Describe the different type of full cyber anti-pattern template. **(12 Marks)**

b. What are the components of a micro anti-pattern templates. **(04 Marks)**

9 a. How does the zachman framework help with cyber security? **(06 Marks)**

b. Describe the architectural problem solving patterns. **(10 Marks)**

10 a. Describe the hardware setup sequence for a desktop pedestal. **(08 Marks)**

b. Describe the implementation with a combination of location protections, services and enterprise services that manage local configurations and services. **(08 Marks)**

* * * * *

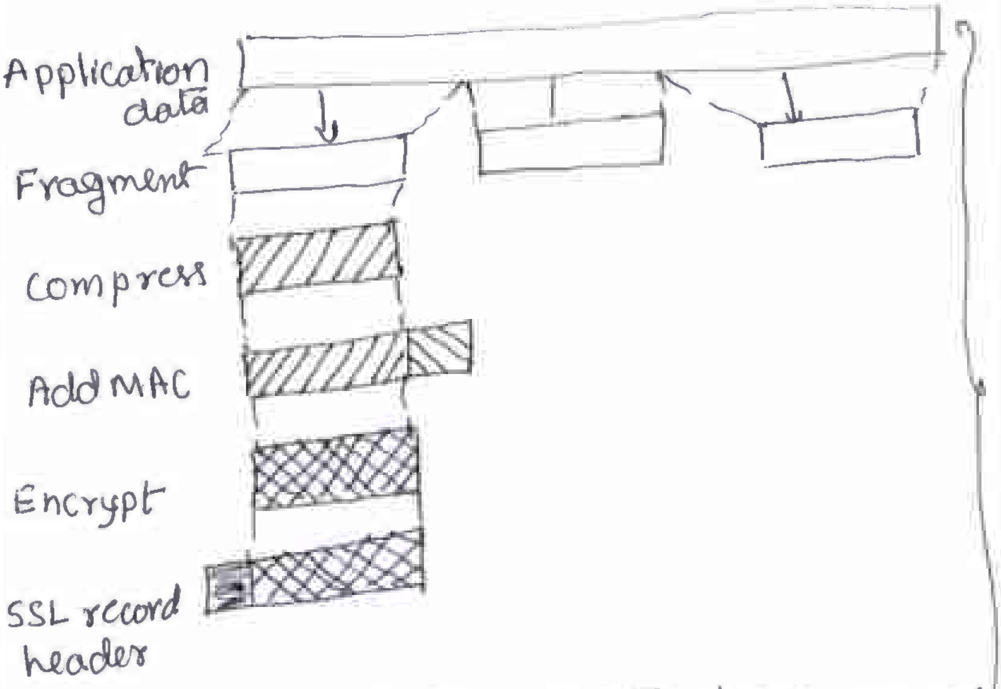
201215EC83528675

Visvesvaraya Technological University
Belagavi, Karnataka – 590 018.

Signature of Scrutinizer

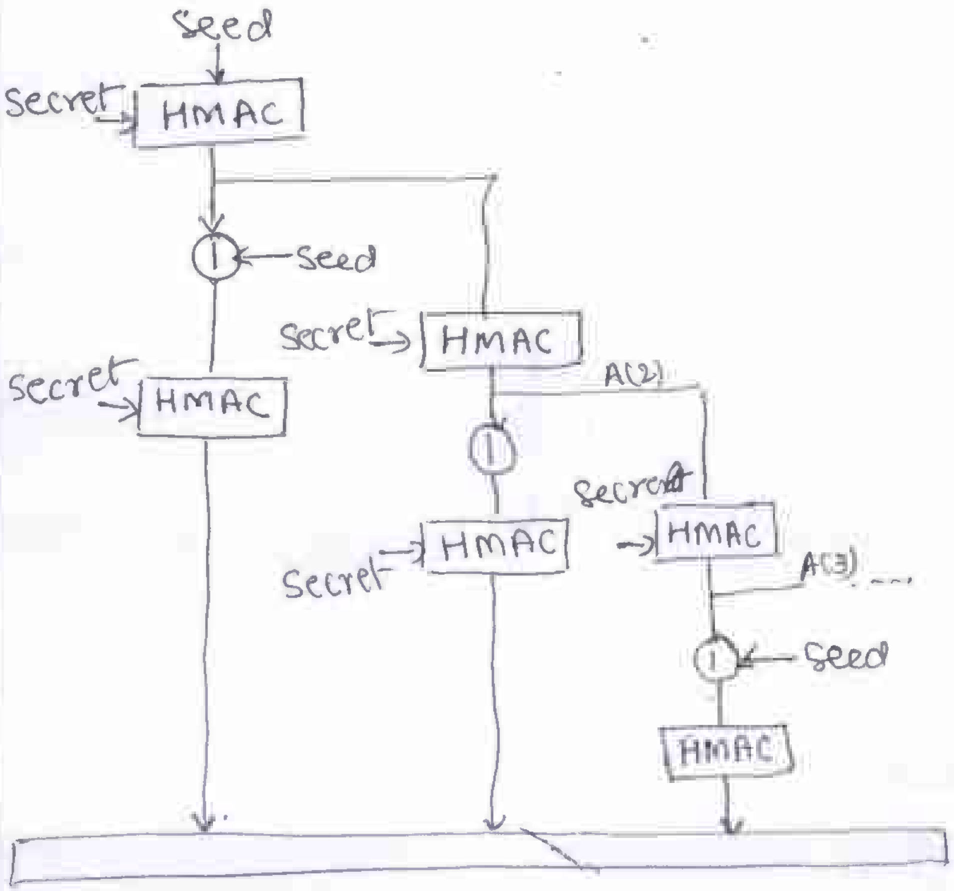
Scheme & Solutions

Subject Title : Network and cyber Security **Subject Code :** 15EC835

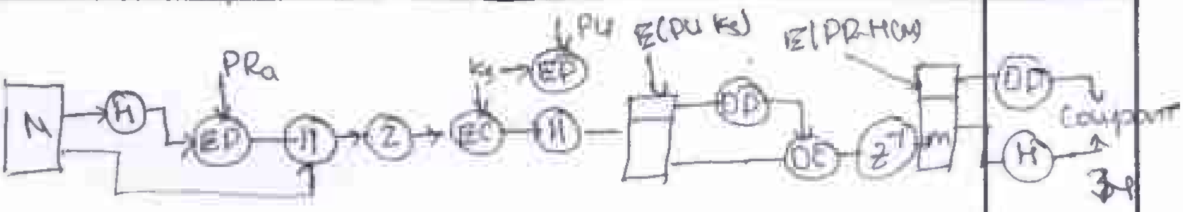
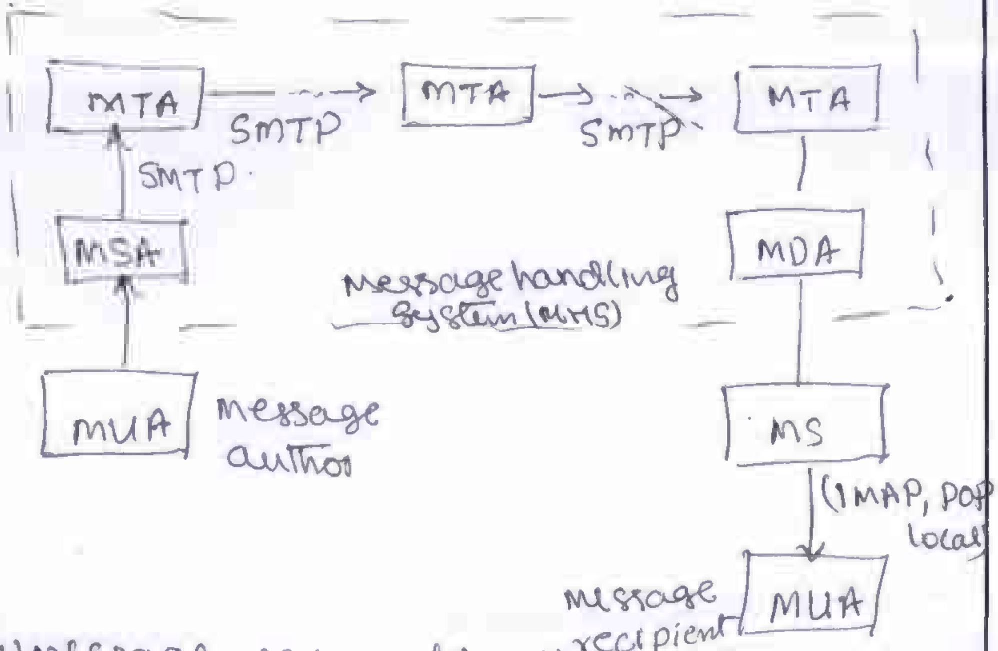
Question Number	Solution	Marks Allocated
1) a)	The SSL Record protocol provides two services for SSL connections. i) confidentiality:- The Handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads. ii) Message integrity:- The Handshake protocol also defines a shared Secrt key that is used to form a message authentication code.	3
	 Application data Fragment compress Add MAC Encrypt SSL record header	5
	Explaindation of the each step of SSL record protocol.	08

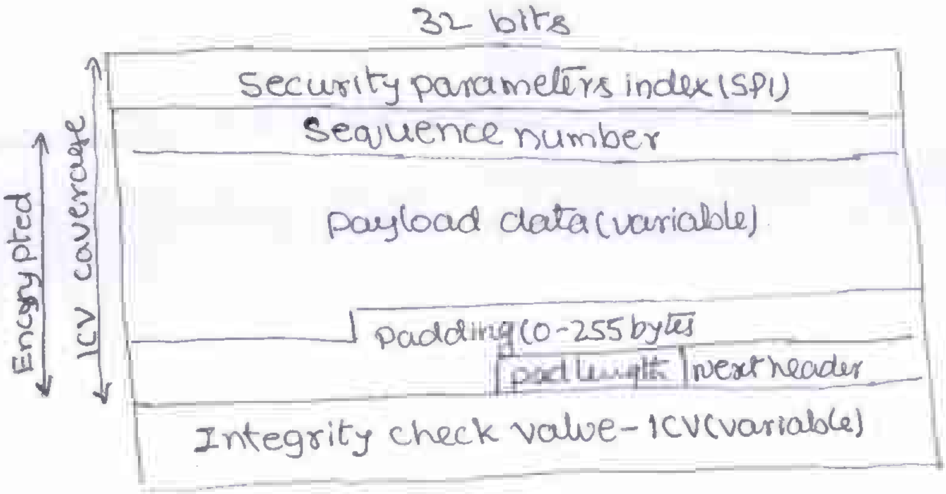
Question Number	Solution	Marks Allocated
b)	The handshake protocol consists of a series of messages exchanged by client and server 1) version (2) Random (3) session ID (4) cipher suite (5) compression methods 6) RSA (7) Fixed Diffie Hellman (8) Ephemeral deffie Hellman (9) Anonymous Diffine Hellman (10) cipher Algorithm (11) MAC Algorithm.	
	Phase-2. server may send certificate, key exchange and reauest certificate. Server signals and hello message phase.	6
	phase-3 Client sends certificate if reauested client sends key exchange. client may send certificate verification. phase-4 change cipher suite and finish handshake protocol.	
	its diagram.	→2.
		08.
2 a)	TLS makes use of a pseudorandom function refered to as PRF to expand secrets into blocks of data for purposes of key generation. The secret value generate longer blocks of data in a secure from the kinds of attacks made on hash functions and MACs. The PRF is based	

Subject Title : **Subject Code :** 15EC835

Question Number	Solution	Marks Allocated
	 Seed Secret HMAC Seed Secret HMAC Secret HMAC A(2) Secret HMAC Secret HMAC A(3) ... Seed HMAC	2
	explaniation of Alert codes. explainaltion of cipher suites. explaination of client certificate types.	6
		08
b)	The user authentication protocol provides the means by which the client is authenticated to the server.	
	(1) message types and formats	2
	(2) SSH_MSG_userauth_Request.	2
	(3) message exchance	2
	(4) Authentication methods. (i) Publickey (ii) password (iii) host based.	2
		08

Subject Title : **Subject Code :** 15EC835

Question Number	Solution	Marks Allocated
3 a)	 N H PRa EP Z Ks EC EP PU E(PU Ks) DP DC Z^{-1} m E(PR H(m)) DP H compare 3	
	explanation of the pgp cryptographic function	6.
		10
b)	1) MIME-version (2) content type (3) content Transfer encoding (4) content ID (5) content -Description.	06.
	OR.	
4 a)	 MTA SMTP MTA SMTP MTA SMTP MSA Message handling System (MHS) MDA MUA Message author MS (IMAP, POP local) MUA Message recipient	3
	1) Message user agent (MUA) 2) Mail submission agent (MSA) 3) message Transfer agent (MTA) 4) mail Delivery agent (MDA) 5) Message Store (MS) } Explanation	7
		10

Question Number	Solution	Marks Allocated
b)	1) MIME-version 2) content-type 3) content-transfer-Encoding 4) content-ID 5) content-Description } explaination.	6.
5 a)	IP Security document categorized roadmap 1) Architecture 2) Authentication Header (AH) 3) Encapsulating Security payload (ESP) 4) Internet key Exchange (IKE) 5) Cryptographic algorithms 6) Others. } Explaination.	6.
b)	IPsec policy is determined primarily by the interaction of two databases. 1) Security association (SAD) database 2) Security policy database (SPD } Explaination.	5 5 10
	OR.	
6) a)	 32 bits Security parameters index (SPI) Sequence number payload data (variable) padding (0-255 bytes pad length next header Integrity check value - ICV (variable) Encrypted ICV coverage	2

Subject Title : **Subject Code :** 15EC835

<table>
<tr><th>Question Number</th><th>Solution</th><th>Marks Allocated</th></tr>
<tr><td></td><td>ESP format contains following fields.
1) security parameters index(32 bits)
2) sequence number (32 bits)
3) payload data(variables)
4) padding(0-255 bytes)
5) pad length (8 bits)
6) Next Header(8 bits)
Explaination</td><td>6</td></tr>
<tr><td></td><td></td><td>8</td></tr>
<tr><td>b)</td><td>Header format for an IKE message.
Bits: 0 8 16 24 31<table>
<tr><td colspan="5">Initiator's Security parameter index(SPI)</td></tr>
<tr><td colspan="5">Responder's security parameter index(SPI)</td></tr>
<tr><td>next payload</td><td>Mjver</td><td>Mnver</td><td>Ex Type</td><td>Flags.</td></tr>
<tr><td colspan="5">Message ID</td></tr>
<tr><td colspan="5">Length</td></tr>
</table></td><td>2</td></tr>
<tr><td></td><td>1) Initiator SPI (64 bits)
2) Responder SPI (64 bits)
3) next payload (8 bits)
4) major version (4 bits)
5) Minor version (4 bits).
6) Exchange types(8 bits)
7) Flags(8 bits).
8) Message ID (32 bits)
9) Length (32-bits)
Explarnation.</td><td>6</td></tr>
<tr><td></td><td></td><td>08.</td></tr>
</table>

Q.No | | Marks

7 a)
1) CISSP
2) DOD
3) A & A,
4) risk management
5) Security controls compliance
6) highly technical person into a policy person
7) Turn a policy person into a highly technical one.

} Explamation.

08

b)
1) network dirce specialist
2) operating system security specialist
3) Database security specialist.
4) System Forensics specialist
5) Reverse Engineering malware specialist

} Explaination

08

OR

8) a)
1) Antipattern name
2) Also known As
3) Refactored solution names
4) unbalanced primal forces
5) Anecdotal Evidence

} head fields.

08

1) Back ground
2) Antipattern solution
3) causes, Symptoms, and conseacuences
4) known exceptions
5) Refactored solution and ~~exp~~ exmples
6) Related Solutions

} body fields.

b)
1) Name
2) Antipattern problem
3) Refactored solution

} explaintaion.

04.

Subject Title : **Subject Code :** 15EC835

Question Number	Solution	Marks Allocated
09) a)	1)This risk exectitive is akey stake holder in investment decisions, in IT. 2) Every decision leading to an IT project and IT system. 3) Developed with visible security reauirement 4) Every organization should have an EA, a blueprint for change. 5) The risk executive uses the EA to assess risks levy security reauirements and ensure continuous monitoring of implementation. 6) To establish an "auditor" user role in the ~~auditors~~ architecture of every system.	06
b)	1) Business Question Analysis 2) Document mining 3) Hierarchy formating 4) Enterprise workshop 5) matrix mining Explaination	10
	OR	
10 a)	1)Position the components on top of the desk 2) connect the monitor pigtail and display cable and secure the thumbscrews, if any. 3) Feed the monitor, mouse and keyboard cables down through a desktop opening, or around the back/side. 4) connect the network, monitor mouse and display ~~through desktop~~ cables to the pedestal 5) For a new ups,	

Subject Title :

Subject Code : 15EC835

Question Number	Solution	Marks Allocated
	6) Connect the pigtail to the pedestal and then conect it to the ups. 7) Always verity work. test the system using boot-able CD/DVD test tools, such as Back track, caine or Helix.	
b)	1) Antivirus 2) Anti spyware 3) Firewall 4) Intrusion detection 5) Intrusion prevention 6) Black listing 7) Real-time integrity checking 8) periodic policy scanning 9) Root kit detection 10) Patch management. Explanation.	8