# Subject Name: Information Security
# Subject Code: 3170720 (OLD)2170709,160702

**Faculties: Ms. Shruti Raval**

## CHAPTER 1

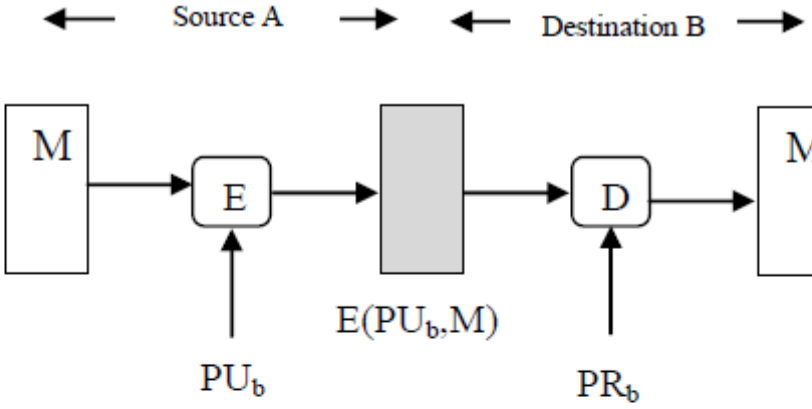
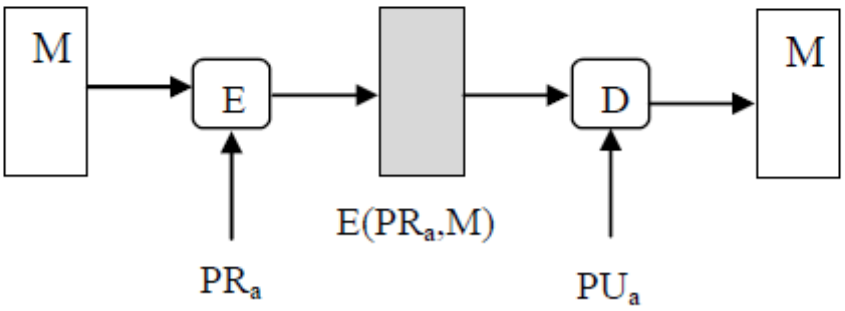
### TOPIC:1 Symmetric Cipher Model, Cryptography

### SHORT QUESTIONS

| | | |
|---|---|---|
| **1** | What do you mean by Cryptographic system.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by Cryptology.**[L.J.I.E.T]** | **01** |
| **3** | Write down two requirements for secure use of conventional encryption.**[L.J.I.E.T]** | **02** |
| **4** | What is the difference between an unconditionally secure cipher and a computationally secure cipher? **(May-2016 OLD)[L.J.I.E.T]** OR When an encryption scheme is said to be unconditionally secure and computationally secure? **(May-2015 OLD)[L.J.I.E.T]** | **02** |
| **5** | _____ Specifies that only the sender and the intended recipient should be able to access the contents of a message. **[L.J.I.E.T]**<br>1. Integrity<br>2. Antivirus<br>3. Confidentiality<br>4. proof of identities<br>5. Availability<br>6. None of the Mentioned | **1** |
| **6** | _____is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction. **[L.J.I.E.T]**<br>1. Information Security<br>2. Database Security<br>3. Network Security<br>4. Physical Security<br>5. Information Security and Cyber Security<br>6. None of the Mentioned | **1** |
| **7** | _____attack attempts to learn or make use of information from the system but does not affect system resources. **[L.J.I.E.T]**<br>1. Passive<br>2. Active<br>3. Digital Signature<br>4. Masquerade<br>5. Replay<br>6. None of the Mentioned | **1** |
| **8** | In order to ensure the security of the Message/information, we need to _____ the data. **[L.J.I.E.T]**<br>1. Decrypt<br>2. Encrypt<br>3. Delete | **1** |

| | | |
|---|---|---|
| | 4. Delete and Encrypt<br>5. None of the Mentioned<br>6. All Mentioned options | |
| **9.** | _____ is a System Design to prevent unauthorized access to or from a Private network. **[L.J.I.E.T]**<br>1. Unauthorized Attacks<br>2. Firewalls<br>3. Virus Attacks<br>4. Fire Attacks<br>5. All Mentioned options<br>6. None of the Mentioned | **1** |
| **10.** | What are the three components of information security? **[L.J.I.E.T]**<br>1. Confidentiality<br>2. Integrity<br>3. Availability.<br>4. Authentication<br>5. None of the Mentioned<br>6. Confidentiality, Integrity, Availability. | **1** |
| **11** | Authentication means _____. **[L.J.I.E.T]**<br>1. Verification of user's identification<br>2. Verification of the data<br>3. Verification of the Sender only<br>4. Verification of the Receiver only<br>5. All Mentioned options<br>6. None of the Mentioned | **1** |
| **12** | Encryption and decryption provide secrecy, or confidentiality, but not _____. **[L.J.I.E.T]**<br>1. Authentication<br>2. Integrity<br>3. Privacy<br>4. Non Repudiation<br>5. Access Control<br>6. None of the Mentioned | **01** |
| **13** | _____is the assurance that someone cannot deny something. **[L.J.I.E.T]**<br>1. Authentication<br>2. Data integrity<br>3. Nonrepudiation<br>4. Data confidentiality<br>5. Access Control<br>6. None of the Mentioned | **01** |

| | | |
|---|---|---|
| **14** | _____Determines who should be able to access what. **[L.J.I.E.T]**<br><br>1. Authentication<br>2. Data Confidentiality<br>3. Data Integrit<br>4. Access Control<br>5. Accountability<br>6. None of the Mentioned | **01** |
| **15** | The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts is called _____. **[L.J.I.E.T]**<br><br>1. Traffic Padding<br>2. Routing Control<br>3. Notarization<br>4. Digital Signature<br>5. Encipherment<br>6. Access Control | **01** |
| **16** | _____is a process that is designed to detect, prevent, or recover from a security attack. **[L.J.I.E.T]**<br><br>1. Security Attack<br>2. Security Service<br>3. Traffic analysis<br>4. Security Mechanism<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| **17** | Provides integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data with recovery attempted is called _____.<br><br>1. Connection Integrity with Recovery<br>2. Connection Integrity without Recovery<br>3. Selective-Field Connection Integrity<br>4. Connectionless Integrity<br>5. Selective-Field Connectionless Integrity<br>6. All Mentioned options | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem. **(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **2** | List and briefly define the security services. **(Nov-2013 OLD)[L.J.I.E.T]**<br>**OR**<br>Describe the term: Authentication, Authorization, Integrity and Non – repudiation.**(Nov-2018 Old)[L.J.I.E.T]** | **03/04** |
| **3** | Explain the conventional security model used for information security **(May-2014 OLD) [L.J.I.E.T] OR** Explain conventional security model used for information security **(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **4** | What is security Services? Explain any three types of security services. **(Nov-2014 OLD) [L.J.I.E.T]** | **07** |
| **5** | What is security mechanism? List and explain various security mechanisms.**(May-2014 OLD)** | **07** |

| | | |
|---|---|---|
| | **[L.J.I.E.T]** | |
| **6** | What are the essential ingredients of a symmetric cipher? **(Oct-2016 OLD) L.J.I.E.T]** | **05** |
| **7** | Explain data confidentiality ,data authentication and non-repudiation. **(Nov-2017 OLD) [L.J.I.E.T]**<br>**OR** Explain data confidentiality ,data authentication and non-repudiation. **(Dec-2018 OLD) [L.J.I.E.T]** | **07** |
| **8** | Explain data confidentiality,data authentication and data integrity. **(May-2016 OLD) [L.J.I.E.T]** | **07** |
| **9** | Briefly explain source repudiation and destination repudiation. **(Nov-2017 OLD)[L.J.I.E.T]** | **03** |
| **10** | Discuss the following terms in brief.**(May-2017 OLD)[L.J.I.E.T]**<br>- authentication - data integrity | **07** |
| **11** | Define the following terms briefly.<br>i) Cryptography ii) Relative Prime Number iii) MAC<br>iv) Digital Signature.**(Nov-2011 OLD)[L.J.I.E.T]** | **04** |
| **12** | What are the essential ingredients of a symmetric cipher?**(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **13** | Which of the following figure provides authentication (only) and which provides confidentiality only? Justify your answer in brief. **(Nov-2017 OLD)[L.J.I.E.T]**<br>  <br><br>**(Figure-1)**<br>  <br><br>**(Figure-2)**<br>Where M is plain text message, E is encryption function, D is decryption function, PRa and PRb are private keys of Source-A and Destination-B respectively while PUa and PUb are public keys of Source-A and Destination-B. | **04** |
| **14** | Explain data confidentiality, data authentication and data integrity.**(May-2018 OLD) [L.J.I.E.T]** | **03** |
| **15** | What is authentication? How it can be done using cryptography?**(May-2018 OLD)(Dec-2018 OLD) [L.J.I.E.T]** | **07** |
| **16** | Which two methods are used to frustrate statistical cryptanalysis?**(May-2019 OLD)** | **03** |

| | | |
|---|---|---|
| | **[L.J.I.E.T]** | |
| **17** | Define following principles of security:<br>1) Confidentiality 2) Integrity 3) Availability**(Nov 2019 OLD)[LJIET]** | **03** |
| **18** | Define the terms: Confidentiality, Data integrity, Non-repudiation. **(Oct 2020 OLD)[LJIET]** | **03** |
| **19** | Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem. **(Oct 2020 OLD)[LJIET]** | **07** |
| **20** | Write the differences between conventional encryption and public key encryption. **(Oct 2020 OLD)[LJIET]** | **03** |
| **21** | Differentiate asymmetric encryption with symmetric encryption. **(Aug 2021 OLD)[LJIET]** | **03** |
| **22** | What is a trap-door one way function? What is its use in cryptography? **(Aug 2021 OLD)[LJIET]** | **03** |
| **23** | Define: Confidentiality, Authenticity and Integrity.**(Jan 2021 OLD)[LJIET]** | **03** |
| **24** | Compare and contrast symmetric key cryptography and asymmetric key cryptography.**(Jan 2021 OLD) [LJIET]** | **03** |
| | **TOPIC:2 Cryptanalysis and Attacks** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Brute-force attack.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by Cryptanalysis.**[L.J.I.E.T]** | **01** |
| **3** | Chosen Plaintext attack means .**[L.J.I.E.T]**<br>1. Adware<br>2. Spyware<br>3. Encryption algorithm, Ciphertext.<br>4. Encryption algorithm, Ciphertext, One or more plaintext-cipher text pairs formed with the secret key.<br>5. Encryption algorithm, Ciphertext, Plaintext message chosen by cryptanalyst<br>6. None of the Mentioned | **01** |
| **4** | Cryptanalysis uses _____. **[L.J.I.E.T]**<br>1. It is basically used to secure the information from unauthorized access.<br>2. Process of converting ordinary plain text into unintelligible text and vice-versa.<br>3. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.<br>4. Mathematical formulas to search algorithm vulnerabilities and break into cryptography.<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| **5** | _____attack attempts to learn or make use of information from the system but does not affect system resources. **[L.J.I.E.T]**<br>1. Passive<br>2. Active<br>3. Digital Signature<br>4. Masquerade<br>5. Replay<br>6. None of the Mentioned | **01** |
| **6** | What do you mean by Brute-force attack? **[L.J.I.E.T]**<br>1. The attacker tries every possible key on a piece of ciphertext until plaintext is obtained. | **01** |

| | | |
|---|---|---|
| | 2. Transforming an intelligible message into one that is unintelligible.<br>3. Retransforming that message back to its original form.<br>4. Types of operations used for transforming plaintext to ciphertext.<br>5. All Mentioned options<br>6. None of the Mentioned | |
| **7** | _____attack attempts to alter system resources or affect their operation. **[L.J.I.E.T]**<br>1. Active<br>2. Passive<br>3. Replay<br>4. Masquerade<br>5. Traffic analysis<br>6. Denial of service. | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain the various types of cryptanalytic attack, based on the amount of information known to the cryptanalyst**..(May-2011 OLD)[LJIET] OR** Define the term cryptanalysis. Explain various types of cryptanalytic attacks(**Dec-2015 OLD)[L.J.I.E.T]** | **04** |
| **2** | What is the objective of attacking an encryption system? Write the two approaches to attack a conventional encryption scheme. **(May-2012 OLD)[L.J.I.E.T]** | **07** |
| **3** | List and explain various types of attacks on encrypted message. **(Dec-2012,Jan-2013 OLD)[L.J.I.E.T]** | **07,07** |
| **4** | Define the terms threat and attack. List and briefly define categories of security attacks. **(Nov-2013 OLD)[L.J.I.E.T]** | **07** |
| **5** | Give examples of replay attacks. List three general approaches for dealing with replay attacks.**(Dec-2015 OLD)[L.J.I.E.T]** | **3.5** |
| **6** | What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.**(Dec-2015 OLD)[L.J.I.E.T]** List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.**(Nov 2013 OLD)[L.J.I.E.T]** | **07,07** |
| **7** | Explain various types of attack on computer system. OR What are the various types of attacks? Explain them in detail.**(May-2014 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **8** | What attacks can be done on encrypted text? Explain them.**(May-2014 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain Different type of Attacks on Crypto System.**(Nov-2018)[L.J.I.E.T]** | **07/04** |
| **9** | Explain cryptanalysis. Discuss any one technique for it.**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **10** | Write a short note on: **(Nov-2016 OLD)[L.J.I.E.T]**<br>i. Cipher text only attack<br>ii. Timing attack. | **03** |
| **11** | Write Short Note on Types of Attacks. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **12** | Briefly explain any two active security attacks. **(May-2017 OLD)[L.J.I.E.T]** | **04** |
| **13** | Discuss the following terms in brief:<br>- brute force attack – cryptography **(May-2017 OLD)[ [L.J.I.E.T]** | **03** |
| **14** | Discuss the following terms in brief:<br>- Passive attack – Cryptanalysis**(Nov-2017 OLD)[L.J.I.E.T]** | **03** |
| **15** | Explain types of Security Attacks. **(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **16** | Explain cryptanalytic attacks with example of any encryption algorithm. **(Nov 2019 OLD)[LJIET]** | **07** |
| **17** | What is brute force attack? Explain with an example. **(Aug 2021 OLD)[LJIET]** | **03** |
| **18** | State the differences between chosen plain text and chosen cipher text attack.**(Jan 2021 OLD)[LJIET]** | **03** |

| | | |
|---|---|---|
| | **TOPIC:3 Substitution and Transposition techniques** | **03** |
| | **SHORT QUESTIONS** | |
| **1** | Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees"**[LJIET]**<br>1. PF IZ TZ EO RT<br>2. LC YO GW BE TR<br>3. PI TU UE FL GX<br>4. PM FL PG MT HK<br>5. GQ WB HQ GP CE<br>6. None of the Mentioned | **1** |
| **2** | Encrypt the Plaintext message "DR GREER ROCKS" with Key "ACBA" using the Hill cipher.**[LJIET]**<br>1. APADJ TFTWLFJ<br>2. SAKNOXAOJNM<br>3. FZIFTOTBXGPO<br>4. TAGZXGSTPOUQ<br>5. ELSCXITQLDNHK<br>6. None of the Mentioned | **1** |
| **3** | _____is a relationship between characters in the plaintext to a character in the ciphertext is one-to-many. **[LJIET]**<br>1. Monoalphabetic Cipher<br>2. Playfair cipher<br>3. Polyalphabetic cipher<br>4. One Time Pad<br>5. Vernam Cipher<br>6. None of the Mentioned | **1** |
| **4** | Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows is called _____.**[LJIET]**<br>1. Rows/Columns Transposition<br>2. One Time Pad<br>3. Rail fence technique<br>4. Vernam Cipher<br>5. Permutation<br>6. None of the Mentioned | **1** |
| **5** | _____replace each letter of the alphabet with the letter standing 3 places further down the alphabet.**[LJIET]**<br>1. Monoalphabetic Substitution Cipher<br>2. Playfair Cipher<br>3. Hill Cipher<br>4. Caesar cipher<br>5. Vigenère cipher<br>6. Vernam Cipher | **01** |
| **6** | Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees" **[LJIET]**<br>1. PF IZ TZ EO RT<br>2. LC YO GW BE TR<br>3. PI TU UE FL GX<br>4. PM FL PG MT HK<br>5. GQ WB HQ GP CE<br>6. None of the Mentioned | **01** |

| | DESCRIPTIVE QUESTIONS | |
|---|---|---|
| **1** | Which two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext?**(May-2015 OLD)[L.J.I.E.T]** | **02** |
| **2** | Define the Caesar cipher. **(May-2012 OLD)[L.J.I.E.T]** | **03** |
| **3** | Explain the one time pad scheme. **(May-2012 OLD)[L.J.I.E.T]** | **03** |
| **4** | Describe mono alphabetic cipher.**(Nov-2017 OLD)[ L.J.I.E.T ]** OR Which type of substitution is called monoalphabetic substitution cipher?**(May-2015 OLD) [L.J.I.E.T]** OR What is cipher? Explain any two mono alphabetic cipher.**(May-2018 OLD)[L.J.I.E.T]** | **01/07** |
| **5** | Is playfair cipher monoalphabetic cipher? Justify. Construct a playfair Matrix with the key "moonmission" and encrypt the message "greet". **(May-2013 OLD)[L.J.I.E.T]** | **03** |
| **6** | Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees"**(May-2011 OLD) (Nov-2013 OLD)[L.J.I.E.T]** | **04** |
| **7** | Construct 5 X 5 playfair matrix for the keyword "OCCURANCE". **(Nov-2011 OLD)[L.J.I.E.T]** | **03** |
| **8** | Construct a Playfair matrix with the key "engineering". And encrypt the message "test this process". **(May-2012 OLD)[L.J.I.E.T]** | **04** |
| **9** | Let the keyword in playfail cipher is "keyword". Encrypt a message "come to the window" using playfair cipher. **(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **10** | Explain play fair cipher with suitable example.**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **11** | Encrypt the following message using playfair cipher. Message: COMSEC means communications securityKeyword: Galois. **(Oct-2016 OLD) [L.J.I.E.T]** | **05** |
| **12** | What are the problems with one-time pad?**(Oct-2016 OLD)[L.J.I.E.T]** | **02** |
| **13** | Using playfair cipher encrypt the plaintext "Why, don't you?". Use the key "keyword".**(Dec-2015 OLD)[ L.J.I.E.T]** | **07** |
| **14** | Explain generation of encryption matrix in play fair cipher. **(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **15** | Use playfair algorithm with key "monarchy" and encrypt the text "jazz".**(May-2015 OLD) [L.J.I.E.T]** | **04** |
| **16** | Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext.<br>Key = ENGINEERING<br>Plaintext=COMPUTER**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **17** | ExplainPlayfair Cipher in detail. Find out cipher text for the following given plain text and key.<br>Key = GOVERNMENT<br>Plain text = PLAYFAIR**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **18** | Encrypt the message "Good morning" and "Exam" using the Hill Cipher with the key<br>**9** 4<br>5 7<br>**(May-2011 OLD)(Dec-2015 OLD)[L.J.I.E.T]**<br>**OR**<br><br>Encrypt the message "meet me at the usual place " using the Hill cipher using key<br>9 4<br>5 7<br>**(Nov-2018 OLD)[L.J.I.E.T]**<br><br>**OR**<br><br>Encrypt the message "Exam" using the Hill cipher with the key. **(May-2015 OLD)[L.J.I.E.T]**<br>9 4<br>5 7 | **04/07** |

| | | |
|---|---|---|
| | . | |
| **19** | Write a brief note on hill cipher. **(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **20** | Explain monoalphabetic cipher and polyalphabetic cipher by giving an example.**(Nov-2013 OLD, Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **21** | Explain Vegenere Cipher.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **22** | Explain generation of encryption matrix in play fair cipher.**(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **23** | What is symmetric key cryptography? What are the challenges of symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **24** | Explain one time pad cipher with example. **(Nov-2017 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **25** | Explain one time Pad in detail. What are the practical issues of this algorithm?**(Oct-2016 OLD)(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **26** | Explain one time pad cipher with example.**(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **27** | Consider the scenario where user A wants to send bulk data (data is in GBs) to user B using networking. Data exchange has to be done in confidential manner. The key which is used for encryption can be intercepted by an attacker. Which is the most efficient and protected way to achieve secure communication? Justify your answer in detail.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **28** | Write a short note on “Hill Cipher”.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **29** | Use Hill cipher to encrypt the text DEF. The key to be used is<br>2 4 5<br>9 2 1<br>3 8 7. **(Dec-2015 OLD)[L.J.I.E.T]** | **05** |
| **30** | Differentiate public key cryptography and symmetric key cryptography. Explain any one substitution method for symmetric key cryptography.**(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **31** | Differentiate mono alphabetic and poly alphabetic substitution method. Vigenere cipher with example. **(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **32** | Explain Columnar Transposition cipher with example.**(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **33** | Explain rail fence transposition technique with example. **(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **34** | Explain rail fence Cipher technique.**(May-2016 OLD, Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **35** | Explain columnar transposition Cipher technique. **(Nov 2017 OLD)(May-2018)[L.J.I.E.T]** | **07** |
| **36** | Explain working of two wheel rotor machine. **(Nov 2017 OLD)[L.J.I.E.T]** | **07** |
| **37** | Write differences between substitution techniques and transposition techniques. **(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **38** | Explain transposition techniques with appropriate example.**(Nov 2017 OLD)[L.J.I.E.T]** | **07** |
| **39** | Explain playfair cipher with example.**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **40** | Apply Caesar cipher to encrypt and decrypt the message “ashish”. Use key value 12.**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **41** | Given key K=<br>17 17 05<br>21 18 21<br>02 02 19<br>and plaintext =”ney”. Find out the ciphertextapplying Hill Cipher. Is Hill cipher strong against ciphertext only attackor known plaintext attack? Justify the answer.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **42** | How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key “hidden” and encrypt the message “Message” using playfair cipher.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **43** | Explain the rail fence cipher. Why a pure transposition cipher is easily recognized?**(May-2019 OLD)[L.J.I.E.T]** | **03** |
| **44** | Encrypt Message "Secure" using Hill Cipher with key<br>[17 10<br>23 19]**(May-2019 OLD)[L.J.I.E.T]** | **07** |

| | | |
|---|---|---|
| **45** | Encrypt the given message using playfair cipher.**(May-2019 OLD)[L.J.I.E.T]**<br>Message : GOOD MORNING<br>Key : GTU EXAMS | **07** |
| **46** | Encrypt the Message "Surgical Strike" with key "GUJAR" using PLAYFAIR technique.**(Nov-2018 OLD)[L.J.I.E.T]** | **04** |
| **47** | Explain the VERNAM Cypher method.**(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **48** | (1)Encrypt the text "trust" using Caesar Cipher with key=25<br>(2)Compare the strength of mono-alphabetic ciphers to poly-alphabetic ciphers.(**Dec-2019 OLD)[L.J.I.E.T]** | **02** |
| **49** | Describe Rail-fence cipher algorithm with example. **(Nov 2019 OLD)[LJIET]** | **04** |
| **50** | Explain one time pad algorithm with example and mention its strength and Weakness. **(Nov 2019 OLD)[LJIET]** | **03** |
| **51** | What is the difference between a mono alphabetic cipher and apolyalphabetic cipher?**(Nov 2019 OLD)[LJIET]** | **04** |
| **52** | Encrypt the message "GTU Examination"?**(Nov 2019 OLD)[LJIET]**<br>using the Hill cipher algorithm with the key matrix<br>[5 17<br>4 15]. Show your calculations and the result. | **07** |
| **53** | Perform encryption in Playfair Cipher algorithm with plain text as"INFORMATION AND NETWORK SECURITY", Keyword is"MONARCHY". (Note: 1.Put j and i both combine as a single field in 5*5matrix).**(Nov 2019 OLD)[LJIET]** | **07** |
| **54** | Construct a Playfair matrix with the key "engineering". And encrypt the message "impossible". **(Oct 2020 OLD)[LJIET]** | **04** |
| **55** | Write a note on Hill Cipher. **(Oct 2020 OLD)[LJIET]** | **04** |
| **56** | Using the Vigenère cipher, encrypt the word "ATTACKATDAWN" using the key "LEMON".**(Oct 2020 OLD)[LJIET]** | **03** |
| **57** | Let the keyword in playfair cipher is "keyword". Encrypt a message "come to the window" using playfair cipher. **(Aug 2021 OLD)[LJIET]** | **04** |
| **58** | Explain Playfair cipher technique in detail. Find cipher text for plain text 'GTUINSEXAM' using 'STUDY' as key. **(Jan 2021 OLD)[LJIET]** | **07** |
| | **CHAPTER 2** | |
| | **TOPIC:1 Stream ciphers and block ciphers, Block Cipher structure** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Stream Cipher.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by Block Cipher.**[L.J.I.E.T]** | **01** |
| **3** | What is the difference between differential and linear cryptanalysis?**(Oct-2016 OLD) [L.J.I.E.T]** | **02** |
| **4** | Explain the terms diffusion and confusion. OR Define the term – confusion, diffusion.**(May-2011 OLD)(Dec-2015 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain the difference between diffusion and confusion.**(Nov-2018 OLD)[L.J.I.E.T]** | **02/03** |
| **5** | What is the difference between a block cipher and a stream cipher? **(Oct-2016 OLD) [L.J.I.E.T]** | **02** |
| **6** | Which of the following statements are true?**[L.J.I.E.T]**<br>i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption<br>ii) The CTR mode does not require an Initialization Vector<br>iii) The last block in the CBC mode uses an Initialization Vector<br>iv) In CBC mode repetitions in plaintext do not show up in ciphertext<br>1. iii)<br>2. ii) and iv) | **01** |

| | | |
|---|---|---|
| | 3. All the Statements are true<br>4. I and ii and iv<br>5. I<br>6. None | |
| **7** | Which of the following modes does not implement chaining or "dependency on previous stage computations"?**[L.J.I.E.T]**<br>1. CTR, ECB<br>2. CTR, CFB<br>3. CFB, OFB<br>4. ECB, OFB<br>5. CBC,OFB<br>6. OFB,CTR | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Draw and explain Feistel's structure for encryption and decryption. . **(Nov-2011 OLD)(Dec-2015 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain Feistel Cipher Structure with respect to its design features. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **3** | The exact realization of Feistel network depends on the choice of which parameters?**(May-2012 OLD)[L.J.I.E.T]** | **03** |
| **4** | Why is it important to study the Feistel cipher? **(Oct-2016 OLD)[L.J.I.E.T]** | **05** |
| **5** | What are the differences between stream cipher and block cipher?**(Nov-2017 OLD)[L.J.I.E.T]**<br>**OR**<br>Differentiate block cipher and a stream cipher.**(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **6** | State the principles for block cipher design and explain in detail. (**Dec-2019 OLD)[L.J.I.E.T]** | **07** |
| **7** | Differentiate block cipher and stream cipher algorithm with example. **(Nov-2019 OLD) [L.J.I.E.T]** | **04** |
| | **TOPIC:2 Data Encryption standard (DES) with example, strength of DES** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Avalanche Effect.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean Timing Attacks.**[L.J.I.E.T]** | **02** |
| **3** | It takes input 48-bits from XOR operation and generate 32-bits using 8 substitution boxes is called _____.**[L.J.I.E.T]**<br>1.P-Box Permutation<br>2.XOR and Swap<br>3.Expansion Permutation<br>4.S-box Substitution<br>5.Key Transformation<br>6.None of the Mentioned | **01** |
| **4** | _____ is an attack that uses a fake identity to gain unauthorized access to personal information. **[L.J.I.E.T]**<br>1. Masquerade attack<br>2. One Time Pad<br>3. Authentication<br>4. Integrity<br>5. Modification of messages<br>6. None of the Mentioned. | **01** |
| **5** | Find The False Statement in the following options. **[LJIET]**<br>1. In Modern Cryptography, Symmetric Key Algorithms Use Same Key Both For | **01** |

| | | |
|---|---|---|
| | Encryption And Decryption.<br>2. The Symmetric Cipher DES (Data Encryption Standard) Was Widely Used In The Industry For Security Product.<br>3. The AES (Advanced Encryption Standard) Cryptosystem Allows Variable Key Lengths Of Size 56 Bits And 124 Bits.<br>4. Public Key Algorithms Use Two Different Keys For Encryption And Decryption.<br>5. All Mentioned options<br>6. None of the Mentioned | |
| **6** | Data Encryption Standard (DES) algorithm uses a _____ key a _____ key is used in AES. **[LJIET]**<br>1. 56-bit and 128 bit<br>2. 128 bit and 56 bit<br>3. 64 bit and 56 bit<br>4. 48 bit and 64 bit<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| **7** | DES follows _____.**[LJIET]**<br>1. Hash Algorithm<br>2. Caesars Cipher<br>3. Feistel Cipher Structure<br>4. SP Networks<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| **8** | It takes input 48-bits from XOR operation and generate 32-bits using 8 substitution boxes is called _____.**[LJIET]**<br>1. P-Box Permutation<br>2. XOR and Swap<br>3. Expansion Permutation<br>4. S-box Substitution<br>5. Key Transformation<br>6. None of the Mentioned | **01** |
| **9** | The acronym DES stands for _____. **[LJIET]**<br>1. Digital Evaluation System<br>2. Digital Encryption Standard<br>3. Digital Encryption System<br>4. Double Encryption Standard<br>5. Data Encryption Standard<br>6. None of the Mentioned | **01** |
| **10** | DES works by using_____. **[LJIET]**<br>1. Permutation and substitution on 64 bit blocks of plain text. | **01** |

| | | |
|---|---|---|
| | 2. Only permutations on blocks of 128 bits.<br>3. Exclusive XORing key bits with 64 bit blocks.<br>4. 4 rounds of substitution on 64 bit blocks with 56 bit keys.<br>5. Only permutations on blocks of 60 bits<br>6. None of the Mentioned | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | What is the purpose of S-boxes in DES? **(Oct-2016 OLD)[LJIET] OR** Explain the avalanche effect.**(May-2011 OLD)[LJIET] OR** What is S Box? How it works? **(May-2018 OLD)[L.J.I.E.T]** | **03/05** |
| **2** | Explain single round function of DES with suitable diagram. . **(Nov-2011 OLD )(Dec-2015 OLD)[L.J.I.E.T] OR**Draw and explain the single round of DES algorithm**(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **3** | Discuss Data Encryption Standard with neat sketches. **(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain scheme for DES encryption.**(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **5** | Explain Avalanche effect in DES. **(Nov-2017 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain Avalanche Effect.**(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **6** | What is meant by meet-in-the-middle attack in double DES? Explainthe same in brief.**(Nov-2017 OLD)[L.J.I.E.T]**<br>**OR**<br>How meet in the middle attack is performed on double DES?**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| **7** | Explain the DES encryption algorithm.OR Write a short note on DES. **(May-2012 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **8** | Explain Sub key generation Process in Simplified DES algorithm with Example. Explain Modes of Operations.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **9** | Explain DES key generation process in detail.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **10** | Explain DES algorithm with Figure. Explain Modes of Operations.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **11** | Define the terms diffusion and confusion. What is the purpose of S-box in DES? Explain the avalanche effect in DES.**(Nov-2013 OLD)[L.J.I.E.T]**<br>**OR** What is the purpose of S-box in DES? Explain the avalanche effect in DES.**(Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **12** | Explain limitation of DES in detail.**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **13** | Explain The Strength of DES. **[L.J.I.E.T]** | **07** |
| **14** | What is the purpose of S-boxes in DES?**(Oct-2016 OLD)[L.J.I.E.T]** | **05** |
| **15** | Explain simplified DES method with example. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **16** | Explain single round of DES.**(Nov-2017 OLD)[L.J.I.E.T] or** Explain single round of DES algorithm. Support your answer with neat sketches. OR Draw and explain simplified model of DES.**(May-2018 OLD)(Dec-2015 OLD)(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **17** | Explain triple DES with two keys. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **18** | Explain avalanche effect in DES and discuss strength of DES in brief. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **19** | With example explain function of s-box in DES. **(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **20** | What are the various mode of operation of DES?**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **21** | Explain double and triple DES.**(May-2018 OLD)[L.J.I.E.T]** | **04** |
| **22** | Explain how DES(Data Encryption standard) algorithm observes Fiestelstructure. Explain key generation and use of S-box in DES algorithm.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **23** | Explain Data Encryption Standards Algorithm with diagram.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **24** | Discuss in detail encryption and decryption process of DES. **(Nov-2018 OLD)[L.J.I.E.T]** | **07** |

| | | |
|---|---|---|
| **25** | Explain S-DES with necessary block diagram. **(Dec 2019 OLD)[LJIET]** | **07** |
| **26** | Draw block diagram to show Broad level steps in DES and also give stepsof one round in DES with another diagram. **(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **27** | What is a meet-in-the-middle attack in double DES?**(Nov-2019 OLD)[L.J.I.E.T]** | **04** |
| **28** | Explain the steps involved in International data encryption standard algorithm**(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **29** | Explain the key generation in DES algorithm. **(Oct 2020 OLD)[L.J.I.E.T]** | **07** |
| **30** | What is the purpose of the S-boxes in DES? Explain the avalanche effect. **(Oct 2020 OLD)[L.J.I.E.T]** | **03** |
| **31** | Define the terms: Diffusion, Confusion. How are these implemented in DES? **(Aug 2021 OLD)[L.J.I.E.T]** | **04** |
| **32** | Explain the single round of DES algorithm. **(Aug 2021 OLD)[L.J.I.E.T]** | **07** |
| **33** | Discuss Avalanche effect and Completeness property of a block cipher. **(Jan 2021 OLD)[L.J.I.E.T]** | **04** |
| **34** | Explain the process of key generation in DES.**(Jan 2021 OLD)[L.J.I.E.T]** | **04** |
| **35** | Draw a detailed block diagram of encryption process in DES. Add appropriate description. **(Jan 2021 OLD)[L.J.I.E.T]** | **07** |
| **36** | Briefly explain Triple DES with two keys.**(Jan 2021 OLD)[L.J.I.E.T]** | **03** |
| | **TOPIC:3 Design principles of block cipher** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write down the design criteria for the S-boxes.**[L.J.I.E.T]** | **07** |
| **2** | Write down the design criteria for Permutation.**[L.J.I.E.T]** | **03** |
| | **TOPIC:4 AES with structure, its transformation functions** | |
| | **SHORT QUESTION** | |
| **1** | For the AES-128 algorithm there are _____ similar rounds and _____ round is different. **[L.J.I.E.T]**<br>1. 2 pair of 5 similar rounds, every alternate<br>2. 9 , the last<br>3. 8 , the first and last<br>4. 10 , no<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| **2** | How many rounds does the AES-192 perform?**[L.J.I.E.T]**<br>1. 10<br>2. 12<br>3. 4<br>4. 16<br>5. 25<br>6. None of the Mentioned | **01** |
| **3** | AES the 4×4 bytes matrix key is transformed into a keys of size _____.**[L.J.I.E.T]**<br>1. 32 words<br>2. 64 words<br>3. 54 words<br>4. 44 words<br>5. None of the Mentioned.<br>6. All Mentioned options. | **01** |
| **4** | How to generate the Rotword? **[L.J.I.E.T]**<br>1. It performs an onebyte circular left shift on a word.<br>2. It performs a twobyte circular left shift on a word. | **01** |

| | | |
|---|---|---|
| | 3. It performs a Three byte circular left shift on a<br>4. Word.<br>5. It performs a one byte circular left shift and a three byte circular leftshift on a word.<br>6. None of the Mentioned.<br>7. All Mentioned options. | |
| **5** | What is the output of following AddRoundKey in AES Algorithm?<br><br>32 + (XOR) 2b= _____**[L.J.I.E.T]**<br><br>1. e9<br>2. 9a<br>3. a0<br>4. 19<br>5. 9a and a0<br>6. None of the Mentioned. | **01** |
| **6** | What do you mean by SubWord? **[L.J.I.E.T]**<br><br>1. PerformsSubstitution on each byte of its input word, using the S-box.<br>2. XORed with a round constant and Rcon.<br>3. Performs a onebyte circular left shift on a word.<br>4. Perform Substitution and Permutation.<br>5. None of the Mentioned.<br>6. All Mentioned options. | **01** |
| **7** | On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function? **[L.J.I.E.T]**<br><br>1. f function<br>2. permutation p<br>3. swapping of halves<br>4. XOR of subkey with function f<br>5. None of the Mentioned<br>6. All Mentioned options. | **01** |
| **8** | The input 128 bit block, this block is arranged in the form of 4 X 4 square matrix of bytes. This block is copied into the _____. **[L.J.I.E.T]**<br><br>1. state array<br>2. Array<br>3. Table<br>4. Block<br>5. Row<br>6. None of the Mentioned | **01** |
| **9** | The AES key expansion algorithm takes as input a _____(16-byte) key and produces a linear array of _____. **[L.J.I.E.T]**<br><br>1. Six word and 40 words<br>2. Four word and 39 words | **01** |

| | | |
|---|---|---|
| | 3. Five word and 42 words<br>4. Four word and 44 words<br>5. Five word and 41 words<br>6. None of the Mentioned | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write down evaluation criteria for AES.**[L.J.I.E.T]** | **07** |
| **2** | Explain working of AES.**(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **3** | Explain ShiftRows Transformation in detail.**[L.J.I.E.T]** | **04** |
| **4** | Explain MixColumns Transformation.**[L.J.I.E.T]** | **04** |
| **5** | Explain Byte substitution and Shift row operation of AES in detail.**( Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **6** | Explain four stages of a single round in AES. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **7** | Elaborate AES encryption with neat sketches. **(May-2017 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain four different stages of AES(Advance Encryption standard)structure.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **8** | Explain AES encryption in detail.**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **9** | Explain various steps of AES in short. **(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **10** | Describe various steps of AES.**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **11** | Discuss in detail encryption and decryption process of AES.**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **12** | Briefly describe Mix Columns and Add Round Key in AES algorithm.**(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **13** | Explain the key generation in AES algorithm. **(Oct 2020 OLD)[L.J.I.E.T]** | **07** |
| **14** | What is the purpose of the State array? How many bytes in State are affected by ShiftRows? **(Oct 2020 OLD)[L.J.I.E.T]** | **03** |
| **15** | Briefly explain the AES encryption structure and discuss its transformation functions. **(Aug 2021 OLD)[L.J.I.E.T]** | **07** |
| | **CHAPTER 3** | |
| | **TOPIC:1 Multiple encryption and triple DES** | |
| | **SHORT QUESTIONS** | |
| **1** | How many keys are used in triple encryption?**(Oct-2016 OLD) [LJIET]** | **02** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain Double DES. And Meet-in-the-Middle Attack in detail.**[L.J.I.E.T]** | **07** |
| **2** | Explain Triple DES with Two and Three Keys.**[L.J.I.E.T]** | **07** |
| **3** | Explain the triple DES scheme with two keys and write about proposed attacks on 3DES.**(May-2012 OLD)[L.J.I.E.T]** | **04** |
| | **TOPIC:2 Block Cipher Modes of Operation** | |
| | **SHORT QUESTIONS** | |
| **1** | What about encrypting plaintext longer than b bits in Block Cipher?**[L.J.I.E.T]**<br>1. Operates on fixed length b-bit input to produce b-bit ciphertext.<br>2. Break plaintext into b-bit blocks (padding if necessary) and apply cipher on each block.<br>3. Plaintext handled one block at a time and each block of plaintext is encrypted using the same key.<br>4. It operates on different length.<br>5. All Mentioned options.<br>6. None of the Mentioned. | **01** |
| **2** | The contents of the shift register are shifted left by s bits, and C1 is placed in the rightmost (least significant) s bits of the shift register. | **01** |

| | | |
|---|---|---|
| | In which Block Cipher Mode Operation Above statement is used.<br>Electronic Code Book (ECB) **[L.J.I.E.T]**<br>1. Cipher Block Chaining (CBC)<br>2. Cipher Feedback (CFB)<br>3. Output Feedback (OFB)<br>4. Counter (CTR)<br>5. None of the Mentioned<br>6. Electronic Code Book (ECB) | |
| **3** | In OFB Transmission errors do not propagate: only the current ciphertext is affected, since keys are generated "locally". **[L.J.I.E.T]**<br>1. True<br>2. False<br>3. May be<br>4. Can't say<br>5. None of the Mentioned<br>6. True and May be | **01** |
| **4** | Which mode requires the implementation of only the encryption algorithm?**[L.J.I.E.T]**<br>1. ECB<br>2. CBC<br>3. CTR<br>4. OFB<br>5. ECB and CTR<br>6. None of the Mentioned | **01** |
| **5** | A _____ is one that encrypts a data stream one bit or one byte at a time **[L.J.I.E.T]**<br>1. Stream cipher<br>2. Block cipher<br>3. Feistel Cipher<br>4. All Mentioned options<br>5. Stream cipher and Block cipher<br>6. None of the Mentioned | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Why mode of operation is defined? Explain the simplest mode for block cipher modes of operation?**(May-2011 OLD)[L.J.I.E.T]** | **04** |
| **2** | List various modes of operations of block cipher. Explain any three of them briefly**. (Nov-2011 OLD, Dec 2018 OLD)[L.J.I.E.T]** | **07** |
| **3** | List and explain various block cipher modes of operation with the help of diagram.**(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **4** | Why mode of operation is defined? Explain the block cipher modes of operation**? (Nov-2013 OLD)[L.J.I.E.T]** | **07** |
| **5** | Define Block Cipher. Explain Design Principles of block cipher. **(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **6** | Explain Modes of Operations.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **7** | What is the limitation of Electronic Codebook Mode (ECB)? How it is overcome by Cipher Block Chaining (CBC) mode? Also explain CBC mode in detail. **(Oct-2016 OLD)(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **8** | Discuss Electronic code book and cipher feedback mode with neat diagrams.**(May-2017 OLD)[L.J.I.E.T]** | **07** |

| | | |
|---|---|---|
| **9** | Explain cipher feedback mode of operation..**(May-2015 OLD)[L.J.I.E.T]** OR Explain cipher feedback mode of DES operation **(May-2018 OLD)[L.J.I.E.T]** | **04/07** |
| **10** | Explain block cipher mode of operation. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **11** | Explain block cipher design principles. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **12** | Discuss the following block cipher modes of operation in detail with neat sketches:<br>- Cipher block chaining mode<br>- Counter mode**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **13** | Explain counter mode of DES operation.**(May-2018 OLD)[L.J.I.E.T]** | **04** |
| **14** | (i) Explain working of ECB.Why ECB (Electronic code book)is rarely used to encrypt message?<br>(ii) Why CFB(Cipher feedback mode) encrypted messages areless subject to tampering than OFB(Output feedback mode)?**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **15** | What is the limitation of Electronic Codebook Mode (ECB)? explain CBC mode in detail. **(Dec 2018 OLD)[L.J.I.E.T]** | **07** |
| **16** | Explain Modes of Algorithm. **(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **17** | Explain CFB algorithm mode with diagram. **(Nov 2019 OLD) [LJIET]** | **03** |
| **18** | Explain Counter (CTR) algorithm mode with diagram.**(Nov 2019 OLD) [LJIET]** | **03** |
| **19** | Explain Modes of Operations.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **20** | Explain Cipher Block Chaining (CBC) and Electronic Code Book (ECB) block cipher modes of operation with the help of diagram. **(Oct 2020 OLD)[LJIET]** | **04** |
| **21** | Explain Cipher Feedback (CFB) and Output Feedback mode (OFB) block cipher modes of operation with the help of diagram. **(Oct 2020 OLD)[LJIET]** | **04** |
| **22** | Why mode of operation is defined for block ciphers? Compare the block cipher modes of operation?**(Aug 2021 OLD)[LJIET]** | **07** |
| | **CHAPTER 4** | |
| | **TOPIC 1: Public Key Cryptosystems with Applications** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Public key Cryptography.**[L.J.I.E.T]** | **01** |
| **2** | List the Application of Public-Key Cryptosystem.**[L.J.I.E.T]** | **01** |
| **3** | A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?**[L.J.I.E.T]**<br>1. Sender encrypts using receiver's private key<br>2. Sender does not encrypt the message<br>3. Receiver does not decrypt the message<br>4. Receiver decrypts using his own private key<br>5. None of the Mentioned<br>6. All Mentioned options. | **01** |
| **4** | A digital signature needs a _____.**[L.J.I.E.T]**<br>1. Private-key system<br>2. Shared-key system<br>3. Public-key system<br>4. All Mentioned options.<br>5. Private-key and public-key<br>6. None of the Mentioned | **01** |
| **5** | In Message Confidentiality, transmitted message must make sense to only intended _____.**[L.J.I.E.T]**<br>1. Receiver<br>2. Sender | **01** |

| | | |
|---|---|---|
| | 3. Modulator<br>4. Translator<br>5. Modulator and Translator<br>6. None of the Mentioned | |
| **6** | Public key system is useful because **[L.J.I.E.T]**<br>1. It uses two keys.<br>2. There is no key distribution problem as public key can be kept in a commonly accessible database.<br>3. Private key can be kept secret.<br>4. it is a symmetric key system<br>5. It uses four keys.<br>6. None of the Mentioned | **01** |
| **7** | In RSA Find n, φ(n),d for p=11 and q= 5 and e=7 **[L.J.I.E.T]**<br>1. N=55,φ(n)=40,d=23<br>2. N=11, φ(n)=39,d=17<br>3. N=18, φ(n)=35,d=19<br>4. N=45, φ(n)=90,d=21<br>5. N=7, φ(n)=65,d=9<br>6. None of the Mentioned | **01** |
| **8** | In public key encryption system if A encrypts a message using his private key and sends it to B **[L.J.I.E.T]**<br>1. if B knows it is from A he can decrypt it using A's public key<br>2. Even if B knows who sent the message it cannot be decrypted<br>3. It cannot be decrypted at all as no one knows A's private key<br>4. A should send his public key with the message<br>5. All Mentioned options<br>6. None of the Mentioned | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write the differences between conventional encryption and public key encryption.**(May-2011 OLD)[L.J.I.E.T] OR** Compare conventional encryption with public key encryption. **(Nov-2013 OLD)[L.J.I.E.T]** | **04** |
| **2** | List the requirements of Public Key Cryptography.**(Nov-2017 OLD)[L.J.I.E.T]** | **03** |
| **3** | Differentiate Symmetric and Asymmetric key cryptography. **(Nov-2011 OLD)[L.J.I.E.T] OR**<br>Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.**(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **4** | Compare public key and private key cryptography. Also list various algorithms for each.**(May-2014 OLD)[LJIET]**OR Compare public key cryptography with private key cryptography. **(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **5** | What is public key cryptography? Compare public it with conventional cryptography.**(Jan-2013 OLD)(Oct-2016 OLD)[L.J.I.E.T]** | **07** |
| **6** | What is cryptography? Briefly explain the model of Asymmetric Cryptosystem.**(Nov-2013 OLD, Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **7** | What are the principal elements of public-key cryptosystem? Explain in brief.**(May-2017 OLD)** | **07** |

| | | |
|---|---|---|
| | **(Oct-2016 OLD)[L.J.I.E.T]** | |
| **8** | Explain various general categories of schemes for the distribution of public keys.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **9** | Explain various general categories of schemes for the distribution ofpublic keys.**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **10** | What is a trap-door one-way function? What is its importance inpublic key cryptography?**(Nov-2013 OLD)[L.J.I.E.T]** | **03** |
| **11** | Explain public-key cryptosystem in detail.**(Dec-2018 OLD)** | **07** |
| **12** | Compare Symmetric Key Algorithm with Asymmetric Key Algorithm. **(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **13** | What are the principal elements of a public-key cryptosystem?**(Nov 2019 OLD)[LJIET]** | **03** |
| **14** | Explain public key cryptosystem with neat diagram. **(Jan 2021 OLD)[LJIET]** | **04** |
| | **TOPIC 2: Requirements and Cryptanalysis** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Requirements for Public-Key Cryptography. **[L.J.I.E.T]** | **07** |
| **2** | Which cryptanalytic attack can occur on Public-Key Cryptography.**[L.J.I.E.T]** | **03** |
| | **TOPIC 3: RSA algorithm, its computational aspects and security** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by RSA?**[L.J.I.E.T]** | **01** |
| **2** | List types of attacks done on RSA.**[L.J.I.E.T]** | **01** |
| **3** | In the RSA public key cryptosystem, the private and public keys are (e,n) and (d,n) respectively, where n=p*q and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that 0<M<n and Φ(n) = (p-1)(q-1). Now consider the following equations.<br>I. M' =Memod n ,M = (M')dmod n<br>II. ed≡ 1 mod n<br>III. ed≡ 1 mod Φ(n)<br>IV.M' =Memod Φ(n) M = (M')dmod Φ(n)<br>Which of the above equations correctly represent RSA cryptosystem?**[L.J.I.E.T]**<br>(I) and (II)<br>(I) and (III)<br>(II) and (IV)<br>(III) and (IV)<br>All Mentioned options.<br>None of the Mentioned | **01** |
| **4** | In a RSA cryptosystem, a participant A uses two prime numbers p=13 and q=17 to generate her public and private keys. If the public key of A is 35, then the private key of A is _____.**[L.J.I.E.T]**<br>1. 11<br>2. 15<br>3. 26<br>4. 14<br>5. 56<br>6. None of the Mentioned | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and Calculate the ciphertext if the given plaintext is 7.**(Dec-2015 OLD)[L.J.I.E.T]** | **07** |
| **2** | In a public key system using RSA, the ciphertext intercepted is C=10.which is sent to the user whose public key is e=5, n=35. What is the plaintext M?**(May-2011 OLD)[L.J.I.E.T]** | **04** |

| | | |
|---|---|---|
| **3** | Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7, M=5.**(May-2011 OLD)(Nov-2013 OLD)(Dec-2015 OLD)[L.J.I.E.T] or** Calculate ciphertext in case of RSA if p=3,q=11,e=3,M=5**(May-2013 OLD)[L.J.I.E.T] or** Perform encryption using the RSA algorithm.<br>p=3,q=11(two random numbers).<br>e(encryption key)=7<br>M(plaintext message)=5**(May-2015 OLD)[L.J.I.E.T]** | **03/04** |
| **4** | Give the steps of RSA algorithm..**(Nov-2011 OLD)[LJIET]**OR Explain encryption and decryption using RSA **(May-2018 OLD)[L.J.I.E.T]** | **04** |
| **5** | Write four possible approaches to attacking the RSA algorithm. .**(May-2012 OLD) [LJIET]** OR Discuss the possible approaches to attack the RSA algorithm. Also discuss various mathematical and timing attacks for RSA algorithm **(Oct-2016 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain in detail RSA algorithm, highlighting its security aspect.**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **6** | Explain Encryption and decryption in RSA algorithm. Also discuss various attacks on RSA.**(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **7** | Define the types of cryptanalytic attacks. Which cryptnalytic attack can occur on RSA algorithm?**(May-2013 OLD)[L.J.I.E.T]** | **04** |
| **8** | Explain RSA algorithm and list the possible approaches to attacking it.**(Nov-2013 OLD)[L.J.I.E.T]** | **04** |
| **9** | Explain RSA algorithm.**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **10** | Elaborate various kinds of attacks on RSA algorithm.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **11** | P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail.**( Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **12** | Explain RSA Algorithm.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **13** | Explain key generation using RSA algorithm. OR Explain key pair generation using RSA algorithm**(Nov-2017 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **14** | Explain RSA algorithm in detail with suitable example.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **15** | Discuss RSA Algorithm with suitable example.**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **16** | Explain RSA algorithm with example. **(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **17** | In a public key cryptosystem using RSA algorithm, user uses two primenumbers 5 and 7. He chooses 11 as Encryption key , find out decryptionkey. What will be the ciphertext, if the plaintext is 2?**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| **18** | Explain the three approaches to attack RSA mathematically. **(May-2019 OLD)[L.J.I.E.T]** | **03** |
| **19** | Explain RSA algorithm with appropriate block diagram and example.**(Dec 2019 old)[LJIET]** | **07** |
| **20** | Explain process of encryption in RSA Algorithm with suitable example.(Prime Number P,Q and Encryption Key E is given for reference) P=7,Q=17, E=7**(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **21** | In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M? **(Oct-2020 OLD)[L.J.I.E.T]** | **04** |
| **22** | Explain RSA algorithm in detail with suitable example.**(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| **23** | How can we find out GCD of two numbers using Euclid algorithm? Explain with the help of example.**(Aug-2021 OLD)[L.J.I.E.T]** | **03** |
| **24** | Perform encryption and decryption using RSA algorithm for following: p=3;q=13,e=5;M=10 **(Aug-2021 OLD)[L.J.I.E.T]** | **04** |
| **25** | Calculate all the values of RSA assuming two primes p=17 and q=11. Assume other values appropriately. **(Jan-2021 OLD)[L.J.I.E.T]** | **07** |
| | **TOPIC 4: Diffie-Hillman Key Exchange algorithm, Man-in -Middle attack** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Briefly explain the Diffie-Hellman key exchange.**(May-2011 OLD) (Nov-2016 or** Explain Diffie | **07** |

| | | |
|---|---|---|
| | – Hellman key exchange **(May-2015 OLD)[L.J.I.E.T]** | |
| **2** | Explain Deffie Hellman key exchange scheme in detail. . **(Nov-2011 OLD)(Jan-2013 OLD)[L.J.I.E.T]**<br>**OR**<br>Briefly explain Diffie Hellman Key exchange with an example**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **3** | Write and explain the Diffie-Hellman key exchange algorithm. OR What is primitive root? Explain Diffi-Hellmen key exchange algorithm with proper example.**(May-2012 OLD)(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **4** | Write Diffie Hellman key exchange algorithm. Explain man-in-the middle attack on this Diffie Hellman key exchange.**(May-2013 OLD)(Oct-2016 OLD)[L.J.I.E.T]** | **07** |
| **5** | Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.**(Dec-2018 OLD)[L.J.I.E.T]** OR Explain man in middle attack in Diffie Hellman key exchange **(Nov-2013 OLD)(May-2018)[L.J.I.E.T] OR** Explain Diffie - Hellman key exchange algorithm. Also explain Man-in-Middle attack with example. **(May-2019 OLD) [L.J.I.E.T]**<br>**OR**<br>Discuss Man in Middle Attack.**)(Nov-2018 OLD)[L.J.I.E.T]** | **07/04** |
| **6** | In symmetric encryption, Describe the ways in which key distribution can be achieved between two parties A and B?**(Dec-2015 OLD) L.J.I.E.T]** | **07** |
| **7** | Explain Diffie Hellman key exchange algorithm.**(May-2017 OLD)[L.J.I.E.T]**or Explain Diffie Hellman key exchange algorithm. **(Jan-2013 OLD)(Nov-2017 OLD)(May-2018)[L.J.I.E.T]** | **07** |
| **8** | Discuss Diffie-Hillman key exchange algorithm in detail?What are the limitations of Diffie-Hellman algorithm? Which are the features of Oakley algorithm? **(Oct-2016 OLD)(May-2017 OLD)[L.J.I.E.T]** | **07,07** |
| **9** | Calculate the shared secret (KA and KB) key using Diffie Hellman<br>Key Exchange Algorithm. Take q=23, α = 5, XA = 6 and XB = 15.**(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **10** | Explain Diffie - Hellman key exchange algorithm.**(May-2016 OLD)(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **11** | For Diffie-Hellman algorithm, two publicly known numbers are primenumber 353 and primitive root of it is 3. A selects the random integer 97and B selects 233. Compute the public key of A and B. Also computecommon secret key.**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| **12** | Explain Diffie-Hellman key exchange protocol with block diagram and example**(Dec 2019 OLD)[LJIET]** | **07** |
| **13** | Describe the Diffie Hellman key exchange Algorithm with example**(Nov-2019 OLD)[L.J.I.E.T]** | **04** |
| **14** | Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.**(Oct-2020 OLD)[L.J.I.E.T]** | **07** |
| **15** | Explain the Deffie Hellman key exchange scheme in detail with an example.**(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| **16** | Write a short note on Man-in-the-middle attack. **(Jan-2021 OLD)[L.J.I.E.T]** | **04** |
| **17** | Calculate all the values for Diffie-Hellman key exchange, consider two primes q=353 and a=3. Assume other values appropriately.**(Jan-2021 OLD)[L.J.I.E.T]** | **07** |
| | **CHAPTER 5** | |
| | **TOPIC 1: Cryptographic Hash Functions, their applications** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Message Digest.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by one-way function.**[L.J.I.E.T]** | **01** |
| **3** | What do you mean by weak collision resistance. **[L.J.I.E.T]** | **01** |
| **4** | What do you mean by strong collision resistance. **[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Illustrate variety of ways in which hash code can be used to provide message authentication.**(May-2011 OLD)[L.J.I.E.T]** | **07** |

| | | |
|---|---|---|
| **2** | 1. Explain the following properties of hash function<br>(i) One way property<br>(ii) Weak collision resistance<br>(iii) Compression functions in hash algorithm.**(May-2011 OLD)[L.J.I.E.T]** | **07** |
| **3** | Explain different characteristics of hash function. OR Write the properties of hash functions**(Nov-2011 OLD)(May-2015 OLD)[L.J.I.E.T]** | **04** |
| **4** | What is the difference between weak and strong collision resistance? **(Nov-2013 OLD)[L.J.I.E.T]** | **03** |
| **5** | "Only Hashing dose not ensures integrity of message in network communication" – Justify your answer with suitable example.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **6** | Write requirements for hash function and briefly explain simple hash function. **(May 2017 OLD)[L.J.I.E.T]** | **07** |
| **7** | Explain basic Hash code generation.**(May-2018 OLD)[L.J.I.E.T]** | **03** |
| **8** | Enlist the practical applications of hashing. .**(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **9** | What is the difference between weak and strong collision resistance?Consider the hash functions based on cipher block chaining, What kindof attack can occur on this?**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| | **TOPIC 2: Simple hash functions, its requirements and security** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain Birthday Attacks.**[L.J.I.E.T]** | **04** |
| **2** | Explain the general structure of secure hash functions.**(Nov-2011 OLD)[L.J.I.E.T]** | **03** |
| **3** | Explain property of Hash function.**[L.J.I.E.T]** | **07** |
| **4** | What characteristics are needed in a secure hash function? Explain the concept of simple hash function.**(Nov-2013 OLD)(Dec-2015 OLD)(Oct-2016 OLD)[L.J.I.E.T]**<br>**OR**<br>Discuss HASH function and its application in Crypto System.**)(Nov-2018)[L.J.I.E.T]**<br>**OR**<br>Discuss clearly Secure Hash Algorithm with its real time application**(Nov-2018)[L.J.I.E.T]** | **04/03/ 07** |
| **5** | What are the characteristics of hash function? Also explain basic techniques of hash algorithm **(May-2019 OLD)[LJIET]** | **07** |
| **6** | What is the role of a compression function in a hash function?**(Nov-2019 OLD)[L.J.I.E.T]** | **03** |
| **7** | Explain basic Hash code generation. **(Oct-2020 OLD)[L.J.I.E.T]** | **03** |
| **8** | Explain how Birthday attack is carried out.**(Jan-2021 OLD)[L.J.I.E.T]** | **04** |
| | **TOPIC 3: Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain the operation of secure hash algorithm on 512 bit block. **(May-2013 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain SHA512 Algorithm. **(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **3** | Differentiate between hashing and encryption. What are the practical applications of hashing? Compare MD5 and SHA1 hashing algorithms.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **4** | What characteristics are needed in secure hash function? Explain the concept of simple hash function. **(Oct-2016 OLD)(Dec-2015 OLD)(Dec-2018 OLD) L.J.I.E.T]** | **07** |
| **5** | Explain SHA-512 algorithm. **(May-2017 OLD)(May-2019 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain the logic of SHA(Secure Hash Algorithm).**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **6** | Write a detailed note on Secure Hash Algorithm.**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **7** | Write a note on following<br>1) Hash algorithm<br>2) Message authentication code<br>3) Digital signature | **14** |

| | | |
|---|---|---|
| | 4) Man in the middle attack**(May-2018 OLD)[L.J.I.E.T]** | |
| **8** | What is SHA-256? Explain with necessary block diagram. **(Dec 2019 OLD)[LJIET]** | **07** |
| **9** | Explain working of Secure Hash Algorithm, with basic arithmetical and logical functions used in SHA.**(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **10** | Justify the characteristics needed for a hash function. Explain Secure Hash Algorithm-1 in brief.**(Jan-2021 OLD)[L.J.I.E.T]** | **07** |
| | **Extra Questions** | |
| **1** | Explain MD5 Algorithm. OR Write MD5 Algorithm OR Describe MD5 message digest algorithm. **(Nov-2014 OLD)(Nov-2011 OLD)(Dec-2015, Dec-2018 OLD)(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain four passes of MD5 message digest algorithm. **(May-2013 OLD)[L.J.I.E.T]** | **07** |
| **3** | What characteristics are needed in a secure hash function? **(Oct-2020 OLD)[L.J.I.E.T]** | **03** |
| **4** | What characteristics are needed in a secure hash function? **(Aug-2021 OLD)[L.J.I.E.T]** | **04** |
| **5** | List out the main features of the SHA-512 cryptographic hash function and briefly explain its compression function.**(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| | **CHAPTER 6** | |
| | **TOPIC 1: Message Authentication Codes, its requirements and security** | |
| | **SHORT QUESTIONS** | |
| **1** | What is Disclosure?**[L.J.I.E.T]** | **01** |
| **2** | What is need of MAC?**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is used.**(May-2011 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain briefly basic uses of MAC.**(Nov-2011 OLD)[L.J.I.E.T]** | **04** |
| **3** | What is the need for message authentication? List various techniques used for authentication. Explain any one. **(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **4** | Is message authentication code same as encryption? How message authentication can be done by message authentication code? **(May-2013 OLD)(May-2015 OLD)[L.J.I.E.T]** **OR** What is MAC ? How it useful in Crypto System**.(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **5** | Write a short note on Message Authentication Code.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **6** | What is message authentication code? What are the requirements for MACs?**(Dec-2018 OLD)[L.J.I.E.T]** Briefly discuss MAC based on DES. **(Oct-2016 OLD)[L.J.I.E.T]** | **07** |
| **7** | How following can be achieved with message authentication code(MAC)? a. Message authentication b. Message authentication and confidentiality**(Dec-2015 OLD) L.J.I.E.T]** | **07** |
| **8** | Give differences between hash function and message authentication codes. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **9** | Write a note on : Message Authentication Codes. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **10** | State the basic difference(s) between message authentication codeand hash function.**(Nov-2017 OLD)[L.J.I.E.T]** | **03** |
| **11** | How message authentication code can be used to achieve message authentication and confidentiality?**(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **12** | Explain MAC code generation using block cipher**(May-2018 OLD)[L.J.I.E.T]** | **03** |
| **13** | Is a message authentication code(MAC) function is similar to encryption.Does MAC provide authentication or confidentiality? Justify your answer**(May-2019 OLD)[L.J.I.E.T]** | **03** |
| **14** | Write the algorithm for message authentication code(MACs) based on HASH functions.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **15** | List three approaches to secure user authentication in a distributed environment.**(May-2019** | **04** |

| | | |
|---|---|---|
| | **OLD)[L.J.I.E.T]** | |
| **16** | What is meant by message digest? Give an example.**(Nov-2018 OLD)[L.J.I.E.T]** | **04** |
| **17** | Is message authentication code same as encryption? How message authentication can be done by message authentication code? **(Oct-2020 OLD)[L.J.I.E.T]** | **04** |
| **18** | What is MAC? Why it is required? **(Aug-2021 OLD)[L.J.I.E.T]** | **03** |
| **19** | Define message authentication code and its characteristics. Discuss MAC based on any standard block cipher.**(Jan-2021 OLD)[L.J.I.E.T]** | **07** |
| | **TOPIC 2: MACs based on Hash Functions** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Illustrate the overall operation of HMAC. Define the terms. **(May-2012 OLD)[L.J.I.E.T]** | **07** |
| **2** | What is MAC? Why it is required? Explain HMAC algorithm. **(Nov-2013 OLD)[L.J.I.E.T]** | **07** |
| **3** | Explain HMAC algorithm. **(Nov-2017 OLD)(May-2018)[L.J.I.E.T]** | **07** |
| **4** | What is MAC? Explain HMAC. **(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **5** | Describe MAC with its security implications.**(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **6** | Briefly explain HMAC algorithm **(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| | **TOPIC 3: Macs based on Block Ciphers** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain CMAC.**[L.J.I.E.T]** | **07** |
| **2** | Explain MAC based on DES.**[L.J.I.E.T]** | **07** |
| | | |
| | **CHAPTER 7** | |
| | **TOPIC 1: Digital Signature, various digital signature schemes** | |
| | **SHORT QUESTIONS** | |
| **1** | What is the need of Digital Signature?**[L.J.I.E.T]** | **01** |
| **2** | Rekha's digitally signs a message and sends it to Ketan. Verification of the signature by Ketan requires _____. **[L.J.I.E.T]**<br>1. Rekha's Public Key<br>2. Ketan's Public Key<br>3. Ketan's Private Key<br>4. Rekha's Private Key<br>5. Rekha's Public Key and Ketan's Private Key<br>6. None of the Mentioned | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write a note on Digital Signature.**(Jan-2013 OLD)[L.J.I.E.T]** | **3.5** |
| **2** | What is digital signature? Explain its use with the help of example.**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **3** | Explain Direct Digital Signature.**[L.J.I.E.T]** | **03** |
| **4** | Explain Arbitrated Digital Signature.**[L.J.I.E.T]** | **07** |
| **5** | Elaborate any one approach to Digital Signatures. **(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **6** | Write a short note on "Digital Signature Algorithm. **(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **7** | Write a note on followings<br>(a) Digital Signature<br>(c) Secure Socket Layer<br>**(Jan-2013 OLD)[L.J.I.E.T]** | **07** |
| **8** | What is digital signature? Explain hash code base digital signature.**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **9** | Explain DSA (Digital Signature Algorithm)**(MAY 2018 OLD)[L.J.I.E.T]**<br>**OR**<br>Briefly explain Digital Signature algorithm.**(Nov-2018 OLD)[L.J.I.E.T]** | |
| **10** | What is the principle of digital signature algorithm(DSA). How a user can create a signature using DSA? Explain the signing and verifying function in DSA.**(May-2019 OLD)[L.J.I.E.T]** | **07** |

| | | |
|---|---|---|
| **11** | Explain Digital Signature. Also explain its use with the help of example. **(May-2019 OLD)[LJIET]** | **07** |
| **12** | Draw Generic Model of Digital Signature Process.**(Nov-2019 OLD)[L.J.I.E.T]** | **03** |
| **13** | What is digital signature? What are the properties a digital signature should have?**(Oct-2021 OLD)[LJIET]** | **04** |
| **14** | List the security services provided by digital signature? **(Aug-2021 OLD)[LJIET]** | **03** |
| **15** | Explain digital signature schemes Elgamal and Schnorr.**(Jan-2021 OLD)[LJIET]** | **07** |
| | **TOPIC 2: Requirements and security** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain Requirements on Digital Signature.**(Oct-2016 OLD) L.J.I.E.T]** | **07** |
| **2** | What are the requirements of digital signature? Explain the concept ofarbitrated digital signature. **(Oct-2016 OLD)(Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **3** | List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.**(Nov-2013 OLD)[L.J.I.E.T]** | **07** |
| **4** | Write a short note on "Digital Signature Algorithm". **(Oct-2020 OLD)[L.J.I.E.T]** | **07** |
| | **TOPIC 3: NIST digital Signature algorithm** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write the Digital Signature Algorithm.**(May-2011 OLD) (Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain digital signature algorithm in detail.**(Nov-2011 OLD)[L.J.I.E.T]** | **07** |
| **3** | Explain DSS Approach in detail.**(Nov-2016 OLD) L.J.I.E.T]** | **07** |
| **4** | Explain any one approach to Digital Signatures.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **5** | Describe Elgamal digital signature.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **6** | Explain digital signature schemes Elgamal and Schnorr.**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **7** | Explain Elgamal Digital Signature Scheme.**(Nov-2019 OLD)[L.J.I.E.T]** | **04** |
| **8** | Explain Schnorr Digital Signature Scheme.**(Nov-2019 OLD)[L.J.I.E.T]** | **04** |
| **9** | What is digital certificate? What is the purpose of X.509?**(Aug-2021 OLD)[L.J.I.E.T]** | **03** |
| **10** | Write and explain the Digital Signature Algorithm.**(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| | **CHAPTER 8** | |
| | **TOPIC 1: symmetric key distribution using symmetric and asymmetric encryptions** | |
| | **SHORT QUESTIONS** | |
| **1** | What is master Key?**(Oct-2016 OLD) [L.J.I.E.T]** | **01** |
| **2** | What is Session Key?**(Oct-2016 OLD) [L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain different key distribution techniques. OR discussdifferent techniques for public-key distribution OR Explain various public key distribution techniques. **(Nov-2011 OLD) (Oct-2016 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **2** | What is KDC? With the help of diagram explain how KDC do key distribution.**(Jan-2013 OLD) [L.J.I.E.T]**<br>**OR**<br>What is KDC? List the duties of a KDC.**(Nov-2018 OLD)[L.J.I.E.T]** | **07/04** |
| **3** | What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center.**(May-2013 OLD)[L.J.I.E.T]** | **07** |
| **4** | List and explain various key management techniques.**(May-2014 OLD)[L.J.I.E.T] OR** List & Explain various key management techniques. **(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **5** | Explain Token authentication.**(May-2016 OLD)[L.J.I.E.T]** | **04** |
| **6** | Explain Key Distribution methods.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **7** | Explain a Transparent Key Control Scheme.**[L.J.I.E.T]** | **07** |
| **8** | Explain/ Discuss Decentralized Key Control.**(Oct-2016 OLD) L.J.I.E.T]** | **05** |

| | | |
|---|---|---|
| **9** | Explain key distribution using KDC.**(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **10** | Write the key distribution scenario in which each user shares a unique master key with key distribution center. **(May-2011 OLD)[L.J.I.E.T]** | **03** |
| **11** | Explain the key distribution scenario and write how does decentralized key control work?**(May-2012 OLD)[L.J.I.E.T]** | **07** |
| **12** | What is the difference between a session key and a master key? List four general categories of schemes for the distribution of public keys. ?**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| **13** | Explain the process of secret key distribution with confidentiality and authentication.**(Aug-2021 OLD)[L.J.I.E.T]** | **04** |
| | **TOPIC 2: distribution of public keys** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Public Announcement.**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by Public Available Directory.**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Discus the ways in which public keys can be distributed to two communication parties. OR Which techniques are used for the distribution of public keys?**(Nov-2013 OLD)(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain Public Key Certificate.**[L.J.I.E.T]** | **07** |
| **3** | List and explain four general categories of schemes for the distribution of public keys**. (May-2012 OLD)(May-2015 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain central authority public key distribution scenario with neat and diagram.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **5** | Explain Exchange of public key certificate scenario with neat diagram. .**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **6** | What is the difference between a session key and a master key?**(Oct 2020 OLD)[LJIET]** | **03** |
| **7** | What do you mean by key distribution? Give at least one method for key distribution with proper illustration. **(Oct 2020 OLD)[LJIET]** | **07** |
| **8** | How public keys can be distributed.**(Oct 2020 OLD)[LJIET]** | **04** |
| **9** | Explain the process of public key distribution using public key authority.**(Aug 2021 OLD)[LJIET]** | **04** |
| **10** | What are different ways for distribution of public keys?**(Jan 2021 OLD)[LJIET]** | **03** |
| **11** | Explain key distribution process using Key Distribution Center (KDC).**(Jan 2021 OLD)[LJIET]** | **04** |
| | **TOPIC 3: X.509 certificates** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain X.509 authentication service.?**(Nov-2011 OLD)[LJIET] OR** What is the purpose of X.509 standard **(Dec-2015 OLD)[L.J.I.E.T]**<br>**OR**<br>What is the purpose of X.509 standard? How is an X.509 certificate revoked?**(May-2019 OLD)[L.J.I.E.T]**<br>**OR**<br>Described briefly the Authentication process covered by X.509.**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain the one –way and two way authentication in X.509.**(May-2012 OLD)[L.J.I.E.T]** | **07** |
| **3** | Write a note on : X.509 Certificate Format.**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain digital public key certificate format**(May-2018 OLD)[L.J.I.E.T]** | **03** |
| **5** | Why is X.509 directory authentication service used? Explain its working. **(Dec 2019 OLD)[LJIET]** | **07** |
| **6** | Explain use of Public-Key Certificate with diagram and draw X.509certificate format. **(Nov-2019 OLD)[L.J.I.E.T]** | **07** |
| **7** | Explain X.509 authentication service.**(Oct 2020 OLD)[LJIET]** | **07** |
| **8** | What is defined by X.509 certificate? Write the process of authentication in X.509. **(Jan 2021 OLD)[LJIET]** | **03** |

| | | |
|---|---|---|
| | **TOPIC 4: Public key infrastructure** | |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain PKI in detail.**[L.J.I.E.T]** | **07** |
| **2** | What is PKI? What are the components of PKI? Explain Certificate Authority in detail.**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **3** | Write a short note on public key infrastructure.**(May-2018 OLD)[L.J.I.E.T]** | **07** |
| | | |
| | **CHAPTER 9** | |
| | **TOPIC 1: Remote user authentication with symmetric and asymmetric encryption, Kerberos** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Kerberos.**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain Kerberos in detail.**(Nov-2011 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain the ticket granting server(TGS) scheme in Kerberos.**(May-2012 OLD)[L.J.I.E.T]** | **07** |
| **3** | What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos.**(Nov-2013 OLD)(Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain Kerberos Authentication System.**(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **5** | What is Kerberos? How Kerberos authenticates the users for authorized service access?**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **6** | What four requirements were defined for Kerberos?**(Dec-2015 OLD)[L.J.I.E.T]** | **04** |
| **7** | Explain inter realm authentication of Kerberos. .**(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **8** | Explain X.509 Directory Authentication Service. **(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **9** | Write a detailed note on : Kerberos**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **10** | Explain the concept of Realm in Kerberos in brief.**(Nov-2017 OLD)[L.J.I.E.T]** | **03** |
| **11** | Explain authentication mechanism of Kerberos.**(May-2016 OLD)(May-2018 OLD)(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **12** | Write a note on followings<br>(b) Kerberos<br>(c) Hill cipher<br>(e) Diffi hellman key exchange.<br>(f) Message Authentication code**(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **13** | What problem was Kerberos designed to address? What are the three threats associated with user authentication over a network or Internet?**(May-2019 OLD)[L.J.I.E.T]** | **04** |
| **14** | Explain Kerberos authentication protocol with necessary diagrams. **(Dec 2019 OLD)[LJIET]** | **07** |
| **15** | What problem was Kerberos designed to address? **(Nov-2019 OLD)[L.J.I.E.T]** | **03** |
| **16** | Explain authentication mechanism of Kerberos.**(Oct-2020 OLD)[L.J.I.E.T]** | **07** |
| **17** | What is Kerberos? How it works? Explain in detail. **(Aug-2021 OLD)[L.J.I.E.T]** | **07** |
| **18** | What is TGT? Explain its use in Kerberose. **(Jan-2021 OLD)[L.J.I.E.T]** | **04** |
| | **CHAPTER 10** | |
| | **TOPIC 1: Web Security threats and approaches** | |
| | **SHORT QUESTIONS** | |
| **1** | How to countermeasure Integrity in Web. **[L.J.I.E.T]** | **01** |
| **2** | How to countermeasure Confidentiality in Web. **[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Briefly explain web security threats.**(May-2017 OLD )[L.J.I.E.T]**<br>**OR**<br>List out the various web security threats.**(Nov-2018 OLD)[L.J.I.E.T]** | **03** |
| **2** | What are the security challenges for Web. **[L.J.I.E.T]** | **04** |

| | | |
|---|---|---|
| **3** | Explain Threats on the Web.**[L.J.I.E.T]** | **03** |
| **4** | Explain Approaches to providing Web security.**[L.J.I.E.T]** | **05** |
| **5** | How can we achieve web security? Explain with example. **(May-2014 OLD)[L.J.I.E.T]** | **07** |
| **6** | Briefly discuss web security threats. **(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **7** | Which types of security threats are faced by user while using the web?**(May-2019 OLD) [L.J.I.E.T]** | **03** |
| **8** | Enlist various web security threats. Explain any one. **(Jan-2021 OLD)[L.J.I.E.T]** | **03** |
| | | |
| | **TOPIC 2: SSL architecture and protocol** | |
| | **SHORT QUESTIONS** | |
| **1** | What is SSL?**[L.J.I.E.T]** | **01** |
| **2** | What do you mean by Session?**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | List and define the parameters that define secure socket layer connection state. **(May-2011 OLD)[L.J.I.E.T]** | **07** |
| **2** | Explain SSL protocol in detail. OR Explain Secure Socket Layer Protocol. **(Nov-2011 OLD)(Nov-2014 OLD)[L.J.I.E.T]** | **07** |
| **3** | Which parameters define session state and which parameters define connection state in SSL (secure socket Layer)? OR Define SSL session and SSL connection. Which parameters define session state and connection state. OR Explain SSL Session and Connections **(May-2012 OLD)(May-2015 OLD)(May-2018 OLD)[L.J.I.E.T]**<br>**OR**<br>Define the parameters that define SSL session state and session connection.**(May-2019 OLD)[L.J.I.E.T]** | **07/03** |
| **4** | Write a note on secure socket Layer. **(Jan-2013 OLD)(Oct-2016 OLD)[L.J.I.E.T]** | **07** |
| **5** | Explain the secure socket layer handshake protocol action. **(May-2013 OLD)[L.J.I.E.T]** | **07** |
| **6** | List and define the parameters that define secure socket layer connection state. **(Nov-2013 OLD)[L.J.I.E.T]** | **07** |
| **7** | Write a short note on SSL.**(May-2016 OLD)(May-2018)[L.J.I.E.T]** | **07** |
| **8** | What is SSL? Which security services does it offers? How does it works?**(Nov-2016 OLD)[L.J.I.E.T]** | **07** |
| **9** | Define – SSL session and SSL connection. Which parameters are used to define SSL state and SSL connection?**(Dec-2015 OLD) L.J.I.E.T]** | **07** |
| **10** | Discuss SSL architecture in brief. **(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **11** | Briefly discuss the working of SSL Record Protocol. **(Nov-2017 OLD)[L.J.I.E.T]** | **04** |
| **12** | Explain SSL architecture. **(Dec-2018 OLD)[L.J.I.E.T]** | **07** |
| **13** | What is SSL? Explain SSL Handshake & Record Protocol.**(May-2019 OLD) [L.J.I.E.T]** | **07** |
| **14** | Explain HAND SHAKE protocol in SSL. **(Nov-2018 OLD) [L.J.I.E.T]** | **03** |
| **15** | What is e-commerce? Discuss requirement of security w.r.t. e-commerce transactions.**(Dec 2019 OLD)[LJIET]** | **07** |
| **16** | Explain SSL architecture .**(Oct 2020 OLD)[LJIET]** | **07** |
| **17** | Write a detailed note on SSL architecture and protocol.**(Jan 2021 OLD)[LJIET]** | **07** |
| **18** | How does secure socket layer protocol work?**(Jan 2021 OLD)[LJIET]** | **03** |
| | **TOPIC 2: Transport layer security** | |
| | **SHORT QUESTIONS** | |
| **1** | What do you mean by Handshake?**[L.J.I.E.T]** | **01** |
| **2** | What is TLS?**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Explain Handshake Protocol in TLS.**[L.J.I.E.T]** | **05** |

| | | |
|---|---|---|
| **2** | Compare TLS and IPSec.**[L.J.I.E.T]** | **04** |
| **3** | Explain the pseudorandom function used by Transport layer security. **(May-2013 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain IP Sec with its benefits. **(May-2019 OLD)[LJIET]** | **07** |
| **5** | Write a short note on IP security. **(Dec 2019 OLD)[LJIET]** | **07** |
| **6** | Write the benefits of IPSec.**(May-2015 OLD)[LJIET]** | **04** |
| | **TOPIC 3: HTTPS and SSH** | |
| | **SHORT QUESTIONS** | |
| **1** | What is HTTPS?**[L.J.I.E.T]** | **01** |
| **2** | What is SSH?**[L.J.I.E.T]** | **01** |
| | **DESCRIPTIVE QUESTIONS** | |
| **1** | Write a short note on HTTPS.**[L.J.I.E.T]** | **04** |
| **2** | Compare HTTP and HTTPS.**[L.J.I.E.T]** | **03** |
| **3** | Explain the use of firewall.List advantages and disadvantages of firewall.**(May-2015 OLD)(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **4** | Explain SSL Architecture **(Oct-2016 OLD)[L.J.I.E.T]** | **07** |
| **5** | Write a short note on SSH.**[L.J.I.E.T]** | **04** |
| **6** | Explain HTTPS in brief.**(Nov-2017)[L.J.I.E.T]** | **03** |
| **7** | Explain use and concept of dual signature in SET.**(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **8** | What is SSH? How does SSH works?**(Nov-2016 OLD)[L.J.I.E.T]**<br>**OR**<br>For what purpose Secure Shell(SSH) is useful? Briefly define SSH protocol.**(May-2019 OLD) [L.J.I.E.T]** | **07/03** |
| **9** | Explain HTTPS and SSH. **(May-2018 OLD)[L.J.I.E.T]** | **07** |
| **10** | What is the main difference between HTTP and HTTPS protocol. WhenHTTPS is used, which elements of the communication are Encrypted?**(Nov 2019 OLD)[LJIET]** | **04** |
| **11** | What is SSH? How it works?**(Aug 2021 OLD)[LJIET]** | **03** |
| **12** | What is HTTPS? How it works?**(Aug 2021 OLD)[LJIET]** | **04** |
| | **Extra Questions** | |
| **1** | Explain Secure electronic transaction protocol. **(Nov-2011 OLD)[L.J.I.E.T]** | **07** |
| **2** | What is a dual signature in reference to secure electronic transaction? OR What is a dual signature? Explain in detail the following transactions supported by SET(secure electronic transaction)<br>(i) Purchase request<br>(ii) Payment authorization**(May-2012 OLD)(Dec-2015 OLD) L.J.I.E.T]** | **07** |
| **3** | Write the key features of secure electronic transaction. **(May-2012 OLD) L.J.I.E.T]** | **04** |
| **4** | Write a note on Firewall. **(Jan-2013 OLD)(May-2015 OLD) L.J.I.E.T]** | **3.5** |
| **5** | Explain packet filtering router in case of firewall. (**May-2013 OLD) L.J.I.E.T]** | **04** |
| **6** | Write the key features of secure electronic transaction. **(Nov-2013 OLD) L.J.I.E.T]** | **04** |
| **7** | Explain Secure Electronic Transaction Protocol. **(Nov-2011 OLD)(Nov-2014 OLD) L.J.I.E.T]** | **07** |
| **8** | Write a short note on Pretty Good Privacy **(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **9** | Write Short Note: PGP**(May-2017 OLD)[L.J.I.E.T]**<br>**OR**<br>Explain PGP with its Authentication and Confidentiality Operation.**(Nov-2018 OLD)[L.J.I.E.T]** | **07** |
| **10** | Write a short note on Pretty Good Privacy (PGP). **(May-2016 OLD)[L.J.I.E.T]** | **07** |
| **11** | Write Short Note: S/MIME**(May-2017 OLD)[L.J.I.E.T]** | **07** |
| **12** | Write a short note on S/MIME. **(Nov-2014 OLD)(Nov-2017 OLD)[L.J.I.E.T] or** Discuss | **07** |

| | | |
|---|---|---|
| | about S/MIME **(Nov-2011 OLD)[L.J.I.E.T]** | |
| **13** | Explain transaction on E-commerce OR Explain Security of E-Commerce. ORWhy E-commerce transactions need security?**(May-2015 OLD)(Nov-2014 OLD)(Nov-2017 OLD)[L.J.I.E.T]** | **07** |
| **14** | Why Transport Layer Security makes use of a pseudo random function?**(May-2019 OLD)[L.J.I.E.T]** | **03** |
| **15** | Explain concept of Dual Signature in SET.**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **16** | Explain the general format of PGP(Pretty Good Privacy) message**(May-2019 OLD)[L.J.I.E.T]** | **07** |
| **17** | Write a note on HTTPS. **(Oct-2020 OLD)[L.J.I.E.T]** | **04** |
| | | |