



Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : X 67547

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020
Sixth Semester
Computer Science and Engineering
CS 1355 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Information Technology)
(Regulations 2008)

Time : Three Hours

Maximum : 100 Marks

Answer ALL questions

PART – A

(10×2=20 Marks)

1. List down the essential ingredients of a symmetric cipher.
2. Define : Diffusion.
3. What is key distribution center ?
4. Mention the application of public key cryptography.
5. Write down the procedure to calculate the Hash value of a message.
6. What are Digital Signature Standard (DSS) ?
7. List out the differences between e-mail security and IP security.
8. Define : PGP.
9. Define a Password.
10. What is web attack ?

**PART – B****(5×16=80 Marks)**

11. a) Encrypt the message “meet me. at the usual place at ten rather than eight o clock” using till cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.
- i) Show your calculations and the result. **(8)**
- ii) Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext. **(8)**
- (OR)
- b) Explain S-DES algorithm in detail. **(16)**
12. a) Explain the Diffie-Hellman key exchange algorithm with example. **(16)**
- (OR)
- b) Explain how Elliptic curve cryptography can be used for message encryption. **(16)**
13. a) i) Describe the use of Hash functions. **(8)**
- ii) Write a note on Digital signature standard. **(8)**
- (OR)
- b) i) What is MD5 message Digest algorithm ? Explain. **(8)**
- ii) Write a note on security of Hash functions and Macs. **(8)**
14. a) Elaborate about the enhancements of Kerberos V5 over Kerberos V4. **(16)**
- (OR)
- b) Draw and explain the IP Security Architecture. **(16)**
15. a) Explain about intrusion detection techniques in detail. **(16)**
- (OR)
- b) Write about trusted systems in detail. **(16)**
-