

DC-135

December-2017

5th Year M.Sc. (CA & IT) Integrated Cryptography

Time : 2 Hours]

[Max. Marks : 100

1. Attempt any **four** : 20
 - (i) Explain in brief Security principles with figure.
 - (ii) Encrypt using rail fence technique with depth 3 “How much wood would a wood chuck chuck if a wood chuck could chuck wood”.
 - (iii) Encrypt “fine” using Hill Cipher for key matrix of size 2×2 where $k_{11} = 9, k_{12} = 4, k_{21} = 5, k_{22} = 7$
 - (iv) Explain Different Substitution and Transposition Techniques.
 - (v) Explain variations of DES with figure.

2. Attempt any **four** : 20
 - (i) If A wants to send a message securely to B, explain it with steps involved in asymmetric key cryptography.
 - (ii) Given two prime Numbers $P=17$ and $Q=29$, find out N, E and D in an RSA encryption process.
 - (iii) Can we use a conventional loss-less compression mechanism as message digest ? Why ?
 - (iv) Explain broad level differences between CRL, OCSP and SCVP.
 - (v) Explain the steps of creation of a digital certificate.

3. Attempt any **four** : 20
 - (i) Why is the SSL layer positioned between the application layer and the transport layer ? What is the purpose of the SSL alert protocol ?
 - (ii) How SET Achieves its Objectives ? How is 3-D Secure different from SET ?
 - (iii) What is electronic money ? Why is anonymous offline electronic money dangerous ?
 - (iv) Mention broad level steps in PEM and PGP.
 - (v) Explain WAP and GSM.

4. Attempt any **four** : **20**
- (i) How Kerberos does works ? Explain with figure.
 - (ii) Can an Unauthorized user use an Authentication token. What are the three aspects of a 3-factor authentication ?
 - (iii) (a) Explain cryptography toolkit.
(b) Draw TCP segment format.
 - (iv) List JAVA cryptography technologies. Explain any one.
 - (v) Explain Certificate based authentication.
5. Attempt any **four** : **20**
- (i) List layers in TCP/IP protocol suit and explain transfer from source to destination at different TCP/IP.
 - (ii) List the ways to configure firewall. Explain any two.
 - (iii) Explain virtual private network with VPN architecture.
 - (iv) Explain security association in IPSec.
 - (v) Define following :
 - (a) Dynamic Packet Filter
 - (b) Demilitarized Zone Network
-