Exam No._____

GANPAT UNIVERSITY

M. TECH SEM- II (Computer Engineering/Information Technology)

REGULAR EXAMINATION- APRIL-JUNE 2015

3CE205/3IT205: Public Key Infrastructure

TIME: 3 HRS TOTAL MARKS:60

Instruction 1. This Question paper has two sections. Attempt each section in separate answer book
2. Figures on right indicate marks.
3. Be precise and to the point in answering the descriptive questions.

Section I

Que.-1

A Explain the type of architecture in which CA's are connected through superior–subordinate relationships with diagram. Also write advantages and disadvantages for that. 6

B List the certificate creation steps. Explain each step in detail with diagram. 4

OR

Que.-1

A What are the reasons for certificate revocation? Explain online revocation status checks in detail with diagram. 6

B What are the principle differences between Kerberos version 4 and version 5? 4

Que.-2

A The two companies want to communicate securely, are geographically on different location. Discuss different possible approaches to achieve the requirement of the companies with advantages and disadvantages. Among all the approaches which one is best and practically used now days? 8

B A host receives an authenticated packet with the sequence number 181. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event? 2

OR

Que.-2

A Explain the SSL sub protocol, in which "client and server negotiate with cipher suite and perform key exchange in between for further communication" in detail with diagram. 6

B What is the difference between fixed password and one time password? What is frequently changed password? How do you implement this scheme? Explain it with an example. 4

Que.-3

A "IPSec prevent from replay attack." – True or False. Justify your answer in detail with diagram. 6

B John sends his own public key to Diana for secure communication, during this process how an attacker can apply Man-In-The-Middle attack? How to prevent MITM in this situation? 3

C On a _____ layer of TCP/IP protocol suite SSL provide security. 1

Section II

Que.-4

A Explain Lempel-Ziv algorithm. Compress following text. 8
"Welcome to the world of security. The world of security is full of interesting problems and solutions."

B Write the benefits provided by smart card. 2

OR

Que.-4

A What is Single-sign on? Explain simple SSO operation with diagram. 4

B For n = 388267, s = 157, v= 24649, show the three rounds of the Fiat-Shamir protocol for the c = 0 & r = 203122, c = 1 & r = 153271 and c =1 & r = 377245. 3

C For s = 157, e = 7, n= 553913,Ø(n)= 552402, v = 444751, show the three rounds of the Guillou-Quisquater protocol for the c = 1 & r = 15024, c = 3 & r = 7235 and c = 4 & r = 423. 3

Que.-5

A Explain following in brief: 6
1. The Access Control Server
2. Merchant Server Plug-in (MPI)
3. The Directory Server

B How sender and receiver extract the information using PGP key ring? Explain it in detail with diagram. 4

OR

Que.-5

A Explain S/MIME in detail with diagram. 6

B How dual signature is important in SET? Explain limitation of SET. 4

Que.-6

A Define biometrics. List the physiological techniques. Explain any four in detail. 4

B Explain challenge response authentication using keyed-hash functions and using digital signature with diagram. 4

C Differentiate: SSL Vs SET 2

END OF PAPER