School of Information Technology
Indian Institute of Technology, Kharagpur

IT60112 Information and System Security **Class Test 2**
Date: March 22nd, 2005. **Total Time: 1 Hour** **Max. Marks: 20**

Answer All Questions. Clearly write any reasonable assumption that you make.

Q1.

Consider yourself to be a user (named **guest** with password **guest**) trying to authenticate in a Kerberos realm. The IP address of your workstation is **10.14.7.35**. There are two servers in the realm – a print server called **agni** and a mail server called **varun**. Name of the ticket granting server is **pravesh**. Show the complete sequence of Kerberos version 4 message exchanges if you need to log on to the system, first access the mail server for checking your mails, then the print server for printing a document and then again the mail server before logging out. You need to have mutual authentication. Supplied data should replace generic data wherever applicable. **[8]**

Q2. Consider the Simplified version of Data Encryption Standard (S-DES). Write the ciphertext after two rounds of encryption of the plaintext. From the ciphertext, show that the decryption procedure gives back the plaintext. Show the output at the end of each stage. **[12]**

Plaintext: 0 1 0 0 0 1 1 0

10-bit Key: 1 0 1 0 0 0 0 0 1 0

For Encryption

IP							
2	6	3	1	4	8	5	7

E/P							
4	1	2	3	2	3	4	1

		C0	C1	C2	C3
S0	R0	1	0	3	2
	R1	3	2	1	0
	R2	0	2	1	3
	R3	3	1	3	2

IP^{-1} : Deduce it.

		C0	C1	C2	C3
S1	R0	0	1	2	3
	R1	2	0	1	3
	R2	3	0	1	0
	R3	2	1	0	3

P4			
2	4	3	1

For Key Generation

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9