REG. NO										

MANIPAL INSTITUTE OF TECHNOLOGY

(A constituent Institute of MANIPAL UNIVERSITY)

MANIPAL - 576 104, KARNATAKA, INDIA

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY)
END SEMESTER EXAM - APRIL 2017
SUBJECT: DESIGN OF SECURE PROTOCOLS (CSE 5221)
DATE: 20-04-2017

TIME: 3 HOURS MAX.MARKS: 50

Instructions to Candidates

- **Note:** Answer all full questions.

1A. Give examples of secure multi-party protocols. 2M

1B. Explain any three generic types of attacks on cryptographic protocols. 3M

1C. Discuss the Keyed hash function along with a diagram and notations involved. 5M

2A. Explain the parallel session attack on Woo-Lam protocol. Clearly write the sequence diagram, notations involved and the message exchange. 5M

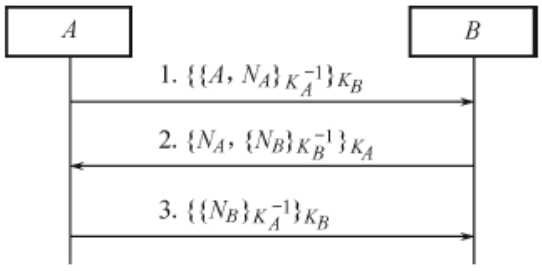
2B. Modify the message $B \rightarrow S: M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$ and show how the data integrity protection is achieved? 2M

2C. Explain any three prudent engineering principles in the security design of protocols. 3M

3A. What is the premise knowledge of an adversary ***I*** in case of public key cryptographic scheme when there are two principals ***A*** and ***B***? 2M

3B. Explain $one - time\ session\ token$ in an authentication protocol and how the replay attack is avoided? 4M

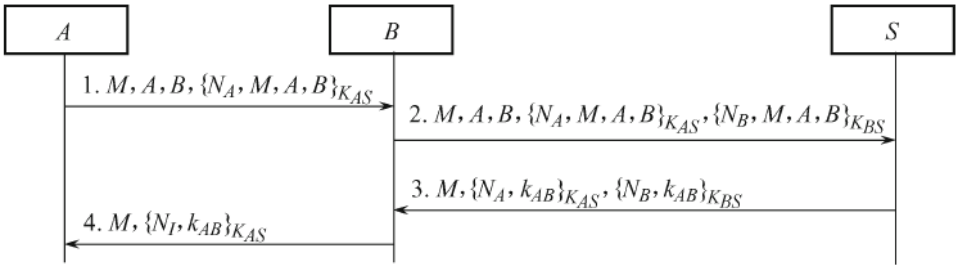
3C. Write the security analysis of the following protocol in a table format using manual security analysis method. 4M



4A. Write the $conv$ and $conv^1$ in a Π between principals $\boldsymbol{A}$ and $\boldsymbol{B}$. When can we say that the authentication protocol is secure using these conversations? And also when adversaries can wins such a Π? 4M

4B. Explain the association rule in simple English $-\{\dots N \dots\}_k \hat{} B_{P_i,t}(\prec \{N, P_i, P_j\}) \hat{} B_{P_i,t}(Key(P_i, k^{-1})) \hat{} B_{P_i,t}(\langle \dots 1N \dots \rangle) \Rightarrow B_{P_i,t}(\langle \dots 1NP_j \rangle)$. 2M

4C. Represent the following protocol using strand space model checking method through a diagram and proper notations. 4M



5A. Specify the security goal and the premise for the following message exchange of a protocol run through multiset belief formalism. 3M

$$Message1\ A \rightarrow B: \{N_A, A\}_{K_B}$$

$$Message2\ B \rightarrow A: \{N_A, N_B\}_{K_A}$$

$$Message3\ A \rightarrow B: \{N_B\}_{K_B}$$

5B. Consider $p = 23,\ \alpha = 5$ and the secret numbers selected by Alice and Bob as 6 and 15 respectively in a D-H protocol. What is the calculated shared secret value between them? 3M

5C. Write the belief multiset formalism based security analysis for the following protocol in a table format. 4M