REG. NO										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY)
END SEMESTER EXAM - APRIL 2018
SUBJECT: DESIGN OF SECURE PROTOCOLS (CSE 5221)
DATE: 17 – 04 – 2018, 9AM – 12AM

TIME: 3 HOURS MAX.MARKS: 50

Instructions to Candidates

- **Note:** Answer all full questions. Missing data can be suitably assumed.

1A. Explain the class of cryptographic protocol which is related to entity/entities authentication. **3M**

1B. Explain the terms *cryptosystem* and *cryptanalysis*. Which cryptographic primitive is called as one *loose one way transformation* and why? **3M**

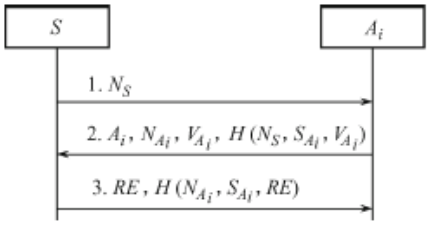
1C. List the reasons why Dolev-Yao (DY) threat model is important and explain the features of DY. **4M**

2A. Explain the $pair - key$ management approach in *sensor networks* along with a neat diagram. Write the notations involved and the message exchange. **5M**

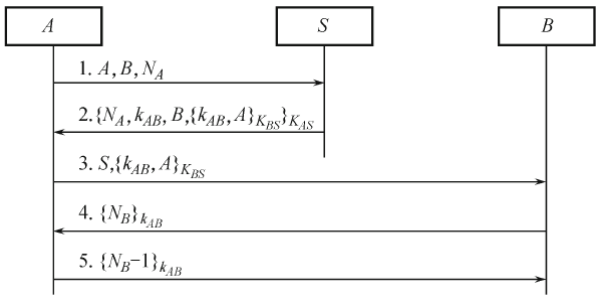
2B. Modify the message $B \rightarrow S: M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$ and show how the data integrity protection is achieved? Which cryptographic primitive suits best for the cryptographic objective "data integrity" in case of symmetric key and public key schemes? **2M**

2C. Explain the *matching conversation* through mathematical symbols. **3M**

3A. What is the disadvantage/drawback in step 3 of the following *Electronic voting protocol* **1M**



3B. Write the signed terms owned by S in *message* 2 in the following protocol. **5M**



3C. Write the security analysis of the DH protocol in a table format using $manual\ security\ analysis\ method$. **4M**

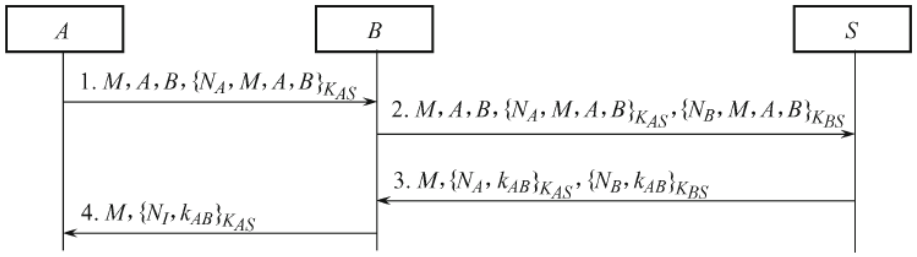
4A. Write the mathematical notations for the following messages: **2M**

a. The principal P_i asserts that the fact ϕ is True, where the fact is principal P_j knows the key k
b. The principal P_i has three assurances. 1) the session key k is confidential, 2) fresh and 3) it is associated with both the principals P_i and P_j

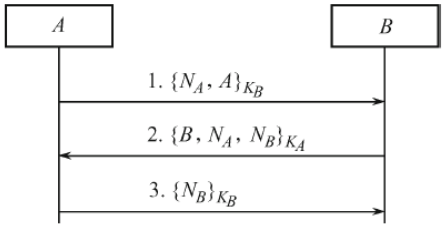
4B. Specify only the $security\ goal$ and the $premise$ for the following message exchange of a protocol run through multiset belief formalism. **3M**

$Message1\ A \rightarrow B: \{N_A, A\}_{K_B}$
$Message2\ B \rightarrow A: \{N_A, N_B\}_{K_A}$
$Message3\ A \rightarrow B: \{N_B\}_{K_B}$

4C. Represent the following protocol using $strand\ space\ model$ checking method through a diagram and use proper notations. **5M**



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



5B. Describe briefly the classification of different types of the channels used in message communication in the secured protocol. **3M**

5C. Consider a use case where you are designing a secure protocol. The programmer has to decide what type of ciphering, what type of MACAlgorithm and what type of encryption algorithm has to be used from the available values in this structure. Write the structure definition which contains the members for each of the following points. Assume the data types. Just a structure definition is expected. This structure is used as a specification for ciphering M and deciphering C. Show the creation of the instance of this specification in the main method **3M**

- Encryption can be done either for the $block\ cipher$ or $stream\ cipher$.
- AES or DES or $DES40$ algorithm can be used for encryption.
- $Md5$, sha can be used for $MACAlgorithm$
- Hash key of 8 $bytes\ length$