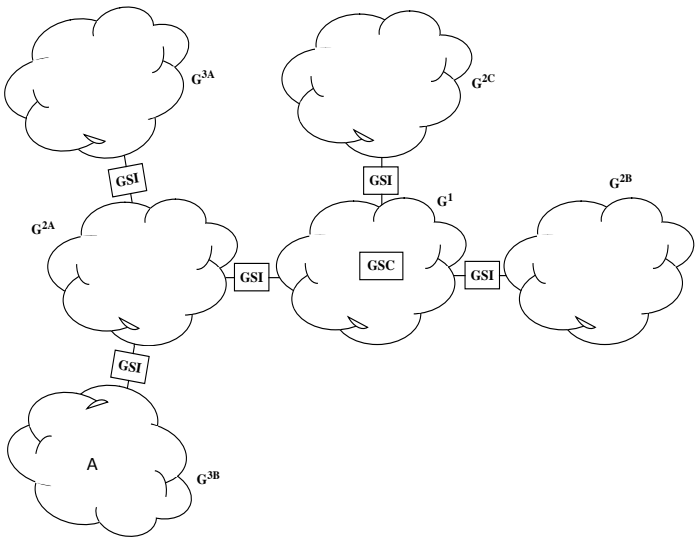
Due date: June 6, 2016 at midnight.

Requirements: HW will be completed by each student individually (no collaboration). Directly borrowing (e.g., copy-paste) from any material and putting in solutions (e.g, from online solutions, Wikipedia, or research papers) isplagiarism (see Syllabus for its corresponding actions).

Please cite very carefully each resource you use, but citing a solution does not give a license to directly put itasan answer.All of your answers must bein your in own words and interpretations. HW should be prepared by LaTeX or Word. Handwritten submissions are not accepted. Note that this homework is extra credit.

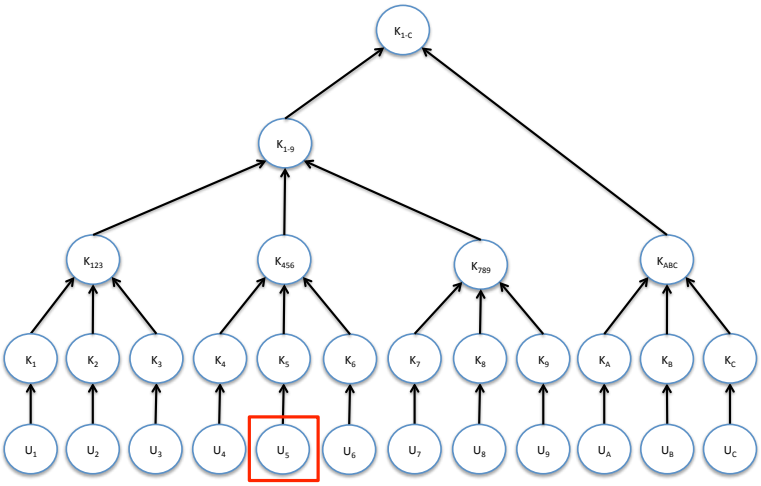
1. (20 points) **Group Diffie-Hellman (GDH)**: We use the GDH3 protocol, and there are five participants in the system. Let α be a generator and q is the order of the algebraic group. M_i denotes the i-th member of the group, N_i is the random exponent generated by the group member M_i. K denotes the group key.
   (a) (10 points) Write the up-flow and down-flow messages, and then show how each member derives the group key K.
   (b) (10 points) Write the number of rounds, total message size, exponentiations per M_i, and total number of exponentiations.

2. (20 points) **Iolus**:
   Consider the following network configuration in which Iolus is used.



Assume the GSC is distributing a new group key to the to the group members using Iolus. How many times will this new key be encrypted and decrypted before A learns the value of the new key? Also describe what entity performs each of the encryptions and decryptions.

3. (12 points) **Key Trees** Consider the following key tree.



   (a) (6 points) If u_5 is removed from the group, what keys should be changed? Write down how keys are distributed with each required step. Assume user oriented re-keying.

   (b) (6 points) Assume a new member is added (at now vacant location u_5). Write down how keys are distributed with each required step. Assume key-oriented re-keying.

4. (20 points) **SSL/TSL**

   (a) (10 points) What is "The Heartbleed Bug", describe in detail how it works against SSL, and how it can be present.

   (b) (10 points) The proper key exchange and cipher suite choices for SSL/TLS continually change. We have discussed a potential key exchange mode and cipher suite selection that would be a reasonable choice at this moment during the class (also with an email). Write down some of the algorithms (discussed on the board), and also state what should be an ultimate care while you configure SSL/TLS (especially while doing international business).

5. (14 points) **Needham-Schroeder, Otway-Rees**

   (a) (12 points) In the Needham-Schroeder protocol (extended version in slides)

      i. (2 points) how is Alice authenticated by the KDC?

      ii. (2 points) How is Bob authenticated by the KDC?

      iii. (2 points) How is the KDC authenticated to Alice?

      iv. (2 points) How is the KDC authenticated to Bob?

v. (2 points) How Alice is authenticated to Bob?

vi. (2 points) How Bob is authenticated to Alice?

(b) (2 points) In the Needham-Schroeder protocol, Alice is the party that is in contact with the KDC, but in the Otway-Rees protocol, Bob is the party that is in contact with the KDC. Explain why this is the case.

6. (14 points) **Kerberos**:

(a) (3 points) When Bob receives a ticket from Alice, how does he know it is genuine?

(b) (3 points) When Bob receives a ticket from Alice, how does he know it came from Alice?

(c) (3 points) When Alice receives a replay, how does he know it came from Bob (that it is not a replay of an earlier message from Bob)?

(d) (5 points) What does the Ticket contain that allows Alice and Bob to communicate securely?