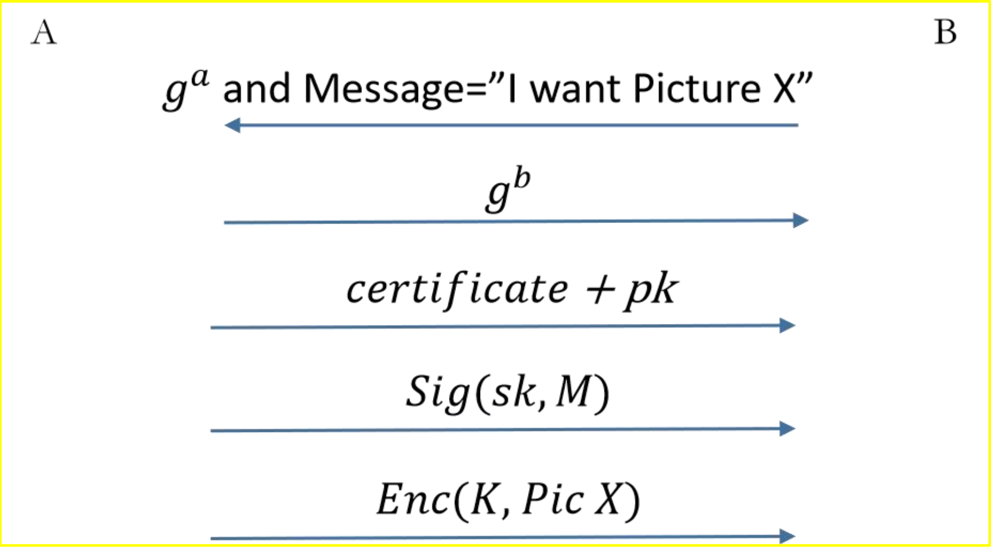
CSCI368 Network Security

Assignment 2 (15 Marks)

Submission Due: **Check Moodle**

Task 1: Read protocol in the below picture and answer questions. The answer to each question cannot be more than 3 sentences.



- Where should K be derived from? (1 mark)
- This protocol uses key transport or key exchange? (2 marks)
- Alice said sending certificate and pk is useless in this protocol. Justify what Alice has said. (3 marks)
- What is the most significant security issue if the signed M includes g^a, g^b only without the Message from B? (3 marks)
- What is the potential security issue if CA forgets to include "subject" in the signed message when generating certificate for A? (3 marks)
- If A and B run the UDP protocol to complete the communication, what could happen at the end of this protocol? (3 marks)

=========END===========

Tips: You are expected to give several keywords to highlight your answer first, followed by your explanations with at most 3 sentences. Same rule will be applied to the final exam.