CS5430 (Fall 2025) Homework 1

General Instructions. You are expected to work alone on this assignment.

Due: Feb 16, 2029 at 11:59pm, No late assignments will be accepted.

Submit your solution using CMS. Prepare your solution as .pdf, as follows:

- Use 10 point or larger font.
- Submit each problem (as a separate file) into the correct CMS submission box for that problem.

Assume that the threat is a Dolev-Yao attacker.

Problem 1: One way to gain a deeper understanding of technical material is to invent multiple-choice questions, since doing this requires inventing incorrect answers that touch on typical misconceptions. Therefore, please devise 5 multiple choice questions for the material covered in the lectures and reading for the introductory part of our course. For each multiple-choice question:

- Give 5 possible choices (a) – (e) for the answer, where only one choice is a correct answer.
- Give a brief explanation (2-3 sentences) justifying the correct answer.
- Give a brief explanation (2-3 sentences) explaining why each of the other choices is not the correct answer.

Problem 2: The starting point for the Needham-Schroeder key distribution protocol is:

```
1.  A --> KDC: A, B
2.  KDC --> A: A, B, {K_AB}K_A
3.  KDC --> B: A, B, {K_AB}K_B
```

This protocol has an awkwardness: `B` could receive an unsolicited message from KDC. That awkwardness prompted our further refinements. But are there other problems with this protocol? Is it possible for an intruder to fool `A` and `B` into using the wrong keys for communicating with each other? If so, exhibit such an attack. If you believe no other attacks are possible then justify your reasoning in a couple of sentences.

Problem 3: The following key distribution protocol was obtained by deleting `n` from all messages in the Otway-Rees authentication protocol.

```
1. A   --> B:   A,B,{r1,A,B}K_A  for fresh r1
2. B   --> KDC: A,B,{r1,A,B}K_A, {r2,A,B}K_B   for fresh r2
3. KDC --> B:   {r1,K_AB}K_A, {r2,K_AB}K_B   for fresh K_AB
4. B --> A:     {r1,K_AB}K_A
```

(a) Can the initial "`A,B`" fields in message 1 be deleted? Explain why or why not.

(b) Can the initial "`A,B`" in message 2 be deleted? Explain why or why not.

(c) What checks on the contents of message 2 should KDC make as a precondition for sending message 3. Why?

(d) What checks on the contents of message 3 should `B` make as a precondition for sending message 4? Why?