1. Given

- A **believes** S **controls** A $\overset{K}{\leftrightarrow}$ B
- A **believes** S **once said** A $\overset{K}{\leftrightarrow}$ B

(a) What other fact(s) would A need to know in order for the following to be true:

{ A **believes** A $\overset{K}{\leftrightarrow}$ B }

(b) Given this additional fact, prove {A **believes** A $\overset{K}{\leftrightarrow}$ B} (show your work)

*over*

2. The paper describes the (flawed) Andrew Secure RPC handshake

1. A $\rightarrow$ B: $\{N_a\}_{K_{ab}}$
2. B $\rightarrow$ A: $\{N_a, N_b\}_{K_{ab}}$
3. A $\rightarrow$ B: $\{N_b\}_{K_{ab}}$
4. B $\rightarrow$ A: $\{$ A $\overset{K'ab}{\leftrightarrow}$ B, $N'_b$ $\}_{K_{ab}}$

and claims that this entitles the following beliefs:

- B **believes** A $\overset{K'ab}{\leftrightarrow}$ B
- A **believes** B **once said** $\{$A $\overset{K'ab}{\leftrightarrow}$ B, $N'_b$ $\}$
- B **believes** A **believes** $N_b$
- A **believes** B **believes** $\{N_a, N_b\}$

But that one is **not** entitled to believe:

- A **believes** A $\overset{K'ab}{\leftrightarrow}$ B

Questions:

1. Why is this belief not justified?

2. How can intruder attack this flawed protocol?

3. How might this protocol be fixed by slightly changing one message?