Problem Set 4 Solutions

Problem 4-1. Logic of Authentication

As we said over email we needed an extra set of assumptions regarding the public keys. So we need to add the following assumptions:

A **believes** $\overset{PB}{\mapsto} B$
B **believes** $\overset{PA}{\mapsto} A$

(a) Let's prove goal 1, that is

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

After message 2 we have that

$$A \ \textbf{sees} \ \{\mathbf{DH}(B, g^y), \ \langle\{\mathbf{DH}(B, g^y), g^x\}_{PB^{-1}}\}\rangle_K$$

Using one of the rules (4) from the BAN paper we can deduce that

$$A \ \textbf{sees} \ \{\mathbf{DH}(B, g^y), g^x\}_{PB^{-1}}$$

Using the SSR rule we can deduce

$$A \ \textbf{believes} \ \mathbf{DH}(B, g^y)$$

and using the DH rule we get to the desired conclusion

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

Similarly for goal 2, that is

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

After message 3 we have that

$$B \ \textbf{sees} \ \langle\{\mathbf{DH}(A, g^x), g^y\}_{PA^{-1}}\rangle_K$$

Using one of the rules (4) from the BAN paper we can deduce that

$$B \ \textbf{sees} \ \{\mathbf{DH}(A, g^x), g^y\}_{PA^{-1}}$$

Using the SSR rule we can deduce

$$B \ \textbf{believes} \ \mathbf{DH}(A, g^x)$$

and using the DH rule we get to the desired conclusion

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

(b) The MACs were not necessary in the deductions above. Indeed we "skipped" them by using the rules (4) from the BAN logic. If the messages were modified as following: 2' . $B \longrightarrow A$: $\mathbf{DH}(B, g^y)$, $\{\mathbf{DH}(B, g^y),\, g^x\}_{PB^{-1}}$
3' . $A \longrightarrow B$: $\{\mathbf{DH}(A, g^x),\, g^y\}_{PA^{-1}}$
then the proof would still go through.

(c) We could not find a way to prove the protocol correct if we remove both the MACs and the SSR rule. Indeed Diffie et al. mention that removing the MACs could create some problems to the security of the protocol (see page 116 of the STS paper.) The idea is that until message 3 B has no idea whom he is talking to. So in message 3 an attacker E could substitute her signature to A's one and the net resultof the protocol is that B thinks he hasexchanged a key with E while he really exchanged the key with A .

(d) We (the teaching staff) tried to prove the original STS protocol (the one with the MACs) with the BAN logic but we failed. Many students experienced the same difficulties. However this does not necessarily mean that the protocol is insecure (many students jumped to that conclusion.) The bug that we encountered was the following: suppose that the attacker E intercepts A's first message. She creates her own Diffie-Hellman key g^y and somehow manages to have the message

$$\{\mathbf{DH}(B, g^y), g^x\} \tag{1}$$

signed with B's public key. Now she sends message 2 and at the end A thinks she exchanged a key with B while she really exchanged key with A.

Problem 4-2. Passwords

The basic idea is to have the screen display a random number r and Alice types on the keyboard $a = p \oplus r$ where p is her password. Now this would be perfectly fine excpet that it requires Alice to perform a XOR in her head, which may not be very convenient for many users. So a way to implement XOR is to have the scree display r and then Alice use the arrow keys in the keyboard to "direct" each digit of r to the right corresponding digit of p.