Answers to Exercise 1

1- In the Dolev-Yao attacker model, an attacker cannot

- ☐ a) eavesdrop all messages
- ☐ b) decrypt all messages
- ☐ c) block all messages
- ☐ d) compose new messages
- ☐ e) create new messages
- ☐ f) decompose messages

2- Assume, in the Dolev-Yao model, the following attacker knowledge:

$$M = \{\{n_1, \{n_2\}_{pk(a)}\}_{inv(pk(a))}\}$$

Which messages can the Dolev-Yao attacker generate?

- ☐ a) n_1
- ☐ b) n_2
- ☐ c) $\{n_1\}_{pk(a)}$
- ☐ d) $\{n_2\}_{pk(a)}$
- ☐ e) $\{n_1, \{n_2\}_{pk(a)}\}_{inv(pk(a))}$
- ☐ f) $\{n_1\}_{inv(pk(a))}$

3- Assume, in the Dolev-Yao model, the following attacker knowledge:

$$M = \{\{n_1, \{n_2\}_{pk(a)}\}_{inv(pk(a))}, inv\ (pk(a))\}$$

Which messages can the Dolev-Yao attacker generate?

- ☐ a) $\{n_1, \{n_2\}_{pk(a)}\}_{pk(a)}$
- ☐ b) $\{n_1, n_2\}_{pk(a)}$
- ☐ c) $\{\{n_1\}_{pk(a)}, \{n_2\}_{pk(a)}\}_{pk(a)}$
- ☐ d) $\{\{n_1\}_{pk(a)}, \{n_2\}_{pk(a)}\}_{inv(pk(a))}$

4- Assume, in the Dolev-Yao model, the following attacker knowledge:

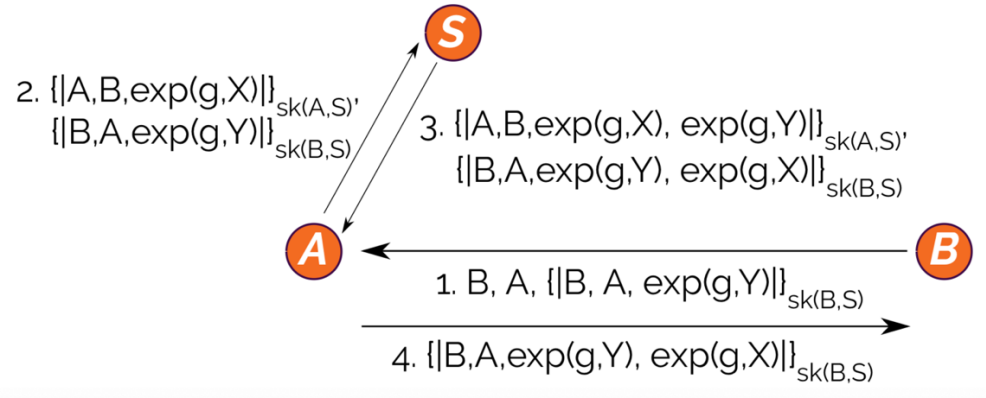
$$M = \{\{n_1, \{n_2\}_{pk(b)}\}_{inv(pk(b))}\}$$

Which messages can the Dolev-Yao attacker generate?

- ☐ a) $\{n_1, \{n_2\}_{pk(b)}\}_{pk(b)}$
- ☐ b) $\{n_1, n_2\}_{pk(b)}$
- ☐ c) $\{\{n_1\}_{pk(b)}, \{n_2\}_{pk(b)}\}_{pk(b)}$
- ☐ d) $\{\{n_1\}_{pk(b)}, \{n_2\}_{pk(b)}\}_{inv(pk(b))}$

Answers to Exercise 2

1- One way of combining both protocols is:



2- Note that the server does not learn the negotiated key $\exp(\exp(g, X), Y)$ of any pair of agents A and B.
Consider an intruder who has recorded all messages between several honest agents and the server. Suppose the intruder is able to break into the server at some point and see all long-term keys $\mathrm{sk}(A, S)$. What concerns all the old recorded traffic, he is now able to decrypt all messages encrypted with $\mathrm{sk}(A, S)$ and thus see what the server could see: the Diffie-Hellman half keys of honest users. The intruder cannot figure out the full keys $\exp(\exp(g, X), Y)$ from any old session, and thus all messages between honest agents based on these keys remain secret. This is called perfect forward secrecy.
In contrast, in the classical protocols like NSCK, the intruder can immediately find out all old session keys once he has compromised the server.

Answers to Exercise 3

1- Non-attack-preserving assumptions can bring great efficiency gains at analysis time. Sometimes it can be a disadvantage to exclude attacks, because the model becomes less general. But restricting the model is not always a bad thing. Some assumptions that add a lot of generality, like for example assuming the intruder can always compromise private keys (maybe by bribing people), introduce attacks that are uninteresting because you cannot really defend against an intruder that powerful anyway.

2- Usually there is some information like port-numbers as part of the plaintext of transmitted messages that are not being authenticated. They play an important role in practice, namely telling the recipient to which protocol the message should be associated – otherwise the recipient would have to try for each protocol if a received message "fits" to that protocol. In our formal models, where we usually omit things like port-numbers, the agents can indeed associate an incoming message to any protocol that they are currently running. Although this in itself is not realistic, it perfectly models that the intruder can change this unauthenticated, non-confidential piece of information and make a receiver parse a message as being part of any protocol where it fits.
   It is different, however, when the information is indeed authenticated in some way (e.g. part of a signed message), which is in general a good idea. Here the agent can check certain properties, e.g., the creator attached information of how to interpret a message that cannot be changed by the intruder. In this case, omitting the information may introduce attacks that are not possible in practice.

Answers to Exercise 4

a) N_B can be observed after two steps: 2
b) $\{|\mathrm{N}_A|\}_{K_{AS}}$ can never be generated by the attacker (attacker cannot obtain K_{AS}): ∞
c) $\{|A|\}_{K_X}$ can directly be generated by the attacker: 0