Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Cornelius Diekmann, M.Sc.
Dr. Ralph Holz

Network Security Winter Term 2014/2015
Exercise 4

Exercise 1 Understanding crypto primitives

a) Some questions with respect to the number of necessary keys:

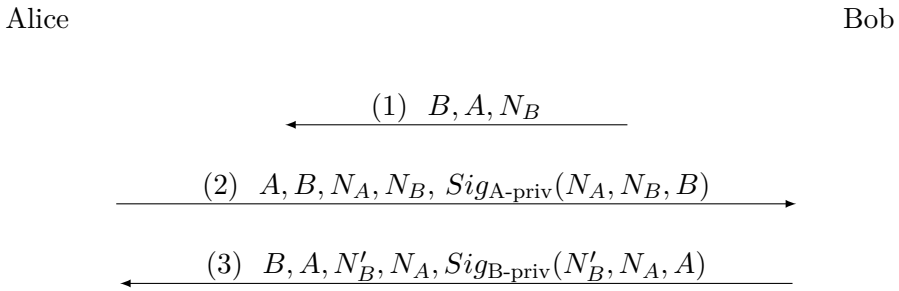
1. Assume there are n users in the system. How many symmetric keys need to exist to support confidentiality between all participants? Use O-notation.
2. If public key cryptography were used for encryption instead of symmetric cryptography, how many keys would be necessary in the system? Use O-notation.

Task 2 Breaking DH

Alice and Bob use the Diffie-Hellman scheme to establish a shared key $K_{A,B}$ over an an insecure channel. Describe how an attacker can perform a Man-In-The-Middle attack (MITM) against the key establishment.

Task 3 Breaking a crypto protocol

Alice, Bob and Mallory are students of Computer Science at the prestigious Terrific University of Madagascar (TUM). At the beginning of the semester, they have all securely pair-wise exchanged their public keys (A-pub, B-pub, M-pub). While Alice and Bob have become good friends, Mallory is secretly very jealous of Alice and only pretends to be friends with the two.
One day, Alice and Bob meet for a coffee at the end of class. Bob is really happy and tells Alice: *I have designed a new authentication protocol. It's really good, look!*



1. B chooses a nonce N_B and sends it to A, explicitly indicating sender and receiver.
2. A responds with a nonce N_A and a signature.

3. B accepts and replies with a new nonce N'_B.

Bob continues: *This ensures the following. When the protocol is complete,*

1. B can be sure that A created message 2 specifically as a response to B's first message. Thus, it must be A with whom B has executed the protocol!

2. The other way around, A can be sure that she is communicating with B because only B can create the signature in the third message!

Alice knows that authentication protocols can be vulnerable in very subtle ways. She takes a good long look at the protocol and then declares: *I am afraid it's broken. An attacker can inject messages such that A would falsely assume she has run the protocol with B, while in fact she was talking to the attacker.*
Bob is down-hearted, so Alice takes pity and explains to him why the protocol is vulnerable. Can you do the same?
Use the following attacker model: Assume that Mallory (M) can control all messages in the network, i. e. read, delete, modify etc. She is only limited by the cryptographic functions, which we assume to be perfect. She does not know any party's private keys (except her own).

a)Show that the **authentication** is broken, as Alice claims. Do this by giving a sequence of message exchanges that conform to the protocol specification yet constitute a violation of Bob's second claim. (Note: **write down the full message exchange, not just your changes!**)

b) State precisely which field in which protocol message causes the vulnerability, and why. Change the thus identified field so the authentication property is not violated anymore. Give the new protocol flow.

c) The following is a variant of Bob's (flawed) protocol that adds a weak kind of key establishment:

Alice Bob

$$\xleftarrow{(1)\quad B, A, N_B, Enc_{\text{A-pub}}(K_B)}$$

$$\xrightarrow{(2)\quad A, B, N_A, N_B,\ Sig_{\text{A-priv}}(N_A, N_B, B), Enc_{\text{B-pub}}(K_A)}$$

$$\xleftarrow{(3)\quad B, A, N'_B, N_A, Sig_{\text{B-priv}}(N'_B, N_A, A)}$$

The shared key is then derived as $(K_A||K_B)$ (i.e. concatenation). Explain why the key establishment does not meet the criteria for Perfect Forward Secrecy (PFS).

d)Show how to enable PFS. Write down the new message flow.

e)We said the key establishment is weak in Bob's version (we do not mean the lack of PFS here). That is because there is a hidden vulnerability in there. Which one? (Say why!)