T-110.5241 Network security
Examination 2012-12-17
Lecturer: Tuomas Aura
No electronic equipment or reference material is allowed in the examination.

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. Authentication protocols

Consider the following key-exchange protocol based on Diffie-Hellman.

1. A → B: g^x, N_A, $Sign_A(g^x, N_A)$, $Cert_A$
2. B → A: g^y, N_B, $Sign_B(g^y, N_B)$, $Cert_B$

A and B calculate SK = ???

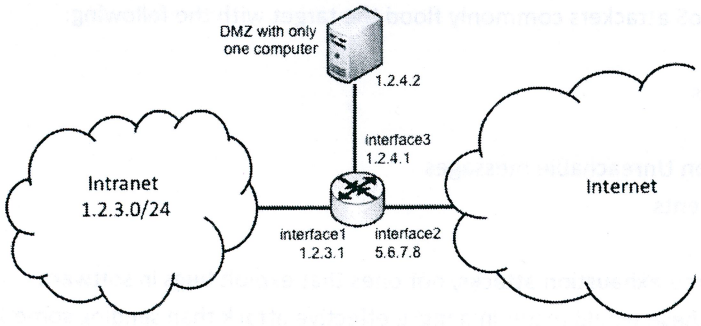
3. A → B:
4. B → A:

(a) What would be a good way to calculate the session key SK? Explain just one way with sufficient detail for it to be implemented.
(b) Does this protocol provide perfect forward secrecy? Explain you reasoning.
(c) Add messages 3 and 4 to implement entity authentication and key confirmation. Keep these messages as simple as possible.

2. Firewalls

Define an anti-spoofing policy for the router in the picture below. The goal is to filter as many packets with spoofed source IP addresses as possible.

Note: Use some easy-to-understand notation for the policy. The policy should be a list of rules, each consisting of conditions (or selectors) and an action. For each packet, the first matching rule is chosen, and the action specified in that rule is taken.



Please turn the paper for problems 3–6.