T-110.5241 Network security

Examination 2011-12-12

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
2. B → A: g^y, $E_{SK}(g^y, g^x, Sign_B(g^y, g^x), Cert_B)$
3. A → B: $E_{SK}(g^x, g^y, Sign_A(g^x, g^y), Cert_A)$

SK = $h(g^{xy})$

(a) What is $Cert_B$, and how does B obtain it?

(b) Modify the protocol so that the exponents x and y can be reused for a limited time period.

(c) How do the security properties of the protocol change when the modification of part (b) is made? Explain why.

2. IPsec

Consider the tunnel and transport modes in IPsec.

(a) What headers are there on the tunnel-mode and transport-mode packets? Draw a picture.

(b) What are the typical applications for tunnel and transport mode?

(c) Would just one of these two modes be sufficient for all applications? What would the advantages and disadvantages be?

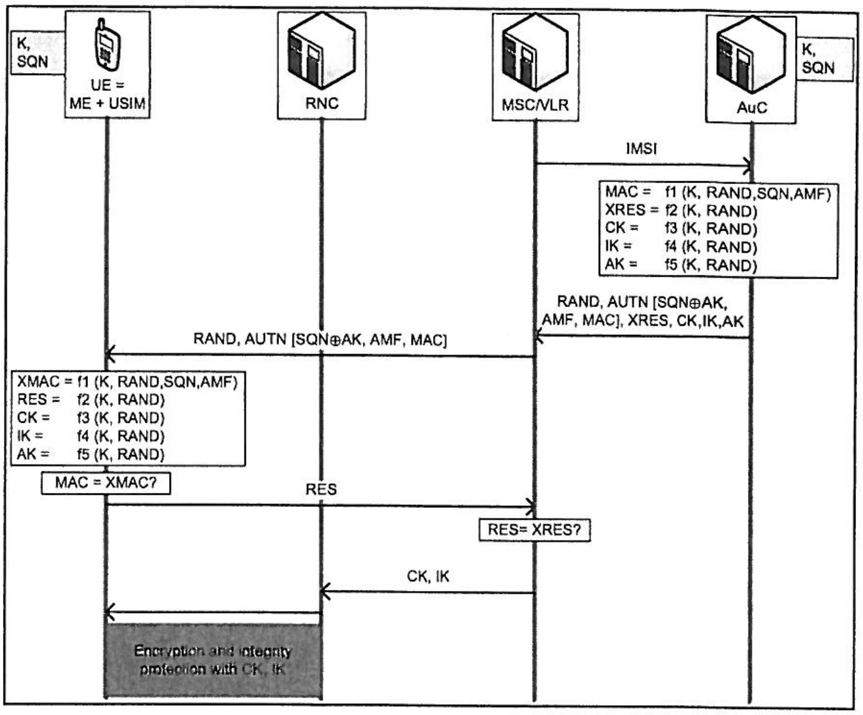
3. Authentication

Explain what a Lamport hash chain is and how it can be used for authentication.

Please turn the paper for problems 4–6.

4. Cellular security

Explain the security and performance requirements that have influenced the design of UMTS AKA (see the picture below), and how they are reflected in the protocol.



5. Wireless security

Alice has configured her wireless router (router with a built-in WLAN access point) and laptop computer to use WPA2-Personal. Explain the protocol that takes place when the laptop computer connects to the access point.

6. Mobility protocol

When you move houses, you can ask the post office to forward your physical mail from the old address to the new one. Consider the threats, attacks, and defense mechanisms from mobility protocols (for example, Mobile IPv6): which of the threats and attacks are relevant to the physical mail forwarding, and how could they be mitigated?