Exam: Security in Networks

1 points for each correct solved problem. To pass 5.5 points are needed.

1. Which of the security mechanisms (Confidentiality, Integrity, Accountability, Nonrepudiation , Authentication of the sender) are needed and which are not, with respect to the following applications.

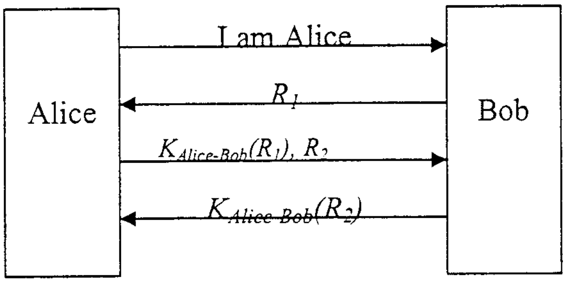
    - Transfer of a project plan.
    - Invitation of a friend for dinner.
    - Selling of illegal cracked software via the internet.
    - Operation of an illegal gambling casino via the internet
    - Transfer of a new mission plan to James Bond
    - Send an order for goods.
    - Statement of accusation at the police against your boss.
    - Send a love letter.
    - Send a ransom demand.
    - Send a job application to a head-hunter.

2. Why is the following secret key authentication protocol flawed? Alice chooses a separate message key K for each message m to be sent. For each receiver *X*, there exists an individual secret key $K_{Alice\text{-}X}$ that is known only to Alice and *X*. Each transmitted multicast message from Alice consists of:

    - a header, containing the coded message keys $K_{Alice\text{-}X}$ (K) for each receiver *X* in the multicast group,
    - the coded message K(m), and
    - a message identification code (MIC_K) of the message, e.g. DES-CBC Residue or a Message Digest based on the message and K.

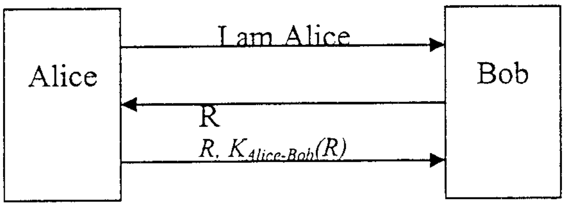
(Please note, that the protocol is working correctly for a single receiver inside the multicast group.)

3. Check whether the following protocol is secure!

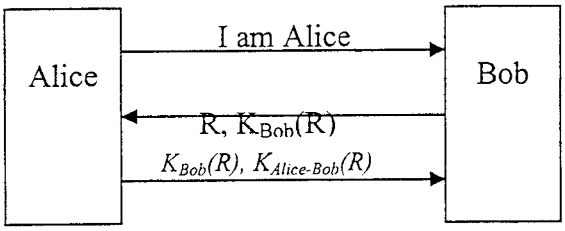


4. In the following two authentication protocols are discussed, each protocol describing the exchange of three messages.

   - In the first case Bob corresponds to a connection-less server. As a reaction to Alice's request Bob sends a random number R. Alice answers to this message with the random number and the encrypted random number $K_{Alice-Bob}(R)$. Is the protocol secure?



   - We now enhance the first protocol by extending Bob's message by additionally including the random number encrypted with a secret key K_{Bob}. Alice must include this secret message in her answer. Is the protocol secure?



5. Assume that Alice would like to communicate with Bob, using 3 chained Key Distribution Centers (KDCs). Indicate the sequence of messages required to establish the connection. What can Bob do, if he wants not trust all KDCs? (Note: give a solution using symmetric keys!)

6. Alice and Bob want to communicate over an insecure medium.

   a) Design, on the basis of shared secret key K_{AB}, a protocol, which enables Alice and Bob to authenticate each other. Assume, that the shared secret key K_{AB} has been negotiated before.

   b) What are the disadvantages related to the use of a shared key?

7. RSA uses large numbers, therefore there is a need for some tricks to speed up computations
   a) Give a method so that the number of multiplications and divisions increases linearly with length of exponent in bits
   b) Use the method to calculate 38^{75} mod 103

8. Calculate the hash value of the sentence “the quick brown fox jumps over the lazy dog”[1] using the following hash function:
   a) Sum of all character codes divide by the number of characters.
   b) Sum of all character codes multiplied by the position of the character modulo 256
   c) Sum of the digits off all character codes (write all character codes next to each other and add all digits) modulo 32

   Determine, which of the above hash functions were used to calculate the following hash values:

   d) hash(„the quick brown“) = 14
   e) hash(„fox jumps over“) = 208
   f) hash(„the lazy dog“) = 96

9. What is a cryptographic hash function? Why do several messages have the same hash value? Which property of a hash function prevents an attacker from exploiting this?

10. Firewalls and Intrusion Detection
    1. Why must the system clock of a network be protected?
    2. Describe the Screen Subnet Architecture (with DMZ).
    3. Which kind of hosts are placed in the DMZ?
    4. Compare misuse and anomaly detection (advantages and disadvantages).
       (1) How can you combine both approaches?

[1] This sentence corresponds to the ASCII-Codes: 116, 104, 101, 32, 113, 117, 105, 99, 107, 32, 98, 114, 111, 119, 110, 32, 102, 111, 120, 32, 106, 117, 109, 112, 115, 32, 111, 118, 101, 114, 32, 116, 104, 101, 32, 108, 97, 122, 121, 32, 100, 111, 103