EXAM questions for the course TTM4137 - Wireless Security
29th November 2007 0900-1300 H

KEY for Part 1

1. d
2. e
3. a
4. b
5. b
6. b Ambiguous question, more than one possible answer
7. b
8. a
9. c
10. a
11. e
12. a
13. e
14. e
15. d
16. e
17. d Ambiguous question, more than one possible answer
18. e
19. a
20. c

EXAM questions for the course TTM4137 - Wireless Security 29th November 2007 0900-1300 H

KEY for Part 2

TOPIC:

1. *f0: random challenge generation, f1: network message authentication, f1*: resynchronization message authentication, f2: user authentication, f3: cipher key derivation, f4: integrity key derivation, f5: anonymity key derivation, f5*: anonymity key derivation for resynchronization, f8: confidentiality, f9: integrity*
2. *See fig 2.1 and 2.2 in textbook*
3. *The purpose of SQN is to provide the user with proof that the authentication vector is fresh. The three ways of generating SEQ: 1. SEQ is an individual counter and its current value is maintained in a database independently for each user. 2. SEQ is based on a global counter, and for each user a deviation from the global counter, called DIF, is maintained in a database. 3. SEQ has two parts SEQ=SEQ1||SEQ2 where SEQ1 is an individual counter and SEQ2 is based on a global counter. The value of SEQ is maintained in a database for each user.*
4. *OP is there to provide separation between the functionality of the algorithms when used by different operators. OP_C is a subscriber-dependent value of OP, it is XORed to the input and output of the kernel functions, thus providing additional protection against attacks. $OP_C=OP \oplus E_K(OP)$*
5. *RLC transparent mode (MAC layer encryption), Unacknowledged mode (UM) (RLC layer encryption), Acknowledged mode (AM) (RLC layer encryption)*
6. *Part of the IV consists of a time-dependent counter COUNT-C. COUNT-C consists of a combination of the counter HFN (Hyper Frame Number) and a shorter counter that changes for each PDU (Connection Frame Number for MAC and RLC sequence number for RLC). HFN is set to zero whenever a new key is generated during AKA to avoid wrap-around.*
7. *MAC-I is computed with the f9 function at the sending side and appended to each RRC message. MAC-I is also computed at the receiving side and the result is checked against the bit string appended to the message. The signaling messages at the RRC layer are considered the most sensitive and important and are thus integrity protected, i.e. the encryption on/off message.*
8. *See fig 6.6 on p. 164 in textbook*

EXAM questions for the course TTM4137 - Wireless Security
29th November 2007 0900-1300 H

KEY for Part 3

1. *Packet leashes are used to defend against wormhole attacks. Main idea: a receiver can determine if the packet has traveled an unrealistic distance. Geographical packet leashes: the receiver computes an upper bound on the distance between the sender and itself based on the timestamp t_s in the packet, the local receive time t_r, the maximum relative error in location information δ, and the locations of the receiver p_r and the sender p_s. $d_{sr} \leq ||p_s - p_f|| + 2v \cdot (t_r - t_s + \Delta) + \delta$. We assume sender and receiver's clocks are synchronized to within $\pm\Delta$ and that the maximum velocity of a node is v.*
2. *An attacker that owns all nodes on a vertex cut through the network, that partitions the good nodes into multiple sets. This is a powerful attacker because it controls all traffic between nodes of the disjoint partitions.*
3. *Advantages: no need to set up symmetric keys in network nodes, adding new nodes to the network is easy. Disadvantages: larger routing message size because of the need of adding certificates, computing overhead in verifying signatures, vulnerability to DoS attacks, the need of CA, certificate revocation problem*
4. *See figure 2 on p. 34 in the paper.*