TTM4137 Exam Dec. 4, 2009 Solution Outline

sfm, Dec. 16, 2009

Part I. Wireless Networks Security Facts

1a, 2a, 3b, 4b, 5d, 6a, 7c, 8a, 9d, 10c, 11a, 12a, 13b, 14a, 15b, 16d, 17c, 18a, 19c, 20a, 21b, 22d, 23a, 24a, 25d.

Part II. Authentication Protocols

26.

```
Procedure Verify1
XMAC ← $f1_k$(IMSI,RAND,XSID)
if MAC $\neq$ XMAC then send(ERROR)
else ...
```

```
Procedure Verify2
XRES ← $f2_K(RAND)$
if RES $\neq$ XRES then send(ERROR)
else send(ACK)
```

27. At the UE side: the random generator function $f0()$ and the Verify2 procedure. At the VTRAN side: The Verify1 procedure.

28. $|\text{AUTV}| + |\text{RES}| + |\text{ACK}| = (128 + 128 + 64) + 128 + 1 = 449$ bits. $|\text{IMSI}|+|\text{AUTN}|+|\text{RAND}|+|\text{RES}|+|\text{ACK}| = 128+128+128+\text{range}[32 \cdots 128]+1 = \text{range}[417 \cdots 513]$ bits.

29. For example, the key distribution proocol of UMTS can be used, see Fig.2.1 and 2.15 in the text book.

30. VTRAN will detect XMAC$\neq$MAC, but VTRAN cannot determine the cause of the error without more information. If the SID value is included in AUTV then VTRAN are able to determine whether the error is caused by SID$\neq$XSID, and initiate a resynchronization protocol. The resynchronization procedure can, for example, take the idea of AUTS in Figures 2.6 and 3.11 of the text book. Sections 2.1.1.3, 2.1.1.4 and 2.1.1.5 describe the design in UMTS.

UE → VTRAN:	(IMSI,RAND, SID⊕AK, MAC-S)
UE ← VTRAN:	(XSID⊕AK, MAC-S)
UE	If MAC-S ok then resynch SID.

Part III. Analysis of IV implementation

31. $p_{42} = 2^{-8}$. $H(X_u) = 2^8 \cdot 2^{-8} \log_2 2^8 = 8$.

32. $p_k = \frac{1.36}{256} = 0,0053125$. $H(X_s) = p_k \cdot \log_2 \frac{1}{p_k} + 255\frac{1-p_k}{255} \log_2 \frac{255}{1-p_k} = 0.0401433 + 7.9595273 = 7.9996707$

33. $D(X) = H(X_u) - H(X_s) = 0.0003293$

34. $U = \lceil 8/0.0003393 \rceil \frac{\text{bits}}{\text{bits/value}} = 24294$ values

35.

$$n = \lceil \frac{\ln{(1 - 24294 \cdot 2^{-24})}}{\ln{(1 - 2^{-24})}} \rceil = 24314$$