TTM4137 Exam Answers, Dec. 17, 2015

Part I

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

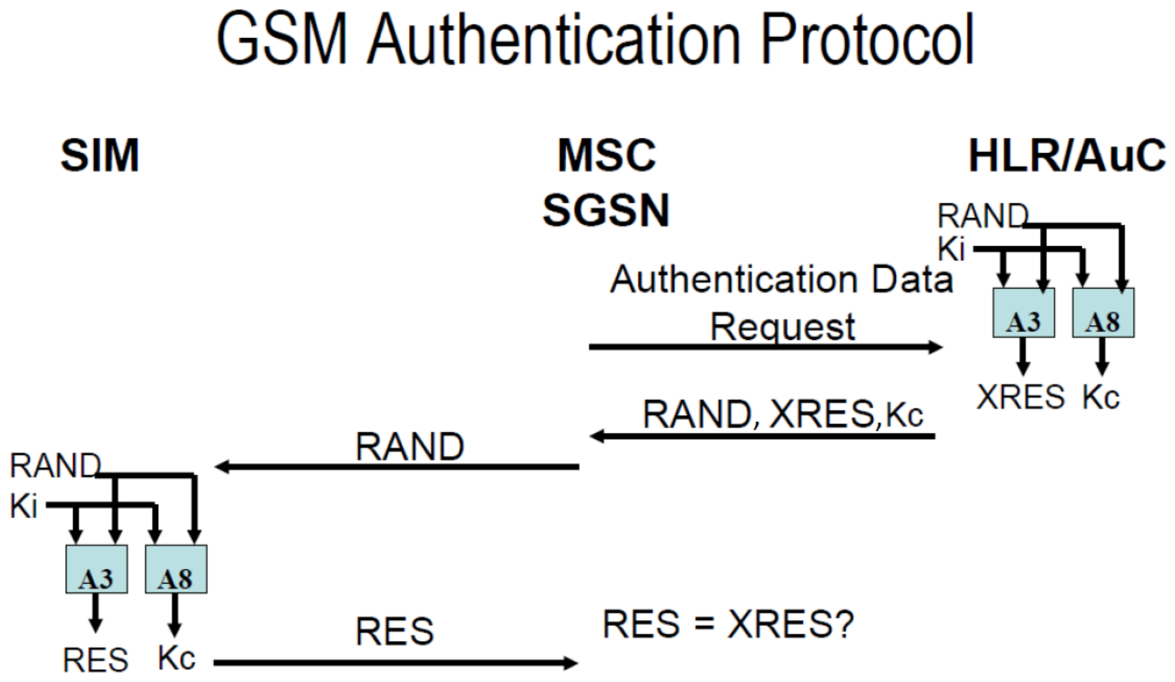
Part II

26.

Ki (128 bits), RAND (128 bits) -> A3 -> SRES/XRES (32 bits)

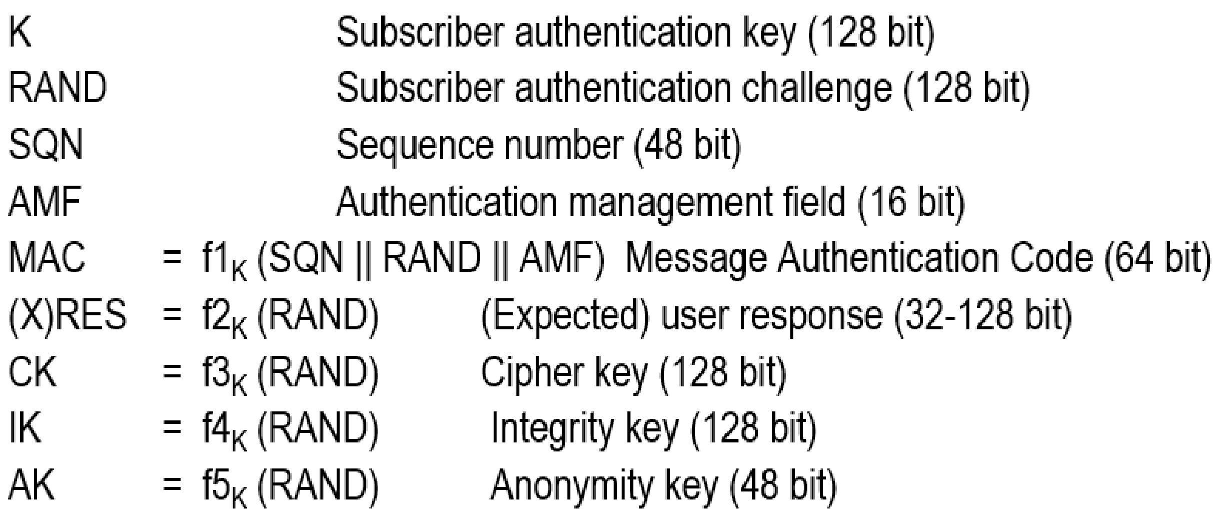
Ki (128 bits), RAND (128 bits) -> A8 -> Kc (54/64 bits)

27.



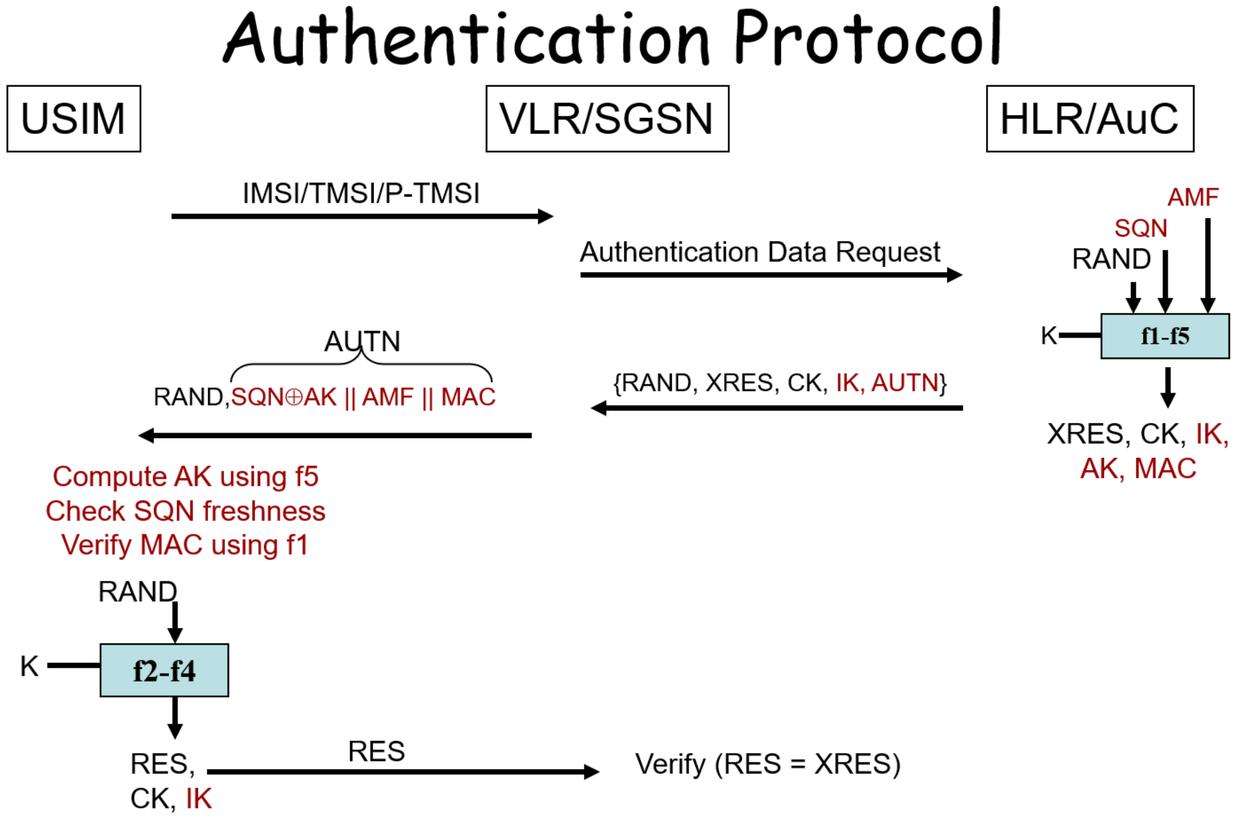
GSM Authentication Protocol

28.



K		Subscriber authentication key (128 bit)
RAND		Subscriber authentication challenge (128 bit)
SQN		Sequence number (48 bit)
AMF		Authentication management field (16 bit)
MAC	= $f1_K$ (SQN || RAND || AMF)	Message Authentication Code (64 bit)
(X)RES	= $f2_K$ (RAND)	(Expected) user response (32-128 bit)
CK	= $f3_K$ (RAND)	Cipher key (128 bit)
IK	= $f4_K$ (RAND)	Integrity key (128 bit)
AK	= $f5_K$ (RAND)	Anonymity key (48 bit)

29.



Authentication Protocol

USIM

VLR/SGSN

HLR/AuC

IMSI/TMSI/P-TMSI

Authentication Data Request

AMF

SQN

RAND

K

f1-f5

XRES, CK, IK, AK, MAC

{RAND, XRES, CK, IK, AUTN}

AUTN

RAND,SQN⊕AK || AMF || MAC

Compute AK using f5
Check SQN freshness
Verify MAC using f1

RAND

K

f2-f4

RES, CK, IK

RES

Verify (RES = XRES)

30. UMTS AKA provides mutual authentication. GSM authentication only authenticates the SIM to the network, not the network to the SIM.

31. The simplest procedure for setting up a false base station is to disable encryption (A5/0), then masquerade as a legitimate base station. Since the SIM does not authenticate the network, it is not able to detect the false base station. This attack is able to intercept ME initiated calls and messages, but not incoming calls and messages. More sophisticated attacks use vulnerable ciphers (A5/1 or A5/2) to break the session key, which enables two-way interception of calls and messages.

32. Yes, it is vulnerable. The false base station can downgrade the security of the ME. The attack consists of two stages. First, masquerade as the victim UE to obtain a fresh RAND and AUTN from the network. Then, use these to masquerade as a base station to the victim. Since the GSM cipher mode command is not protected, the false base station can disable encryption after the AKA procedure. See slides from Lecture 8 for details.

33. The serving network also (implicitly) authenticates itself to the UE in EPS/LTE through cryptographic network separation using the SNid. That is not the case in UMTS, where only the home network authenticates itself to the USIM.

34. Since the UE can be instructed to not use LTE, then the attack from question 32 can be used. For details, see: “Practical attacks against privacy and availability in 4G/LTE mobile communication systems” by Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. P.

Part III

35. One possible attack is to set up a rogue access point with a web page asking for credentials, preferably using the same SSID as SecureCorp’s network. Any other attack that would work in practice and that does not break the constraints in the assignment should be accepted.

36. One approach would be to extract the GTK, then use ARP poisoning to act as a man-in-the-middle for all the traffic. There may be other ways to achieve the goal, so other creative attacks are also accepted as long as they do not break the constraints given in the assignment.

37. One obvious recommendation is to use a stronger EAP method, such as EAP-TLS. Another possible recommendation is to use VPN with two-factor authentication. If a rogue access point was used to obtain the password, then user awareness training is also a valid recommendation. The recommendations must reflect the vulnerabilities exploited in 35. and 36.