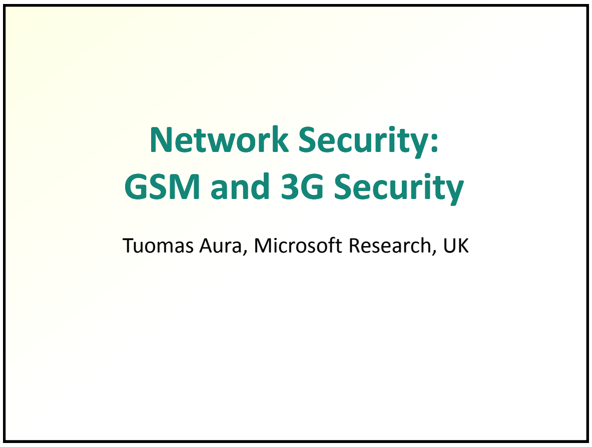
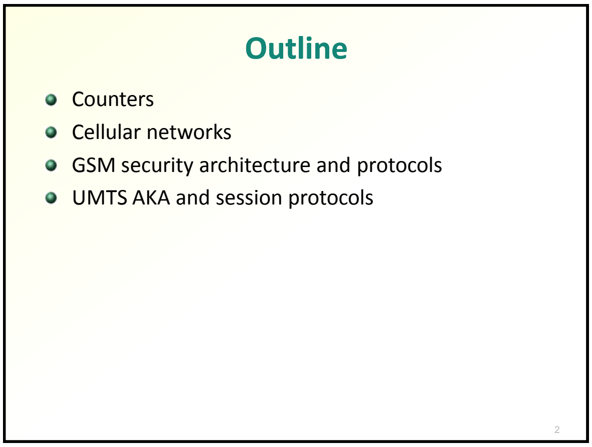


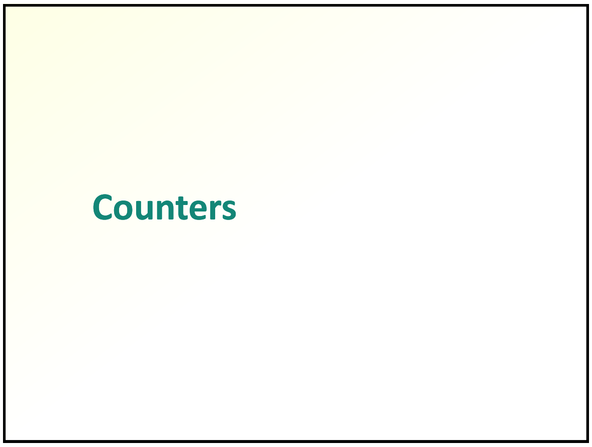
Network Security: GSM and 3G Security

Tuomas Aura, Microsoft Research, UK

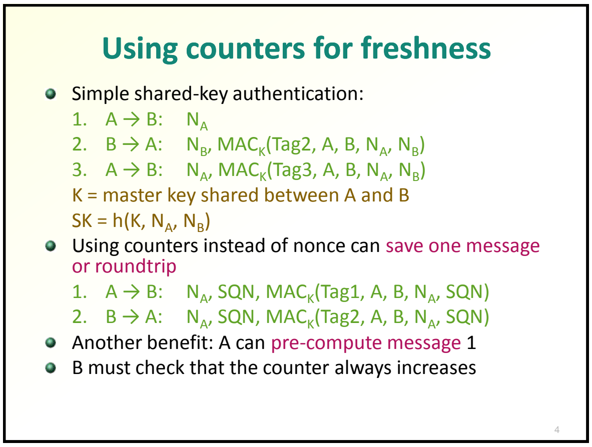


Outline

- Counters
- Cellular networks
- GSM security architecture and protocols
- UMTS AKA and session protocols



Counters

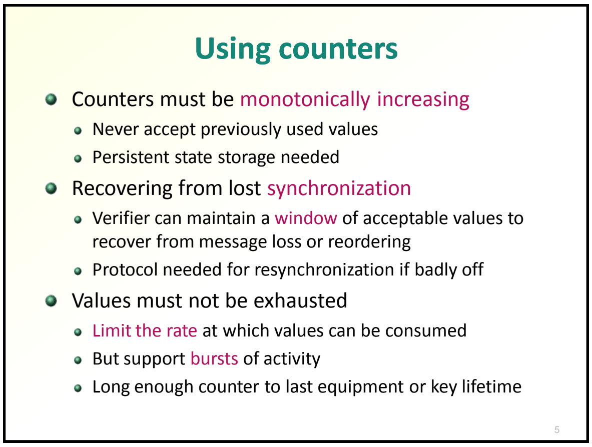


Using counters for freshness

- Simple shared-key authentication:
  1. A → B: N_A
  2. B → A: N_B, MAC_K(Tag2, A, B, N_A, N_B)
  3. A → B: N_A, MAC_K(Tag3, A, B, N_A, N_B)

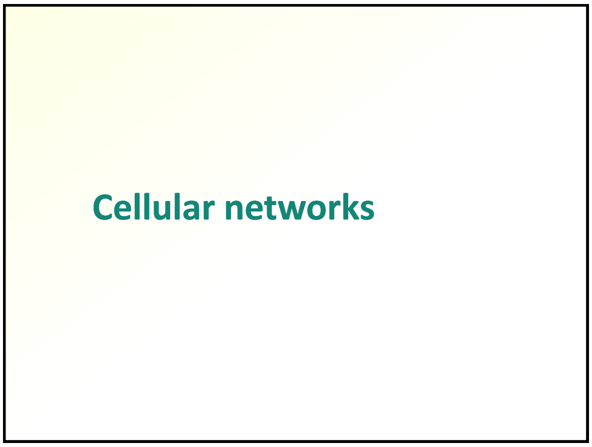
  K = master key shared between A and B

  SK = h(K, N_A, N_B)
- Using counters instead of nonce can save one message or roundtrip
  1. A → B: N_A, SQN, MAC_K(Tag1, A, B, N_A, SQN)
  2. B → A: N_A, SQN, MAC_K(Tag2, A, B, N_A, SQN)
- Another benefit: A can pre-compute message 1
- B must check that the counter always increases



Using counters

- Counters must be monotonically increasing
  - Never accept previously used values
  - Persistent state storage needed
- Recovering from lost synchronization
  - Verifier can maintain a window of acceptable values to recover from message loss or reordering
  - Protocol needed for resynchronization if badly off
- Values must not be exhausted
  - Limit the rate at which values can be consumed
  - But support bursts of activity
  - Long enough counter to last equipment or key lifetime



Cellular networks

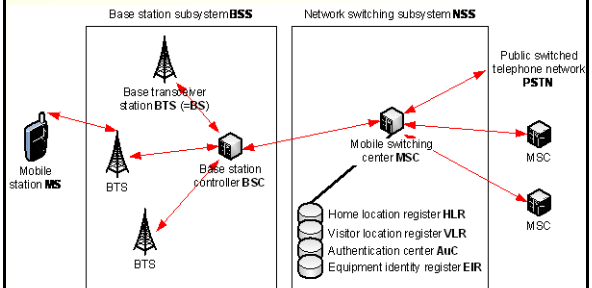
History

- GSM
  - Groupe Spéciale Mobile (GSM) founded in 1982
  - Standardized by European Telecommunication Standards Institute (ETSI)
  - Renamed Global System for Mobile Communications (GSM)
  - First Release in 1990, GPRS (2.5G) in 1997
- UMTS
  - Universal Mobile Telecommunications System (UMTS)
  - Standardized by the 3rd Generation Partnership Project (3GPP) formed by ETSI and Japanese, Korean and Chinese standards bodies
  - First Release 1999
  - High-Speed Downlink Packet Access (HSDPA) standardized in 2001; coming to wide use now

GSM network

- Mobile station (MS) = mobile equipment (ME) + subscriber identity module (SIM)
- Base station subsystem (BSS) = base station controller (BSC) + base transceiver stations (BTS)
  - BTS = base station (BS)
- Network switching subsystem (NSS) = mobile switching centers (MSC) and their support functions
  - MSC is an advanced telephone exchange
  - MSC uses the SS7 signalling network (but moving to IP)
- Advanced functions (not covered in this lecture):
  - Text messages
  - GPRS, HSDPA
  - IP multimedia subsystem (IMS)

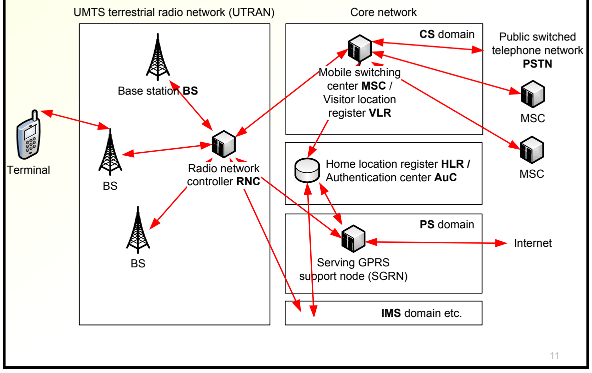
GSM network architecture


Base station subsystem **BSS**
Network switching subsystem **NSS**
Base transceiver station **BTS** (=**BS**)
Mobile station **MS**
BTS
Base station controller **BSC**
BTS
Mobile switching center **MSC**
Public switched telephone network **PSTN**
MSC
MSC
Home location register **HLR**
Visitor location register **VLR**
Authentication center **AuC**
Equipment identity register **EIR**

UMTS network

- Based on the GSM architecture
- User equipment (UE) i.e. terminal = mobile equipment (ME) + universal subscriber identity module (USIM)
- UMTS terrestrial radio access network (UTRAN) = radio network controller (RNC) + base stations (BS)
- Core network = different service domains + home location register
- 3GPP Release 8 specifies an all-IP network for signalling and data, but deployment will take time
- Circuit-switched (CS) domain for voice
- Packet-switched (PS) domain for IP data

UMTS architecture


UMTS terrestrial radio network (UTRAN)
Core network
Base station **BS**
Terminal
BS
Radio network controller **RNC**
BS
CS domain
Mobile switching center **MSC** / Visitor location register **VLR**
Public switched telephone network **PSTN**
MSC
MSC
Home location register **HLR** / Authentication center **AuC**
PS domain
Serving GPRS support node (SGRN)
Internet
IMS domain etc.

Threats against cellular networks

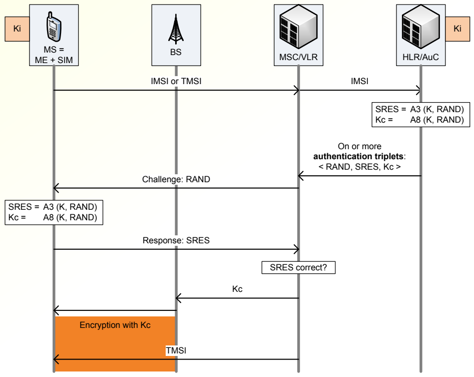
- Discussion: What the threats?
- Charging fraud, unauthorized use
- Charging disputes
- Handset cloning (impersonation attack)
  - → multiple handsets on one subscription
  - → let someone else pay for your calls
- Voice interception → casual listening and industrial espionage
- Location tracking
- Handset theft
- Network service disruption
- What about intergrity?

GSM security

GSM security architecture

- Home location register (HLR) keeps track of the mobile's location
- Visitor location register (VLR) keeps track of roaming mobiles at each network
- Shared key Ki between SIM and authentication center (HRL/AuC) at the home network
- VLR of the visited network obtains authentication triplets from AuC of the mobile's home network and authenticates the mobile
- Encryption between mobile and the base station

GSM authentication



GSM authentication

- Alice-and-Bob notation:
  1. Network → MS: RAND
  2. MS → Network: A3 (Ki, RAND)

  Ki = shared master key

  Kc = A8 (Ki, RAND) — session key
- After authentication, BS asks mobile to turn on encryption. A5 cipher with the key Kc

GSM security

- Mobile authenticated → prevents charging fraud
- Encryption on the air interface
  → No casual sniffing
  → Encryption of signalling gives some integrity protection
- TMSI → not easy to track mobile with a passive radio
- Algorithms A3, A8 can be replaced
  - AuC and SIM must use the same algorithms
- Non-protocol features:
  - Subscriber identity module (SIM) card separate from handset
    → Flexibility
    → Thiefs and unlockers don't even try to break the SIM
  - International mobile equipment identity (IMEI) to track stolen devices

GSM security weaknesses

- Only the mobile is authenticated, network not
- BS decides when to turn on encryption; mobiles have no indicator
  → Possible to set up a fake BS that uses no encryption
- Integrity protection depends on encryption but some networks do not use encryption
- Decryption at BS, but BS may be at a hard-to-monitor location and compromised
- Early encryption algorithms based on COMP128, which has been broken. A5 cannot be upgraded without replacing the handset
- Authentication triplets transferred over the SS7 signalling network, which can be accessed by thousands of operators
- No non-repudiation → no protection against false charges from dishonest operators
- IMSI sent when requested by BS → IMSI catchers to track mobiles
- IMEI not authenticated → can be changed to prevent the tracking of stolen mobiles

UMTS improvements over GSM

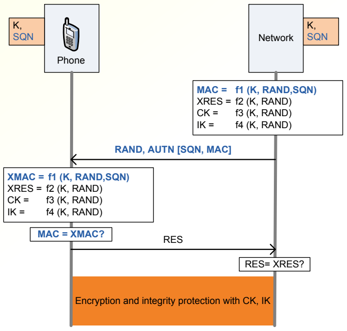
- RAN separate from CN
  - Roles of radio-network operator and service operator separated
- Encryption endpoint moved from BS to RNC
- Mutual authentication protocol AKA
- Support for multiple service domains
  - Circuit-switched, packet-switched, multimedia, WLAN
- Protection of core-network signalling
- Security indicator to user (e.g. encryption off)

UMTS authentication and key agreement (AKA)

UMTS AKA

- AKA = authentication and key agreement
- Based on GSM authentication
- Mutual authentication
- Sequence number for freshness to mobile
  → saves one roundtrip to AuC
  → authentication vectors can be retrieved early, several at a time

UMTS AKA (simplified)


K, SQN

Phone

Network

K, SQN

MAC = f1 (K, RAND,SQN)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)

RAND, AUTN [SQN, MAC]

XMAC = f1 (K, RAND,SQN)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)

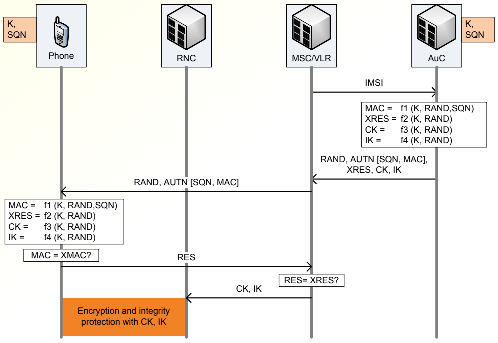
MAC = XMAC?

RES

RES= XRES?

Encryption and integrity protection with CK, IK

UMTS AKA (simplified)


K, SQN

Phone

RNC

MSC/VLR

AuC

K, SQN

IMSI

MAC = f1 (K, RAND,SQN)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)

RAND, AUTN [SQN, MAC], XRES, CK, IK

RAND, AUTN [SQN, MAC]

MAC = f1 (K, RAND,SQN)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)

MAC = XMAC?

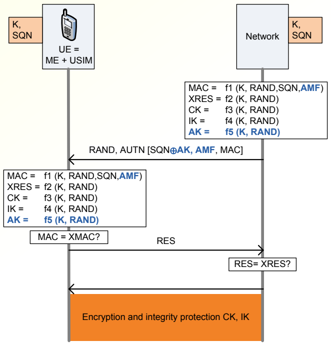
RES

RES= XRES?

CK, IK

Encryption and integrity protection with CK, IK

UMTS AKA


K, SQN

UE = ME + USIM

Network

K, SQN

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

RAND, AUTN [SQN⊕AK, AMF, MAC]

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

MAC = XMAC?

RES

RES= XRES?

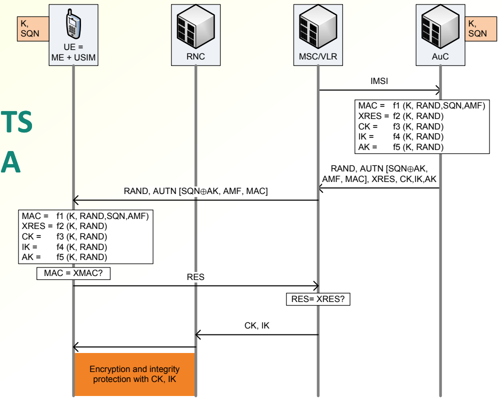
Encryption and integrity protection CK, IK

UMTS authentication

- Alice-and-Bob notation:
  1. Network → terminal: RAND, SQN⊕AK, f1 (K, RAND, SQN)
  2. Terminal → Network: f2 (K, RAND)

  CK = f3 (K, RAND)
  IK = f4 (K, RAND)
  AK = f5 (K, RAND)
- USIM must store the highest received SQN value
- AuC must also store SQN and increment it for each authentication
- Masking SQN with AK prevents the use of SQN to identify the mobile

UMTS AKA


K, SQN

UE = ME + USIM

RNC

MSC/VLR

AuC

K, SQN

IMSI

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

RAND, AUTN [SQN⊕AK, AMF, MAC], XRES, CK,IK,AK

RAND, AUTN [SQN⊕AK, AMF, MAC]

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

MAC = XMAC?

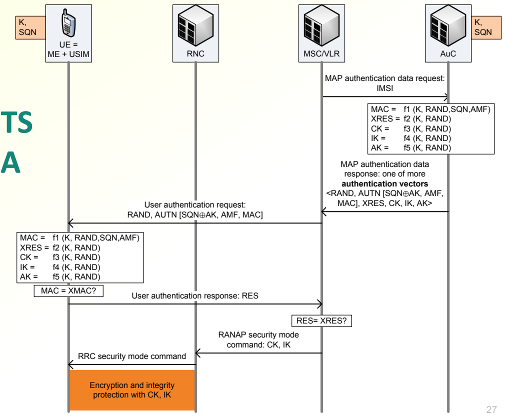
RES

RES= XRES?

CK, IK

Encryption and integrity protection with CK, IK

UMTS AKA


K, SQN

UE = ME + USIM

RNC

MSC/VLR

AuC

K, SQN

MAP authentication data request: IMSI

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

MAP authentication data response: one of more **authentication vectors** <RAND, AUTN [SQN⊕AK, AMF, MAC], XRES, CK, IK, AK>

User authentication request: RAND, AUTN [SQN⊕AK, AMF, MAC]

MAC = f1 (K, RAND,SQN,AMF)
XRES = f2 (K, RAND)
CK = f3 (K, RAND)
IK = f4 (K, RAND)
AK = f5 (K, RAND)

MAC = XMAC?

User authentication response: RES

RES= XRES?

RANAP security mode command: CK, IK

RRC security mode command

Encryption and integrity protection with CK, IK

Sequence number SQN

- Implementation can be changed in USIM and AuC
  - Length is fixed to 48 bits
- One suggested implementation:

SEQ1 (19 bits)	SEQ2 (24 bits)	IND (5 bits)

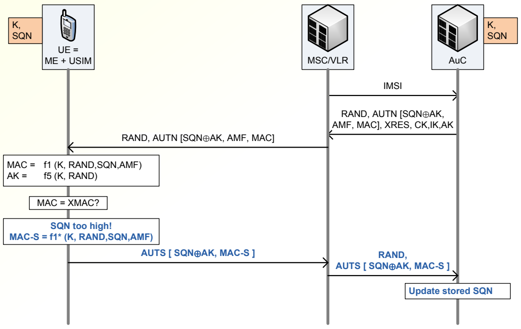
  - SEQ2 — time counter, 2^{24} seconds = 194 days, individual mobile may run ahead of the global time but can never be left behind (Note: the clock is local to AuC; mobile has no secure clock!)
  - SEQ1 — per-mobile epoch counter, incremented when SEQ2 wraps, or appears to wrap
  - IND — partitions the SQN space to independent sequences; highest used SEQ1|SEQ2 stored independently for each IND value 0..31
- IND enables creation of multiple simultaneously valid authentication vectors
  - Enables buffering of unused authentication vectors in VLR
  - Enables parallel authentication in CS, PS, IMS and WLAN domains

Staying in sync

SEQ1 (19 bits)	SEQ2 (24 bits)	IND (5 bits)

- Mobile may run ahead of the global time counter SEQ2 if it needs a burst of values; long-term authentication rate capped at 1/s
- Incrementing SEQ at AuC:
  - if SEQ2 is less than the global time counter, set equal
  - if equal or slightly (at most 2^{16}) higher than global time, increment by 1
  - otherwise, SEQ2 has wrapped → set SEQ2 equal to global time and increment SEQ1
- USIM stores the largest received value of SEQ1|SEQ2 for each IND value 0..31
  - If mobile receives a lower or equal value, authentication fails
  - If mobile receives a slightly higher value (SEQ1|SEQ2 increased by at most 2^{28} = 8.5 years), USIM updates the stored value
  - If the increment is larger than 2^{28}, USIM initiates a resynchronization procedure

RSQ Resynchronization


K, SQN

UE = ME + USIM

MSC/VLR

AuC

K, SQN

IMSI

RAND, AUTN [SQN⊕AK, AMF, MAC], XRES, CK,IK,AK

RAND, AUTN [SQN⊕AK, AMF, MAC]

MAC = f1 (K, RAND,SQN,AMF)
AK = f5 (K, RAND)

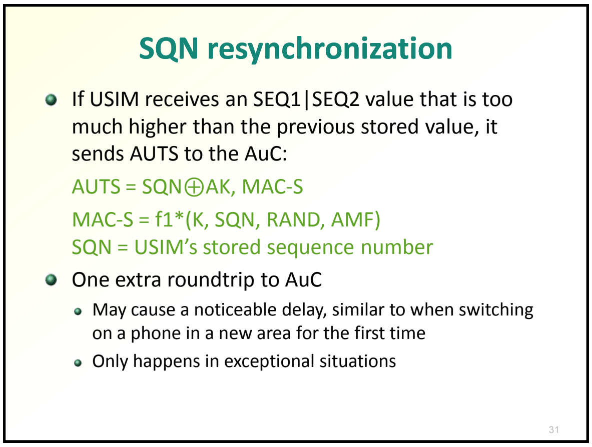
MAC = XMAC?

SQN too high!
MAC-S = f1* (K, RAND,SQN,AMF)

AUTS [SQN⊕AK, MAC-S]

RAND, AUTS [SQN⊕AK, MAC-S]

Update stored SQN



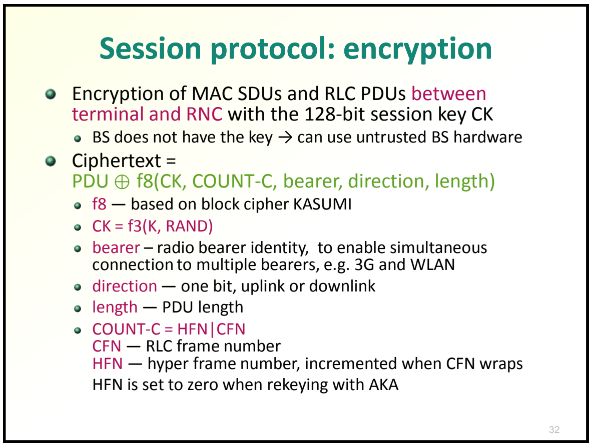
SQN resynchronization

- If USIM receives an SEQ1|SEQ2 value that is too much higher than the previous stored value, it sends AUTS to the AuC:

  AUTS = SQN⊕AK, MAC-S

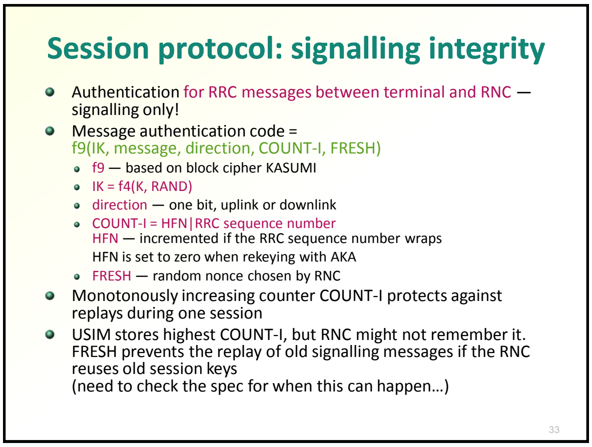
  MAC-S = f1*(K, SQN, RAND, AMF)

  SQN = USIM's stored sequence number
- One extra roundtrip to AuC
  - May cause a noticeable delay, similar to when switching on a phone in a new area for the first time
  - Only happens in exceptional situations



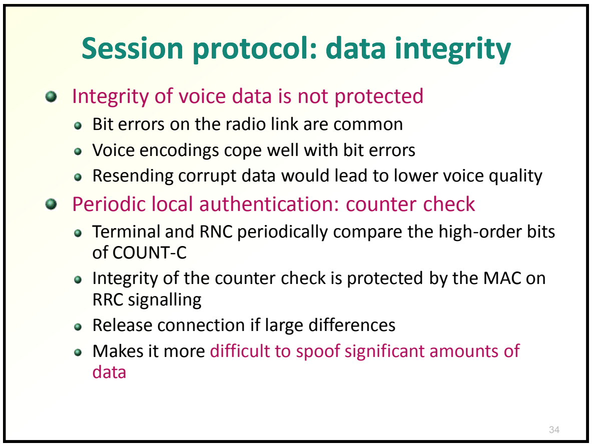
Session protocol: encryption

- Encryption of MAC SDUs and RLC PDUs between terminal and RNC with the 128-bit session key CK
  - BS does not have the key → can use untrusted BS hardware
- Ciphertext =
  PDU ⊕ f8(CK, COUNT-C, bearer, direction, length)
  - f8 — based on block cipher KASUMI
  - CK = f3(K, RAND)
  - bearer – radio bearer identity, to enable simultaneous connection to multiple bearers, e.g. 3G and WLAN
  - direction — one bit, uplink or downlink
  - length — PDU length
  - COUNT-C = HFN|CFN
    CFN — RLC frame number
    HFN — hyper frame number, incremented when CFN wraps
    HFN is set to zero when rekeying with AKA



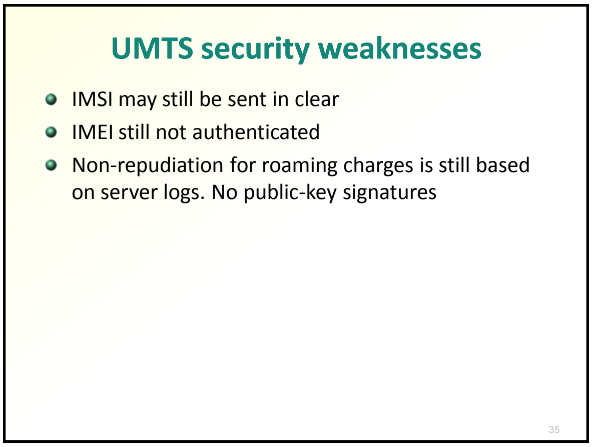
Session protocol: signalling integrity

- Authentication for RRC messages between terminal and RNC — signalling only!
- Message authentication code =
  f9(IK, message, direction, COUNT-I, FRESH)
  - f9 — based on block cipher KASUMI
  - IK = f4(K, RAND)
  - direction — one bit, uplink or downlink
  - COUNT-I = HFN|RRC sequence number
    HFN — incremented if the RRC sequence number wraps
    HFN is set to zero when rekeying with AKA
  - FRESH — random nonce chosen by RNC
- Monotonously increasing counter COUNT-I protects against replays during one session
- USIM stores highest COUNT-I, but RNC might not remember it. FRESH prevents the replay of old signalling messages if the RNC reuses old session keys
  (need to check the spec for when this can happen…)



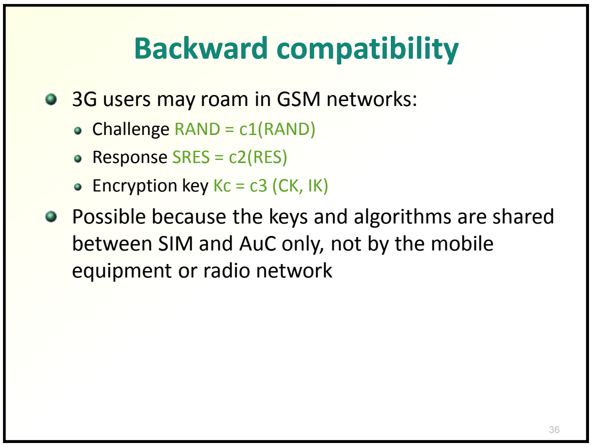
Session protocol: data integrity

- Integrity of voice data is not protected
  - Bit errors on the radio link are common
  - Voice encodings cope well with bit errors
  - Resending corrupt data would lead to lower voice quality
- Periodic local authentication: counter check
  - Terminal and RNC periodically compare the high-order bits of COUNT-C
  - Integrity of the counter check is protected by the MAC on RRC signalling
  - Release connection if large differences
  - Makes it more difficult to spoof significant amounts of data



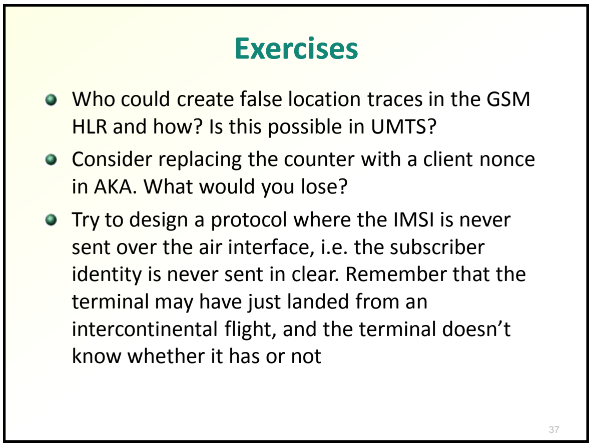
UMTS security weaknesses

- IMSI may still be sent in clear
- IMEI still not authenticated
- Non-repudiation for roaming charges is still based on server logs. No public-key signatures



Backward compatibility

- 3G users may roam in GSM networks:
  - Challenge RAND = c1(RAND)
  - Response SRES = c2(RES)
  - Encryption key Kc = c3 (CK, IK)
- Possible because the keys and algorithms are shared between SIM and AuC only, not by the mobile equipment or radio network



Exercises

- Who could create false location traces in the GSM HLR and how? Is this possible in UMTS?
- Consider replacing the counter with a client nonce in AKA. What would you lose?
- Try to design a protocol where the IMSI is never sent over the air interface, i.e. the subscriber identity is never sent in clear. Remember that the terminal may have just landed from an intercontinental flight, and the terminal doesn’t know whether it has or not