GSM and UMTS security

Why is security more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
- broadcast communications
  - wireless usually means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

- ➢ eavesdropping is easy
- ➢ injecting bogus messages into the network is easy
- ➢ replaying previously recorded messages is easy
- ➢ illegitimate access to the network and its services is easy
- ➢ denial of service is easily achieved by jamming

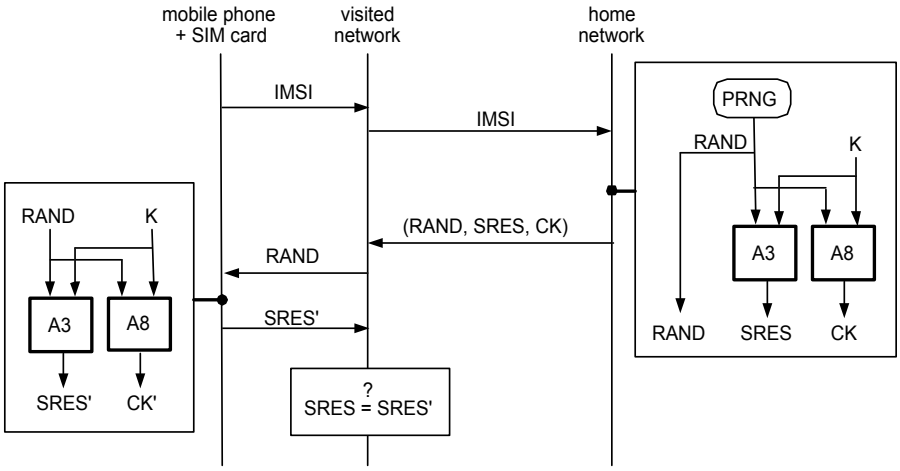
GSM Security

- main security requirement
  - subscriber authentication (for the sake of billing)
    - challenge-response protocol
    - long-term secret key shared between the subscriber and the home network operator
    - supports roaming without revealing long-term key to the visited networks
- other security services provided by GSM
  - confidentiality of communications and signaling over the wireless interface
    - encryption key shared between the subscriber and the visited network is established with the help of the home network as part of the subscriber authentication protocol
  - protection of the subscriber's identity from eavesdroppers on the wireless interface
    - usage of short-term temporary identifiers

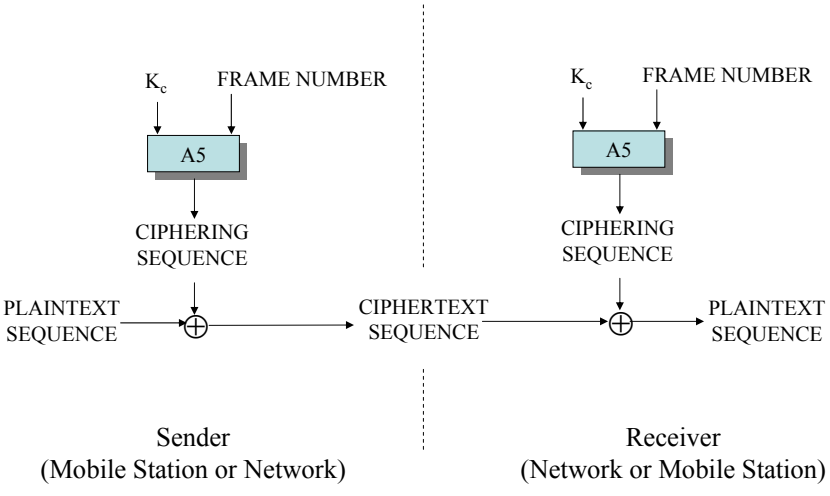
The SIM card (Subscriber Identity Module)

- tamper-resistant
- protected by a PIN code (checked locally by the SIM)
- removable from the terminal
- contains all data specific to the end user which have to reside in the Mobile Station:
  - IMSI: International Mobile Subscriber Identity (permanent user's identity)
  - PIN
  - TMSI (Temporary Mobile Subscriber Identity)
  - K_i : User's secret key
  - CK : Ciphering key
  - List of the last call attempts
  - List of preferred operators
  - Supplementary service data (abbreviated dialing, last short messages received,...)

GSM authentication and cipher key setup



Ciphering in GSM



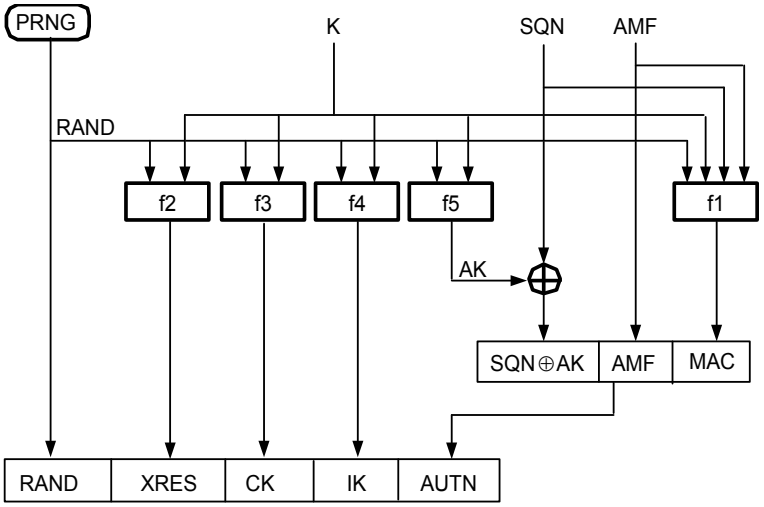
Conclusion on GSM security

- focused on the protection of the air interface
- no protection on the wired part of the network (neither for privacy nor for confidentiality)
- the visited network has access to all data (except the secret key of the end user)
- generally robust, but a few successful attacks have been reported:
  - faked base stations
  - cloning of the SIM card

3GPP security design principles

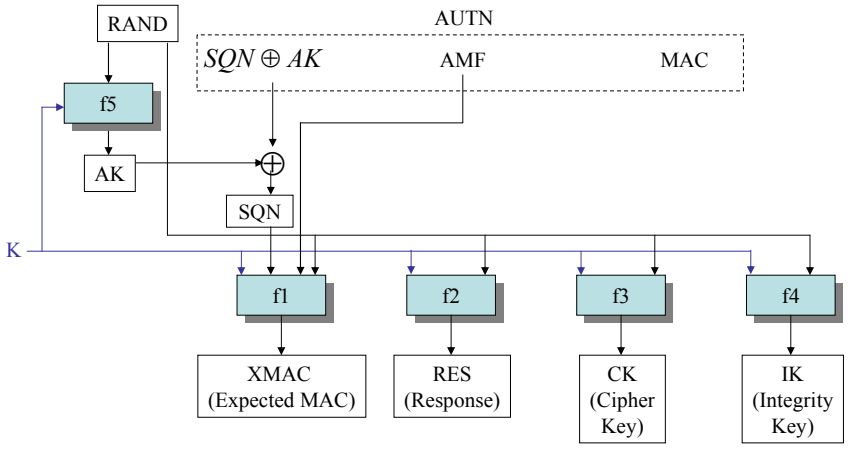
- Reuse of 2nd generation security principles (GSM):
  - Removable hardware security module
    - In GSM: SIM card
    - In 3GPP: USIM (User Services Identity Module)
  - Radio interface encryption
  - Limited trust in the Visited Network
  - Protection of the identity of the end user (especially on the radio interface)
- Correction of the following weaknesses of the previous generation:
  - Possible attacks from a faked base station
  - Cipher keys and authentication data transmitted in clear between and within networks
  - Encryption not used in some networks ➔ open to fraud
  - Data integrity not provided
  - …

3GPP authentication vectors



AMF: Authentication and Key Management Field

Processing in the USIM



- Verify that SQN is in the correct range
- Verify MAC = XMAC

USIM: User Services Identity Module

Conclusion on 3GPP security

- Some improvement with respect to 2nd generation
  - Cryptographic algorithms are published
  - Integrity of the signalling messages is protected
- Quite conservative solution
- Privacy/anonymity of the user not completely protected
- 2nd/3rd generation interoperation will be complicated and might open security breaches