GSM Network and Services

Authentication and encryption

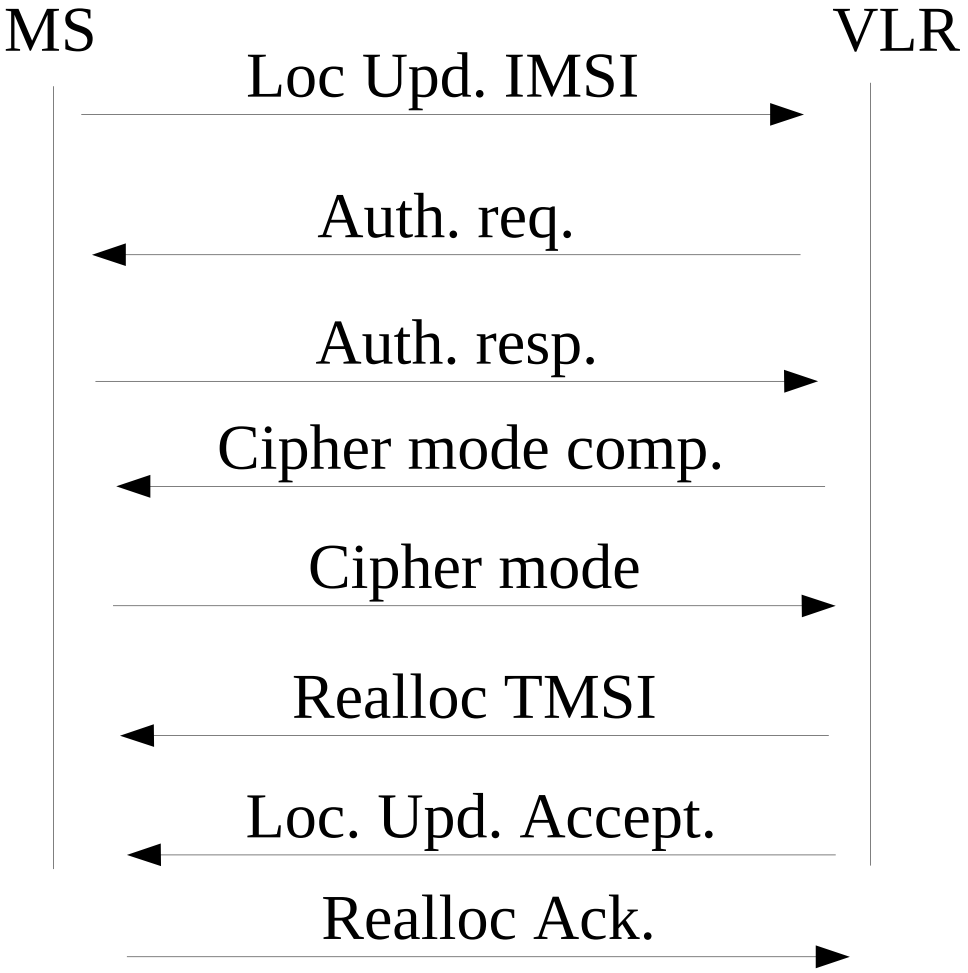
Encryption

- How do we authenticate the user?
  - part of the signaling layer
- How do we ensure privacy?
  - Should people be able to listen in on my conversation.
  - Should people be able to know that I'm calling and to whom I'm calling?

TMSI

- We do not want to use our IMSI number every time we signal to the network. Trudy would be able to know that we are calling, some one is calling us and also that we have entered a location area.
- Solution: allocate a *temporary mobile subscriber Identifier* (TMSI) the first time we do an attach, then only use the TMSI.
- TMSI is local to a VLR!

Location registration



MS

VLR

Loc Upd. IMSI

Auth. req.

Auth. resp.

Cipher mode comp.

Cipher mode

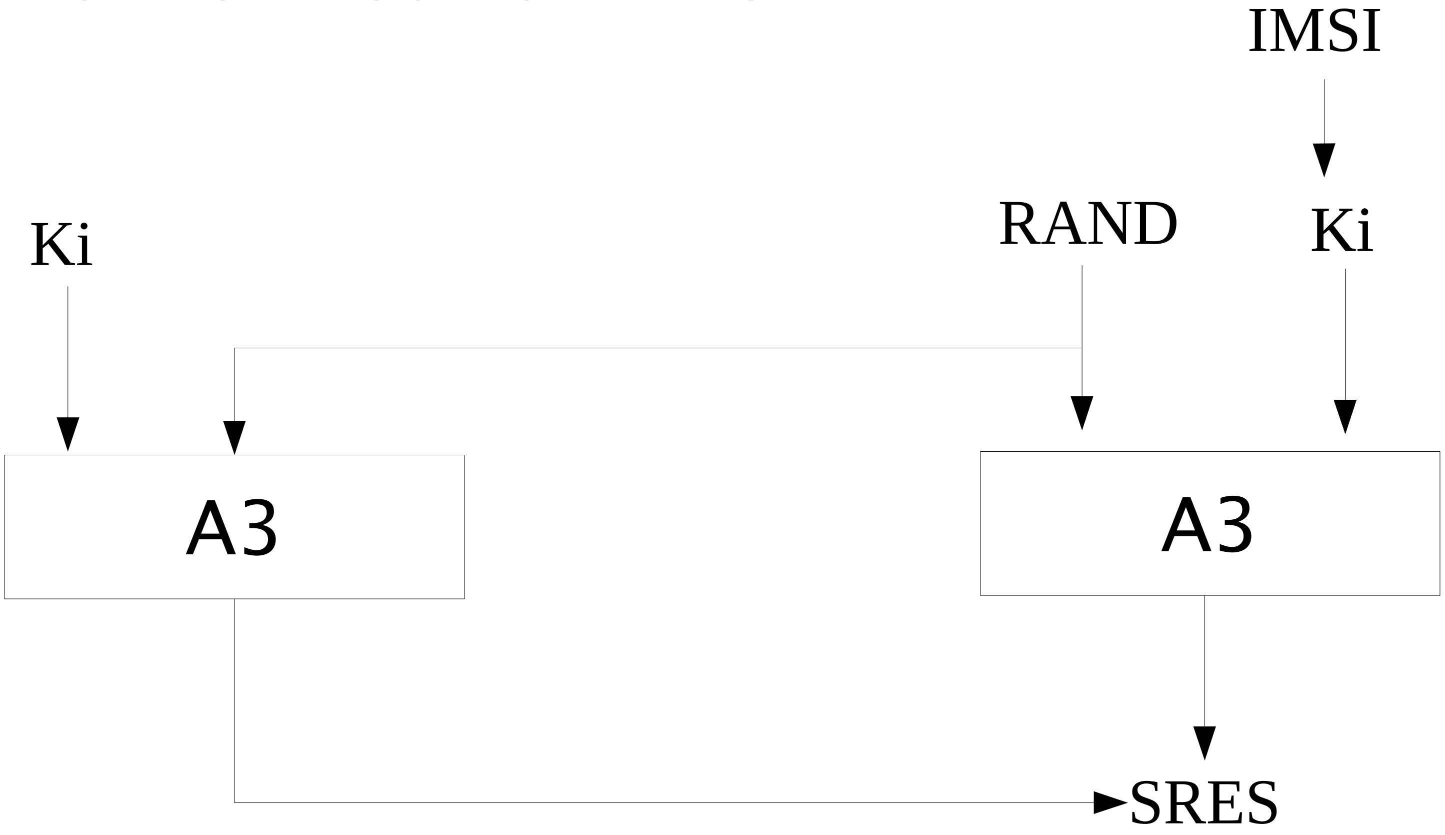
Realloc TMSI

Loc. Upd. Accept.

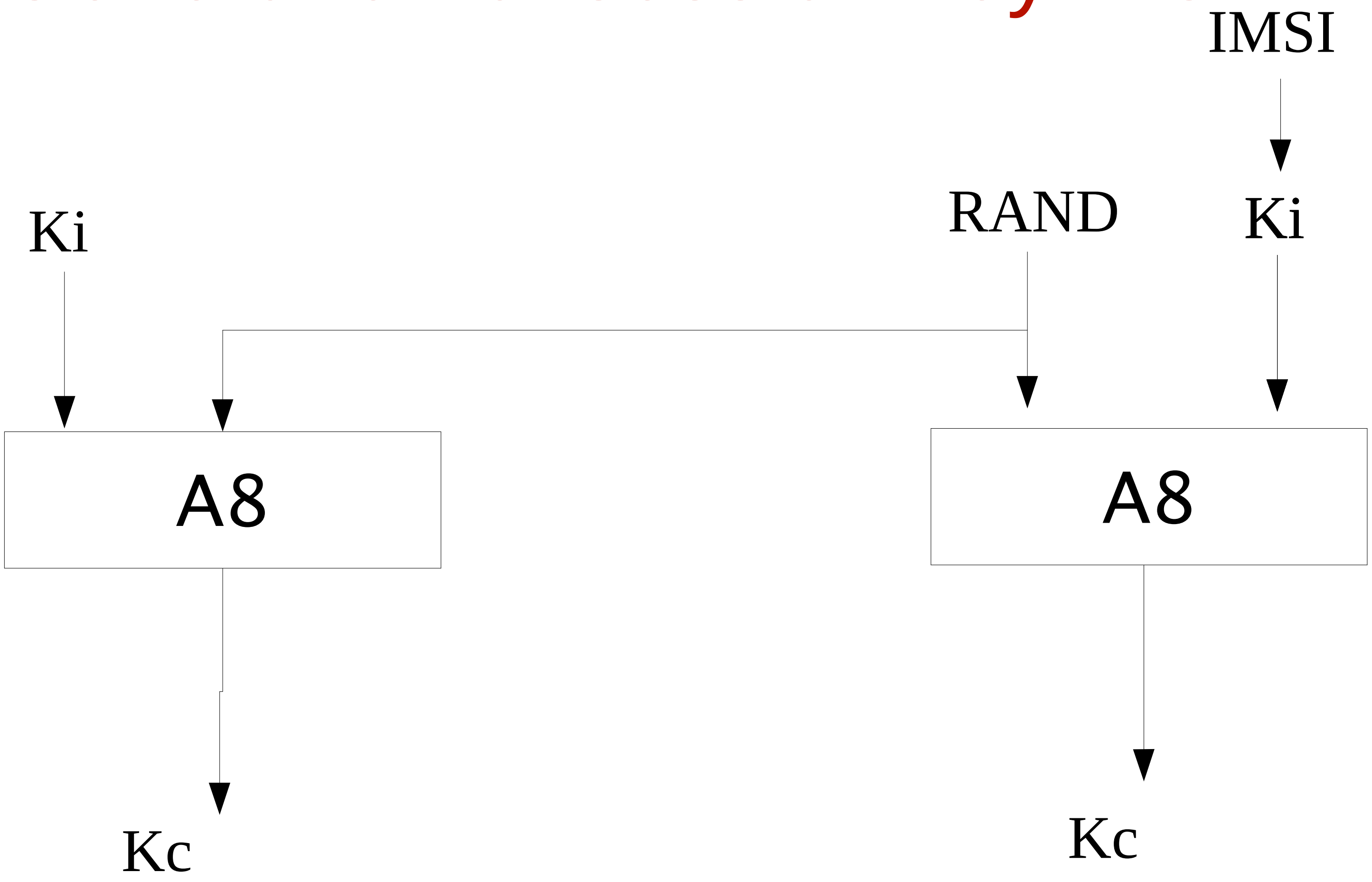
Realloc Ack.

Stores IMSI/TMSI

Authentication A3

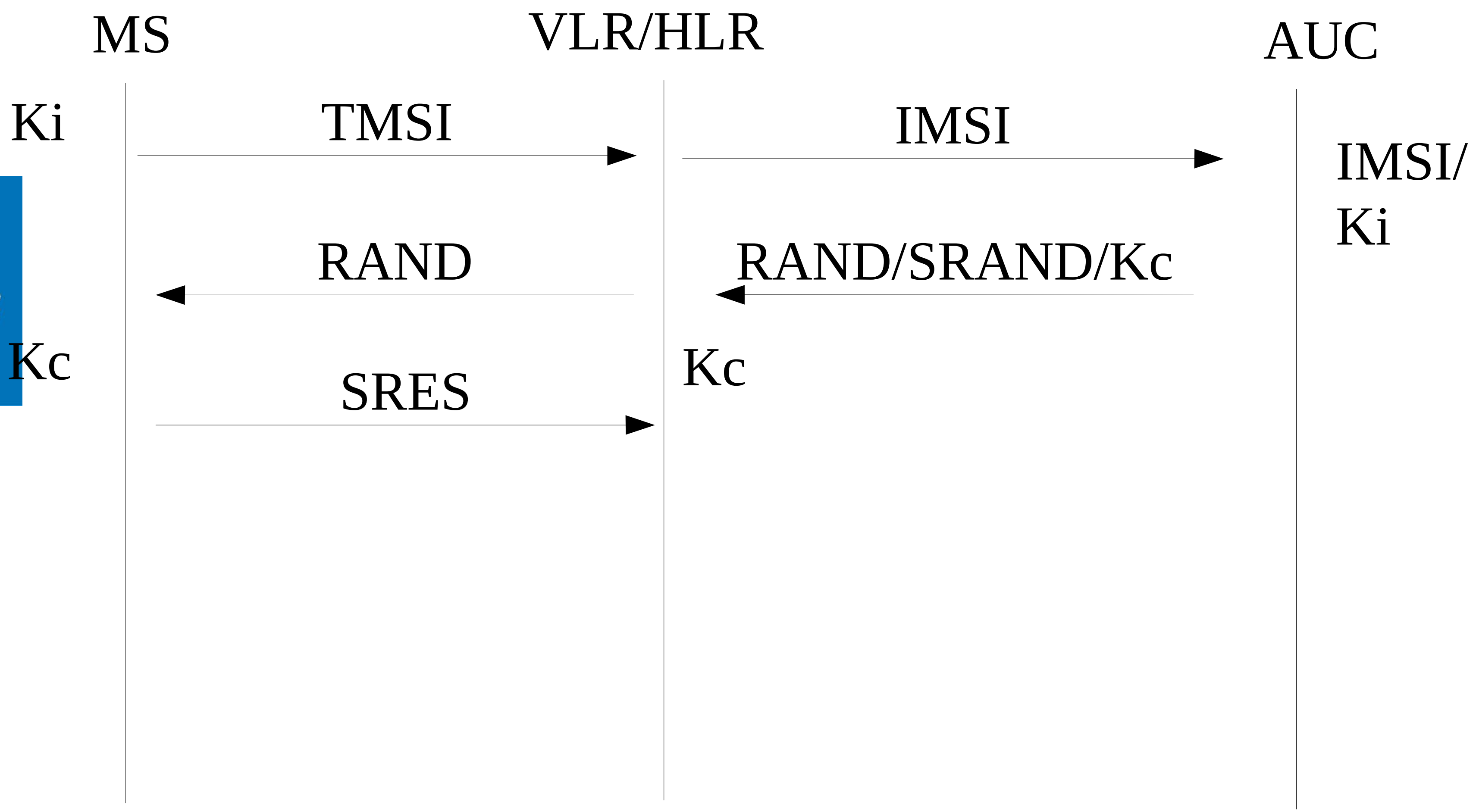


Generation of session key A8

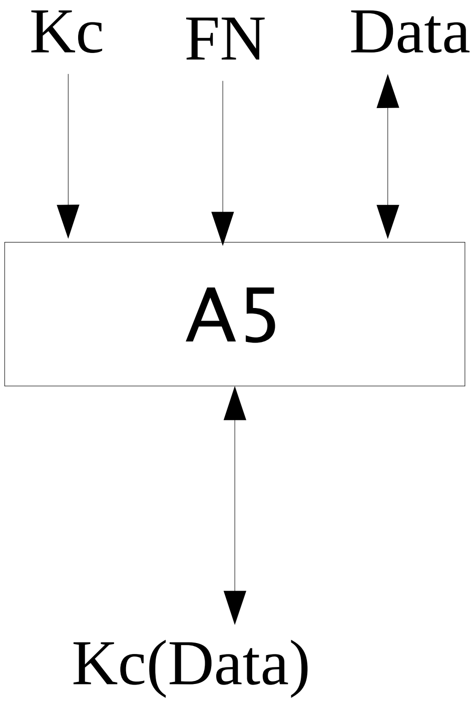


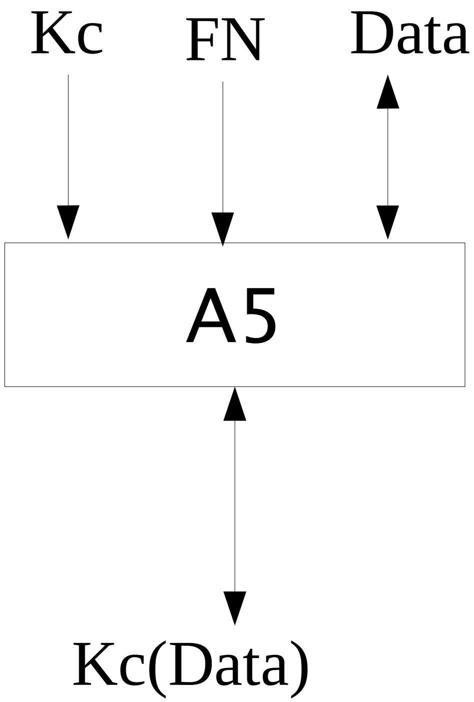
Done at the same time as
authentication.

Keeping Ki a secret



Encryption A5





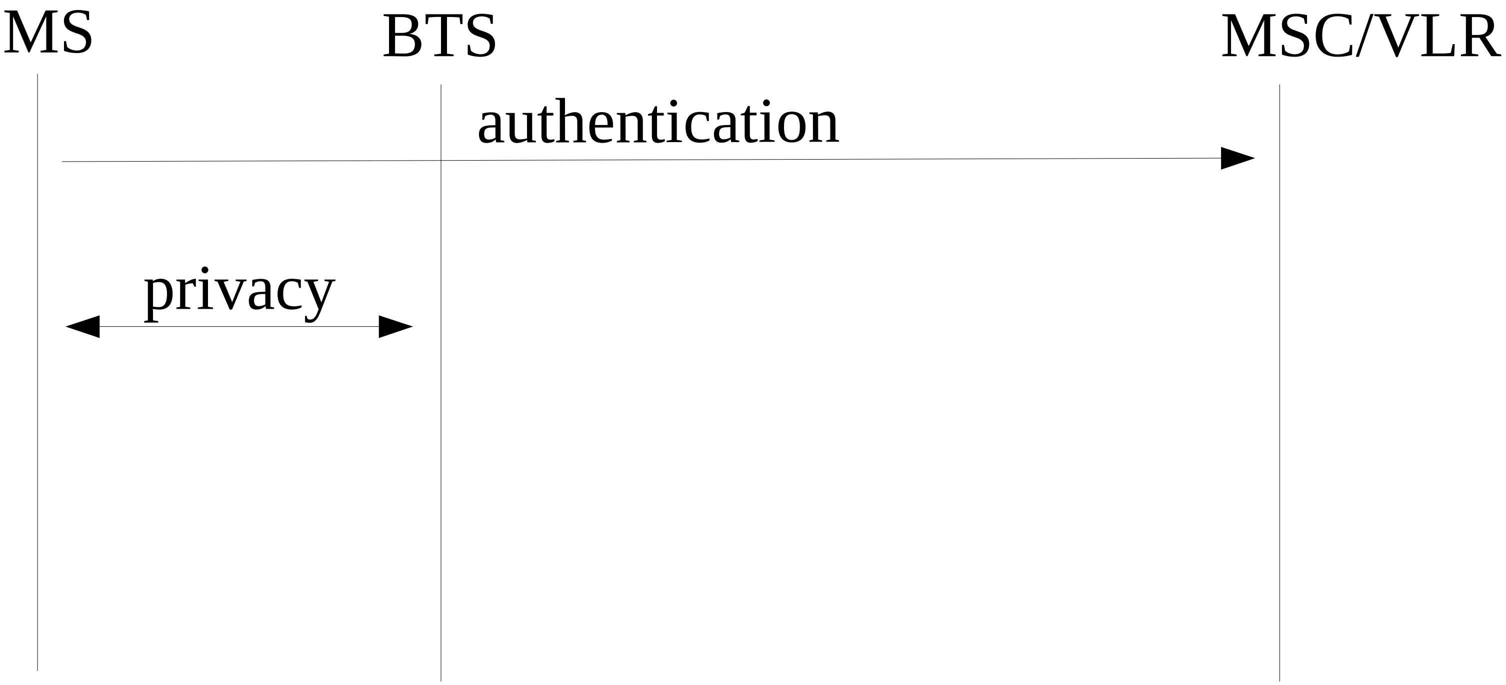
A5

- A5/0 : no encryption.
- A5/1 : original A5 algorithm
- A5/2 : weaker algorithm created for export
- A5/3 : strong encryption created by 3GPP

A5

- A5 is a stream cipher.
- Uses three linear feed-back shift registers (LFSR) of different length (19/21/22) and variable clock. The xor of the three registers is the bit stream that is then xored with the plain text.
- The key is the initial content of the registers, in total 64 bits derived from Kc and the frame number.

Authentication and privacy



The network is not authenticated!

From www.gsm-security.net

- Alex Biryukov, Adi Shamir and David Wagner showed that they can find the A5/1 key in less than a second on a single PC with 128 MB RAM and two 73 GB hard disks, by analyzing the output of the A5/1 algorithm in the first two minutes of the conversation.
- Ian Goldberg and David Wagner of the University of California at Berkeley published an analysis of the weaker A5/2 algorithm showing a work factor of 2^16, or approximately 10 milliseconds.
- Elad Barkhan, Eli Biham and Nathan Keller of Technion, the Israel Institute of Technology, have shown a ciphertext-only attack against A5/2 that requires only a few dozen milliseconds of encrypted off-the-air traffic. They also described new attacks against A5/1 and A5/3.

From www.gsm-security.net

- Ian Goldberg and David Wagner of the University of California at Berkeley demonstrated that all A8 implementations they looked at, including the few that did not use COMP128, were deliberately weakened. The A8 algorithm takes a 64-bit key, but ten key bits were set to zero. The attack on the A8 algorithm demonstrated by Goldberg and Wagner takes just 2^19 queries to the GSM SIM *Subscriber Identity Module), which takes roughly 8 hours.
- Josyula R. Rao, Pankaj Rohatgi and Helmut Scherzer of IBM and Stephane Tinguely of the Swiss Federal Institute of Technology have published Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards which shows a method by which COMP128 can be broken in less than a minute.