Security in Digital Networks

network access security
user domain security
application domain security
network domain security

Security in digital networks

Authentication:

- authorization to use terminal or service (PIN code)
- user authentication (GSM, DECT, UMTS)
- network authentication (UMTS)

Integrity:

- signaling data integrity (UMTS)

Confidentiality (»privacy):

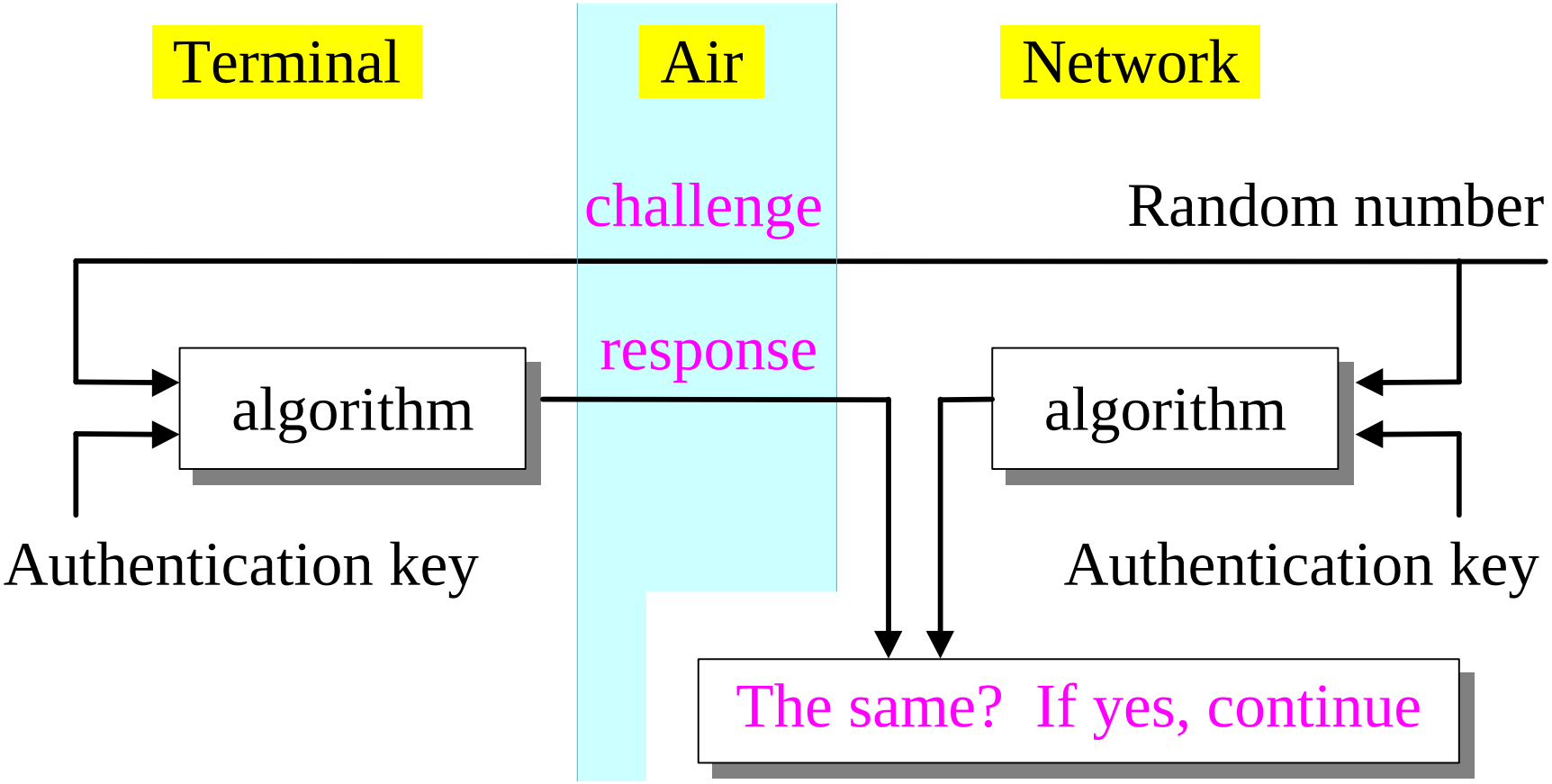
- encryption of signal over radio interface (GSM, UMTS)
- no user identifiers over radio interface (GSM, UMTS)
- end-to-end encryption (offered by service provider)

Authentication

Authentication: The procedure of verifying the authenticity of an entity (user, terminal, network, network element). In other words, is the entity the one it claims to be?

- PIN code authentication is local (network not involved)
- in GSM, only user (SIM) is authenticated
- in UMTS, both user (SIM) and network are authenticated
- user (SIM) authentication is done before each user-network transaction (e.g. before connection set-up)

Basic principle of user authentication



Algorithm considerations

- Using output and one or more inputs, it is in practice not possible to calculate “backwards” other input(s)
  “brute force approach”, “extensive search”

- Strength of algorithm is that it is secret => bad idea!
  “security through obscurity”

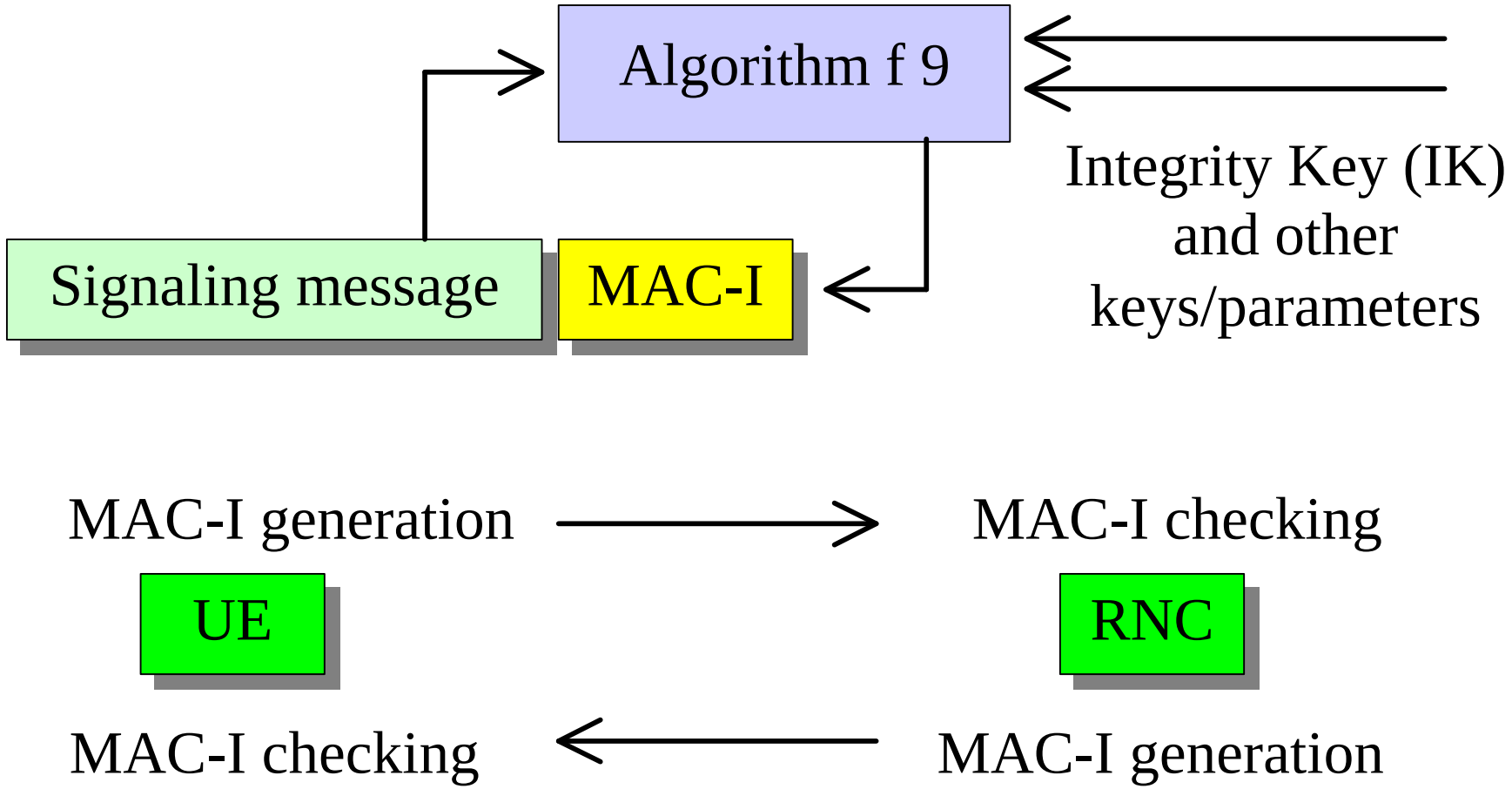
- Open algorithm can be tested by engineering community

Integrity

Data integrity: The property that data has not been altered in an unauthorised manner.

- "Man-in-the-middle" security attack, e.g. false BS
- Data integrity checking is not done in GSM
- In UMTS, signaling messages are appended with a 32 bit security field (MAC-I) at the terminal or RNC before transmission and checked at the receiving end
- In UMTS, also volume of user data is integrity protected

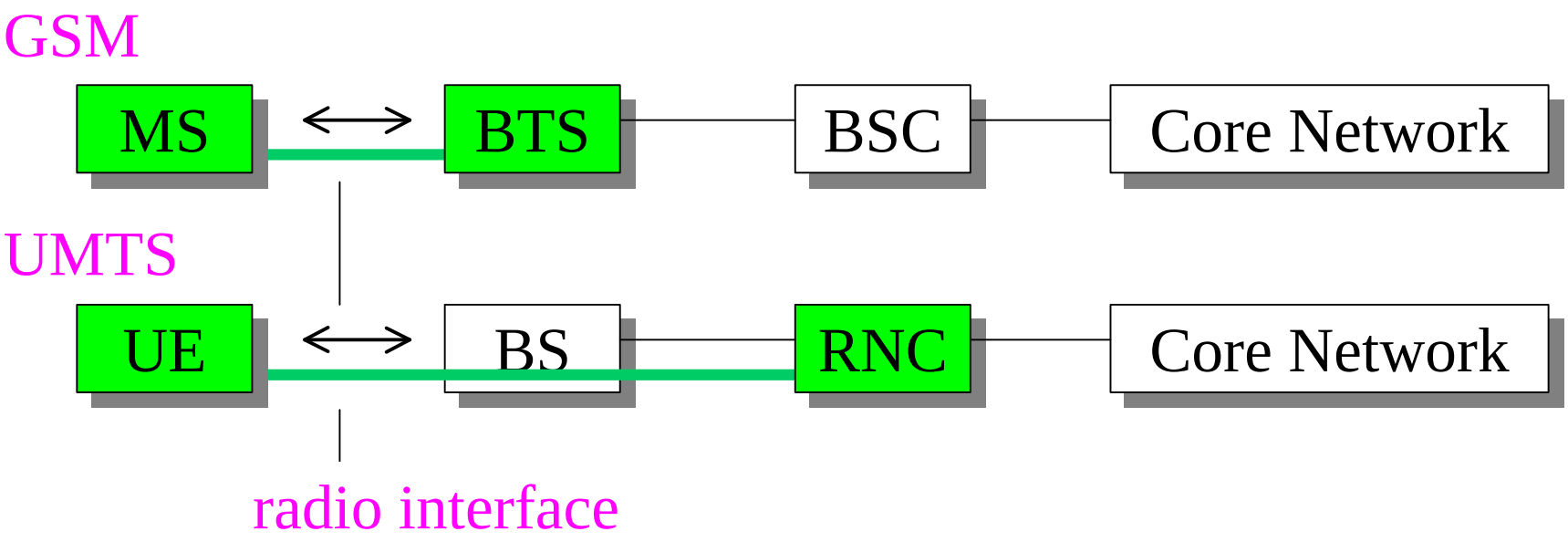
Signaling message integrity check in UMTS



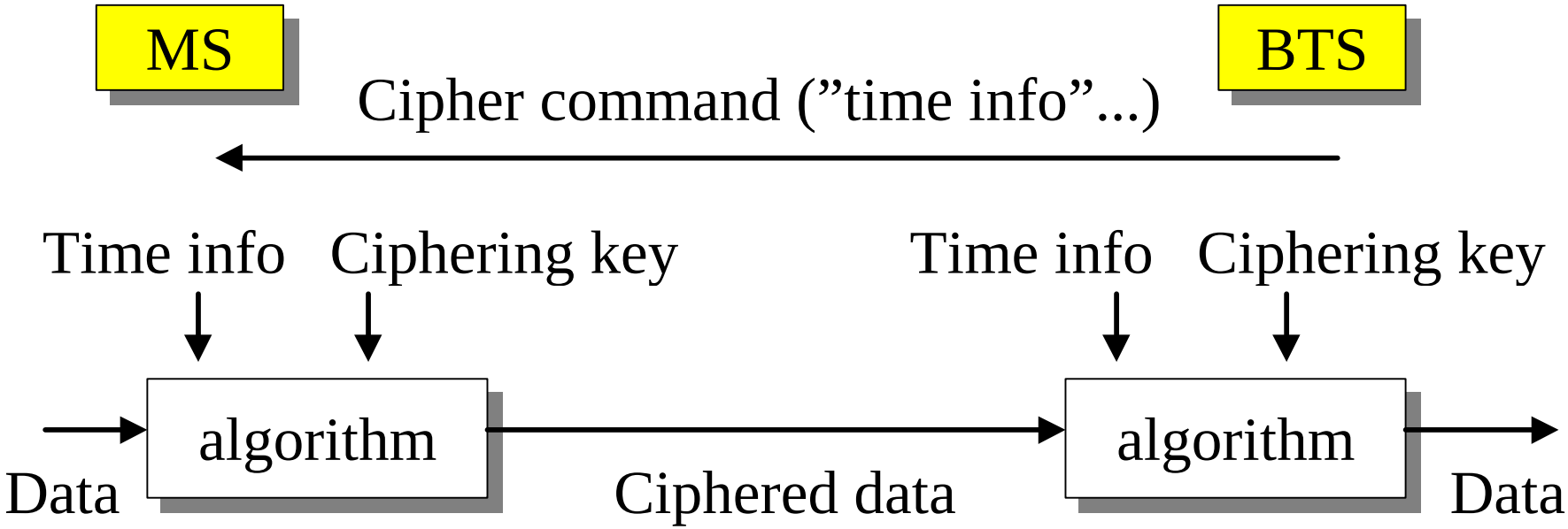
Confidentiality

Confidentiality: The property that information is not made available to unauthorised individuals, entities or processes.

Example 1: Ciphering (encryption) in radio access networks

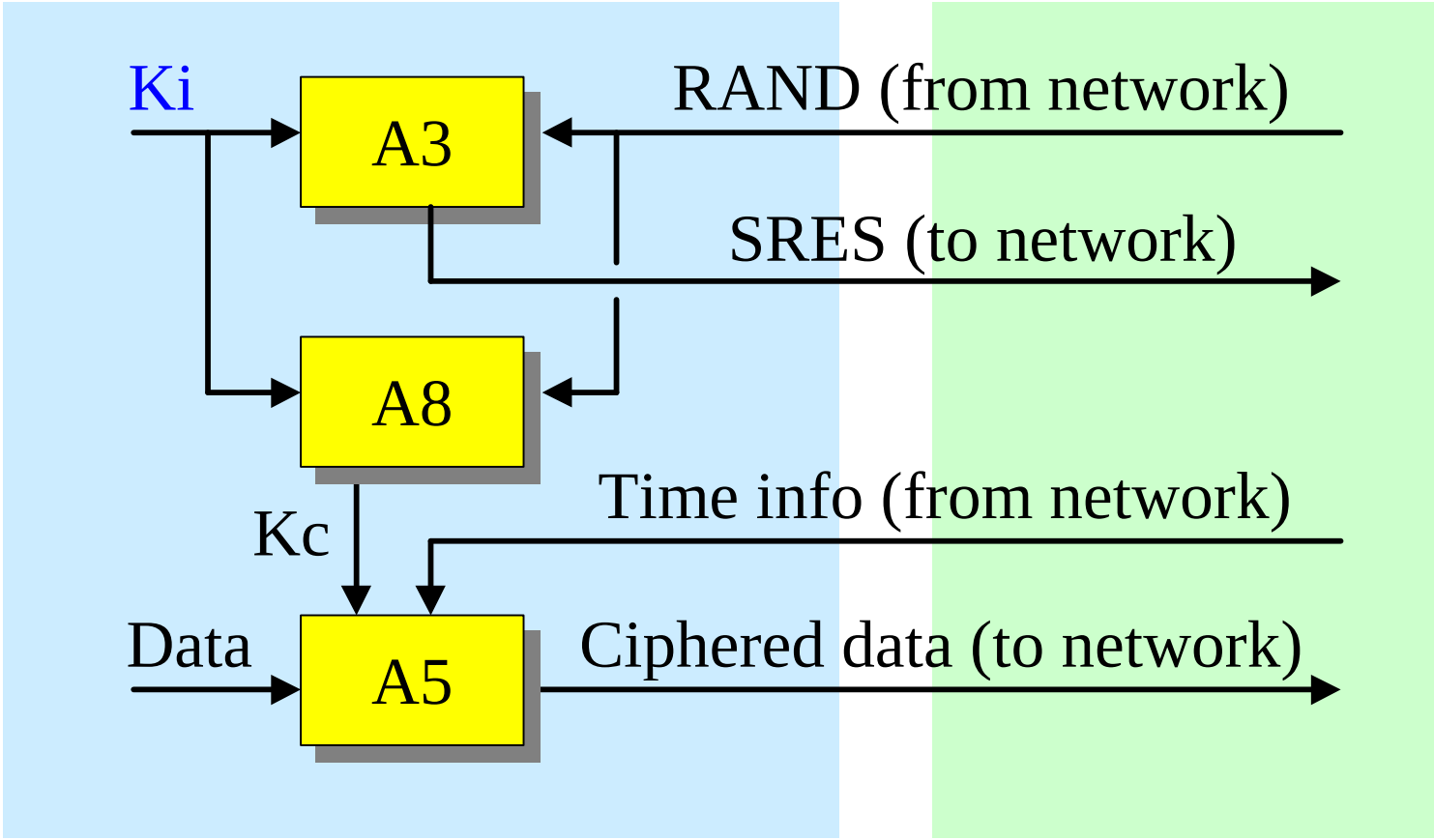


Ciphering in GSM (only uplink shown)

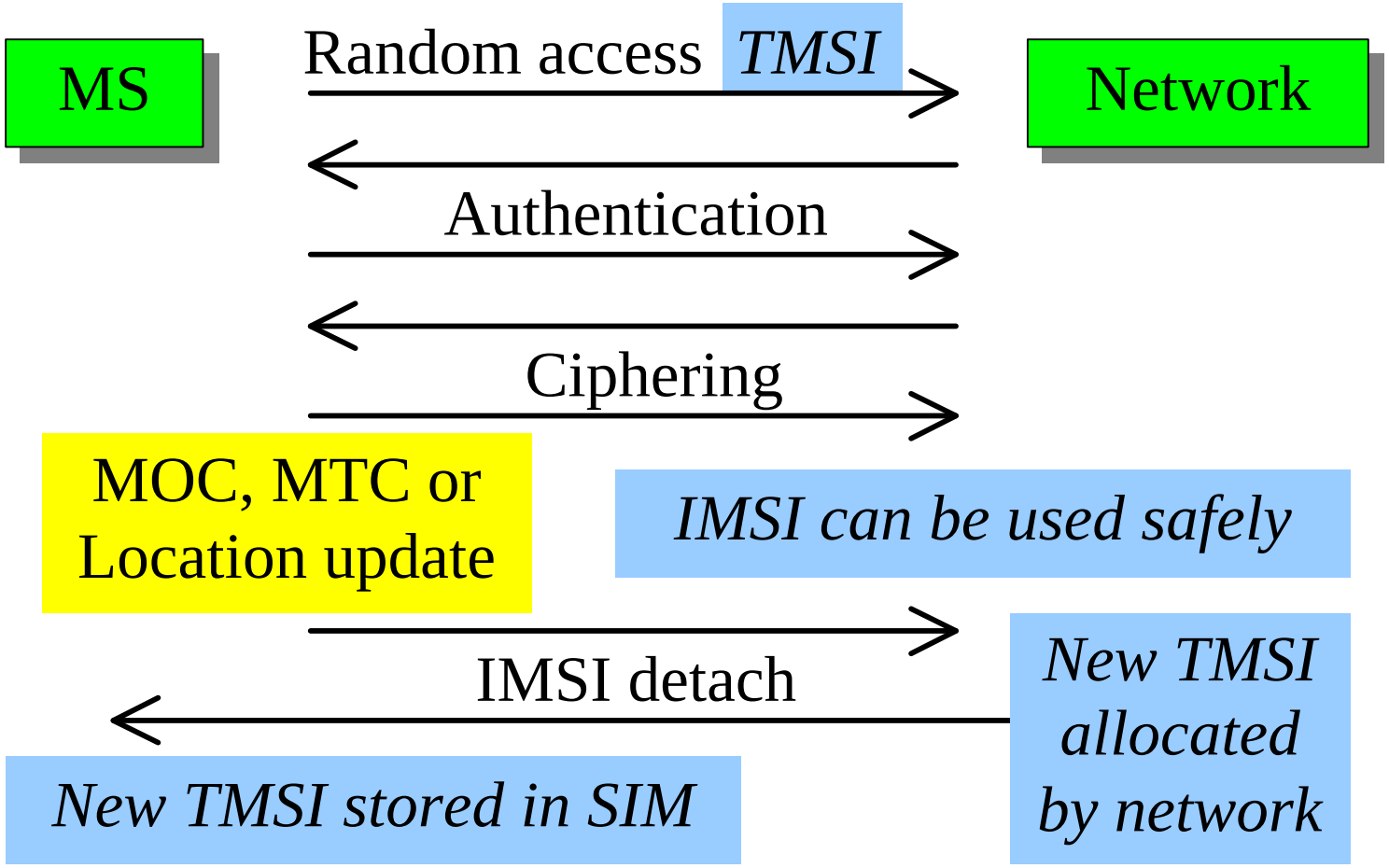


Ciphering key (Kc) is generated during authentication both in MS and MSC (in same way as “response”) for each call.

Three security algorithms in GSM MS



TMSI / IMSI usage in GSM



Network domain security

- Circuit switched network => quite good
- IP-based network (Internet) => rather poor at present (security mechanisms are being developed by IETF...)

Some security threats in IP-based network:

(confidentiality) Sniffing (electronic eavesdropping)

(integrity) Spoofing, session hijacking

Denial of service (DoS), spamming