GSM SECURITY

Dr. A. Beulah

AP/CSE

Security

- GSM offers security services with the help of Confidential information stored in
  - The AuC
  - The individual SIM
- AuC contains
  - The algorithms for authentication and generates the values needed for user authentication
  - The keys for encryption
- SIM stores
  - Personal data
  - Secret data.
  - These are protected with the help of PIN

Security Services

- Access control and Authentication
  - Authentication of a valid user for the SIM.
  - The user needs a secret PIN to access the SIM
  - Subscriber Authentication has to be done.
- Confidentiality
  - User data is encrypted
  - After authentication, BTS and MS apply encryption to voice, data, and Signal.
  - Confidentiality exists only between MS and BTS.
- Anonymity
  - User identifiers are not used over the air.
  - TMSI (newly assigned by the VLR) is transmitted after each location update
  - VLR can change the TMSI at any time.

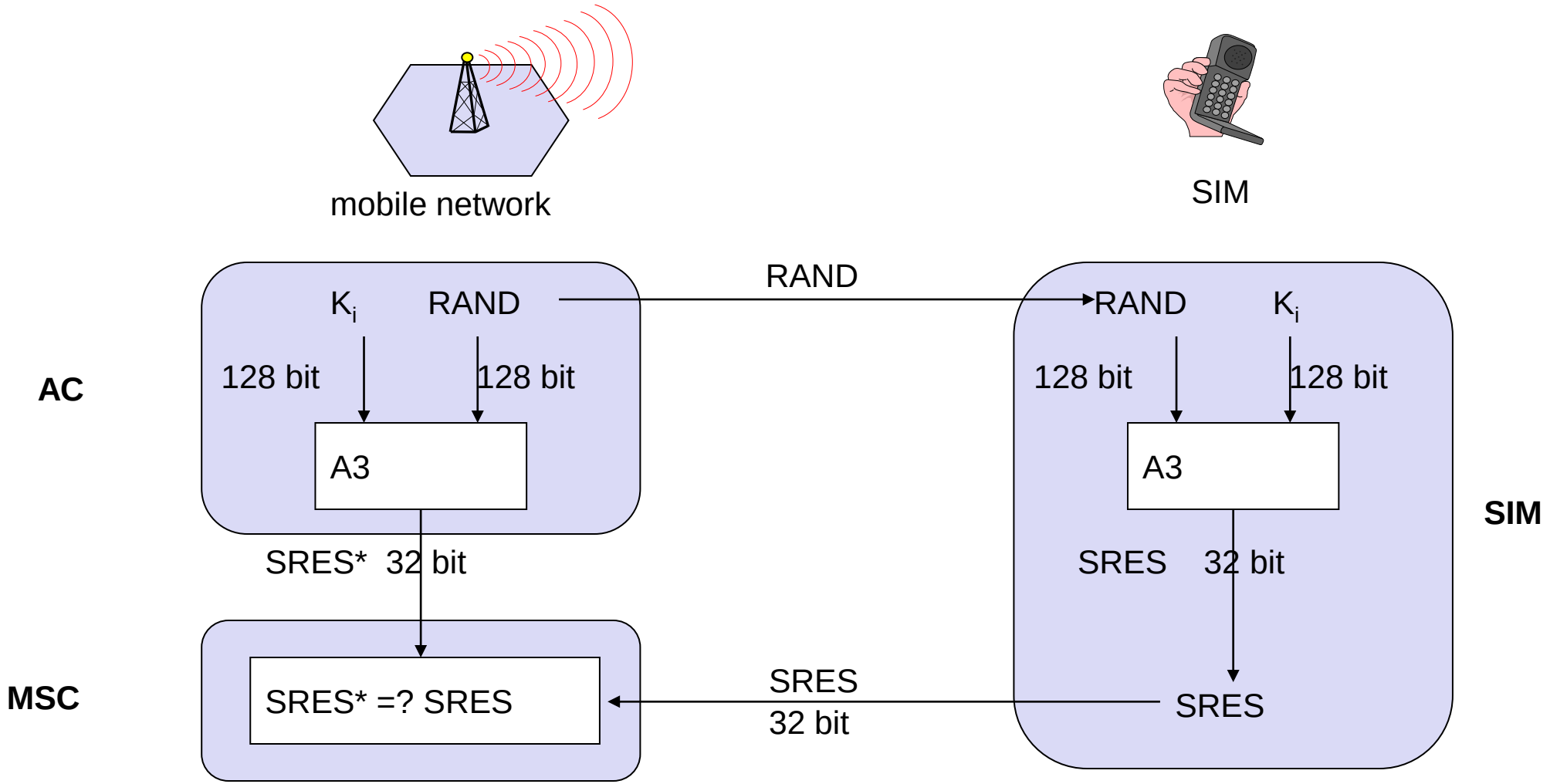
Security Services

- 3 Algorithms
- Algorithm A3 is used for authentication
- Algorithm A5 for Encryption
- Algorithm A8 for the generation of a Cipher Key.

Authentication

- The user should be authenticated, before using any service from the network.
- Authentication is based on SIM
- SIM contains
  - Authentication key K_i
  - User Identification IMSI
  - Algorithm A3 → algorithm used for authentication.
- Authentication uses a challenge-response method.

Authentication

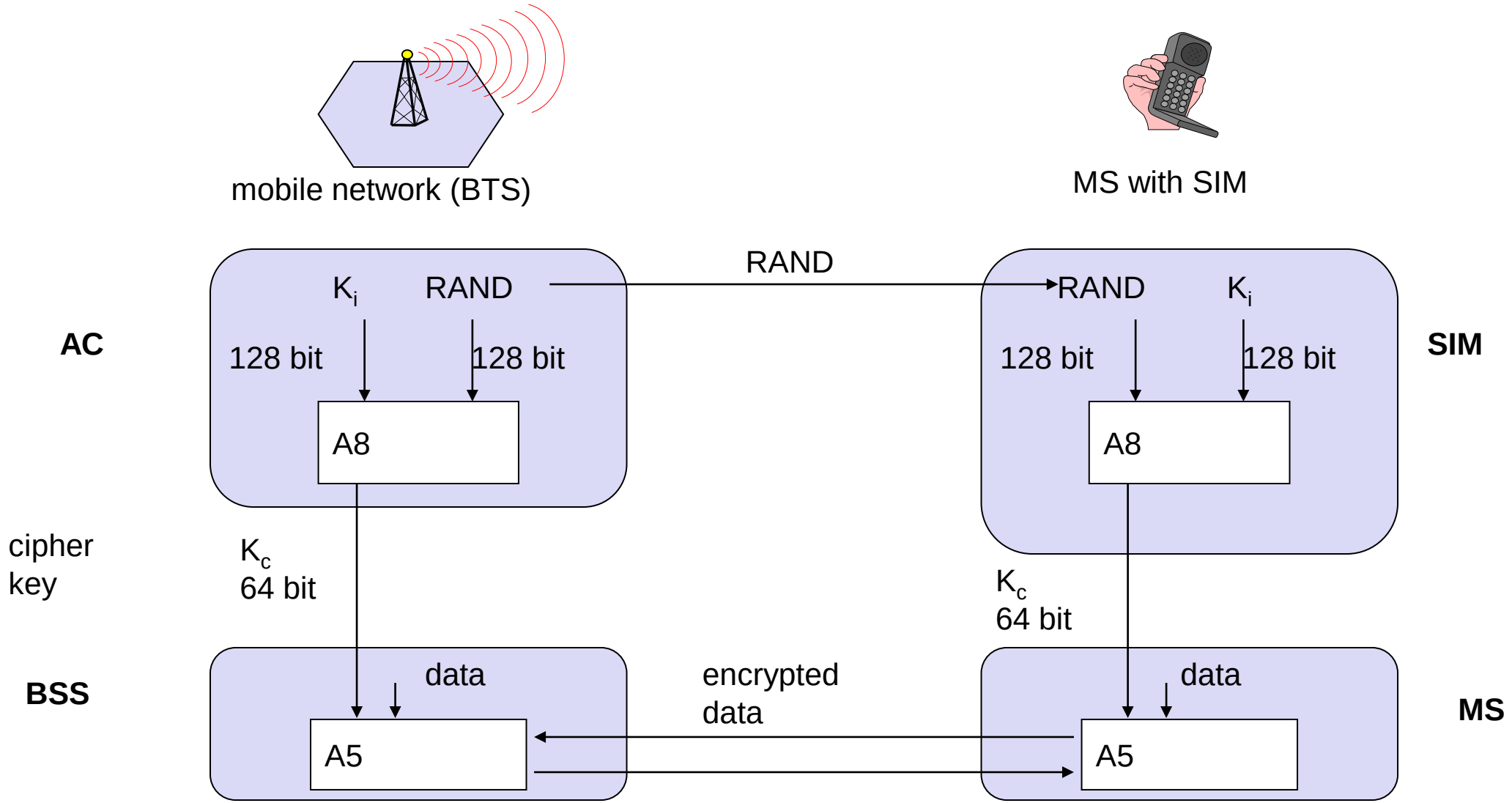


K_i: individual subscriber authentication key SRES: signed response

Encryption

- User data are encrypted
- MS and BTS uses k_c (cipher key) for encryption
- K_c is generated using the authentication key k_i and a random value by applying the algorithm A8

Encryption


mobile network (BTS)
MS with SIM
AC
SIM
RAND
K_i
RAND
RAND
K_i
128 bit
128 bit
128 bit
128 bit
A8
A8
cipher key
K_c
64 bit
K_c
64 bit
BSS
MS
data
encrypted data
data
A5
A5

Summary

- GSM Services
  - Bearer service
  - Teleservice
  - Supplementary service
- GSM Architecture
  - RSS
  - NSS
  - OSS
- GSM Security

Test your understanding

- Identify the main reason as to why a mobile handset is compact and lightweight and yet provides a large number of features such as roaming, camera, audio and video play, record internet etc., while traditional landline phone handsets are bulky and provide only limited features.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.