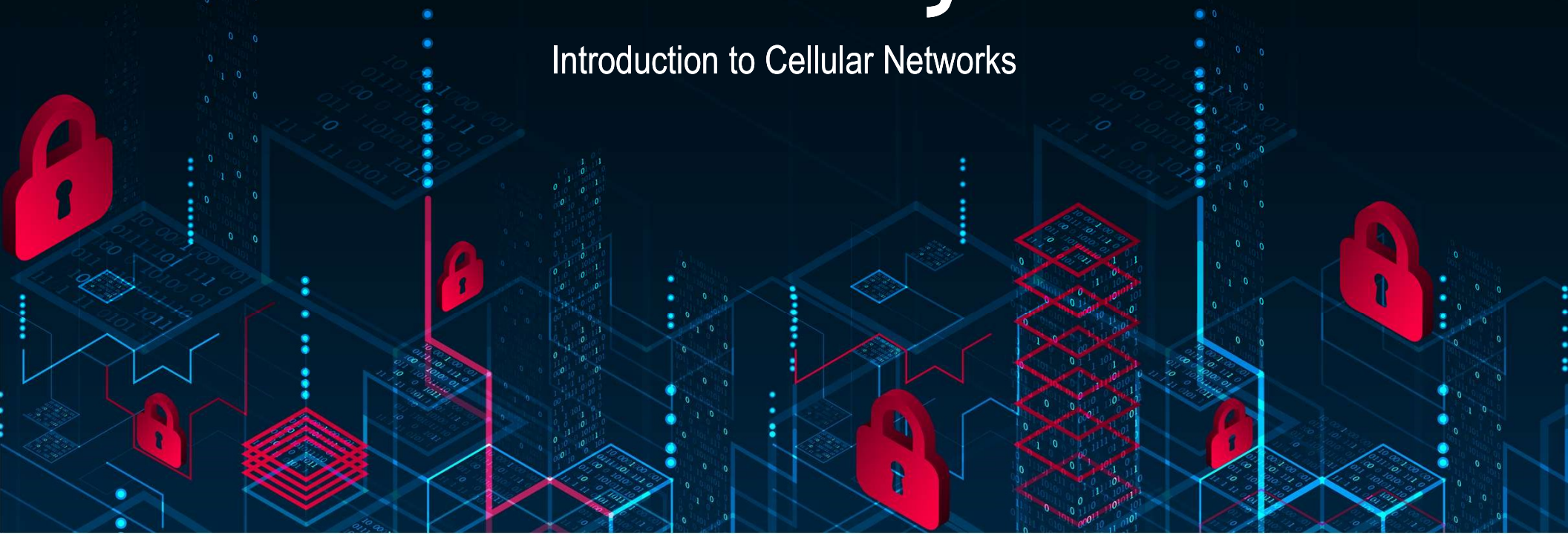
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

Introduction to Cellular Networks



Video summary

- GSM Authentication Algorithms
- Encryption Algorithm (A5)
- Subscriber Identity Protection
- Attacks Against GSM

Authentication

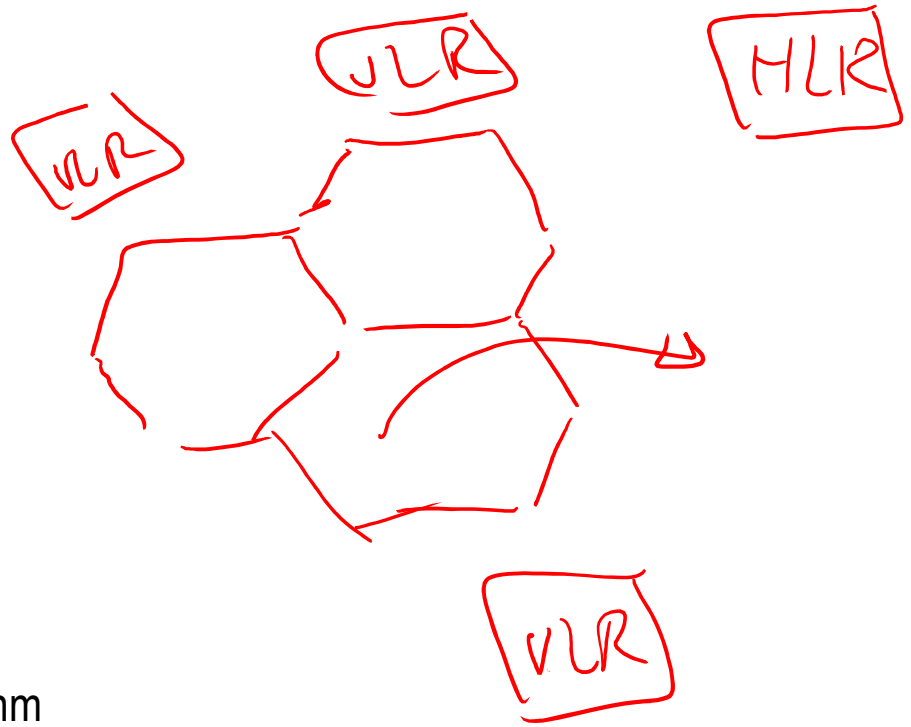
➢Authentication Goals

- Subscriber (SIM holder) authentication, protection of the network against unauthorized use
- Create a session key for the next communication

➢Authentication Scheme

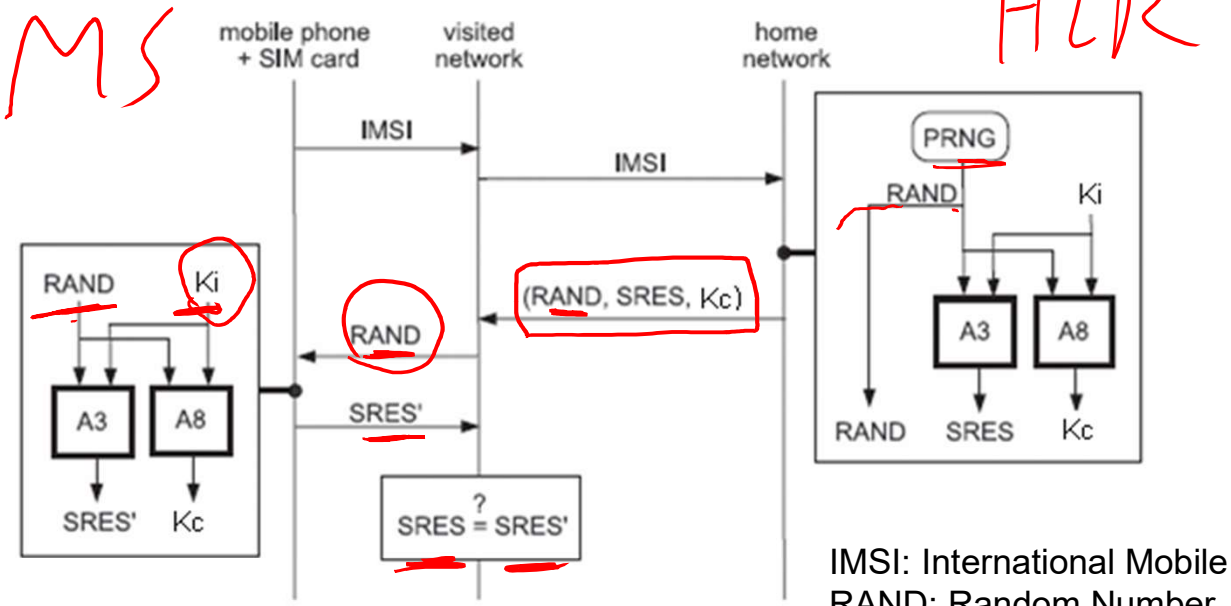
- Subscriber identification: IMSI/TMSI
- Challenge-Response authentication of the subscriber
- Long-term secret key shared between the subscriber and the home network
- Supports roaming without revealing long-term key to the visited networks

Authentication Parameters



- Network Contains
  - AuC : Authentication Center
  - HLR : Home Location Register
  - VLR : Visitor Location Register
- Algorithms
  - A3: Mobile Station Authentication Algorithm
  - A8: Session (cipher) key generation Algorithm
  - PRNG: Pseudo-Random Number Generator
- Random number, keys and signed response

GSM Authentication Protocol

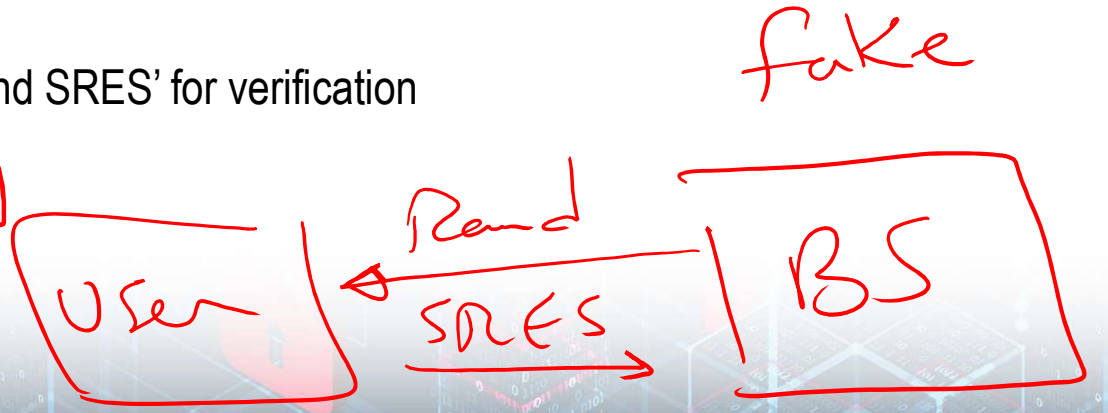


IMSI: International Mobile Subscriber Identity
RAND: Random Number
SRES: Signed Response
Ki: Stored in the HLR and in the SIM
Kc: Cipher Key

Authentication Procedure

- MS send IMSI to the network subsystem (AuC and HLR)
- The network subsystem received the IMSI and find the correspondent Ki of the IMSI
- The AuC generate a 128-bit RAND and send (RAND, SRES, Kc) to MS
- The AuC calculate the SRES with A3 algorithm
- MS calculates a SRES with A3 using Ki and the given RAND
- MS sends the SRES' to the network
- The visited network compare the SRES and SRES' for verification

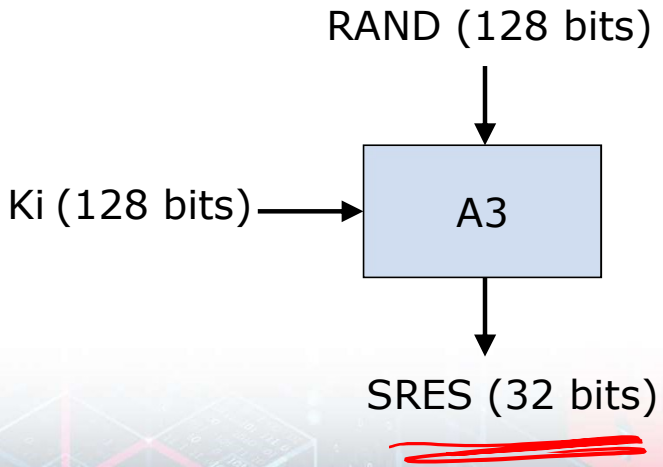
- Note: no base station authentication



A3 – Authentication Algorithm

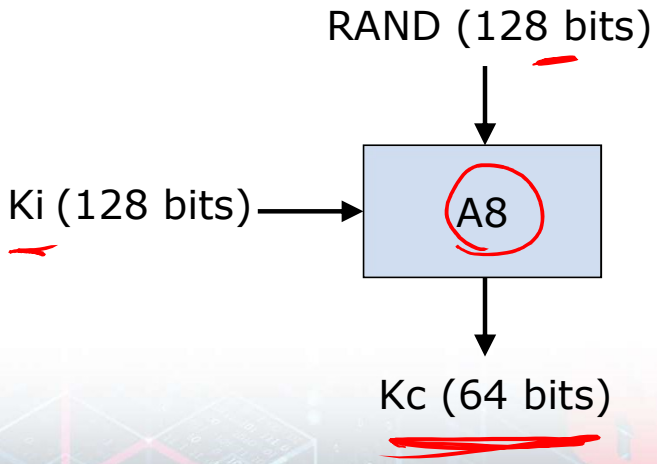
➢Goal

- Generation of SRES response to random number RAND
- Run-time of A3 < 500ms



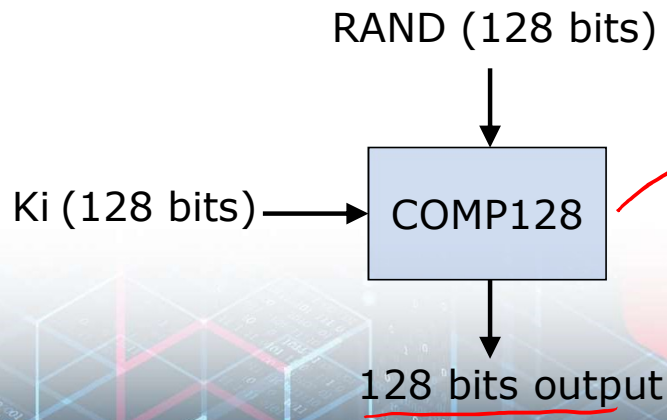
A8 – Cipher Key Generation Algorithm

- Goal - Voice Privacy
  - Generation of Cipher key – Kc
  - A8 specifications never made public



Implementation of A3 and A8

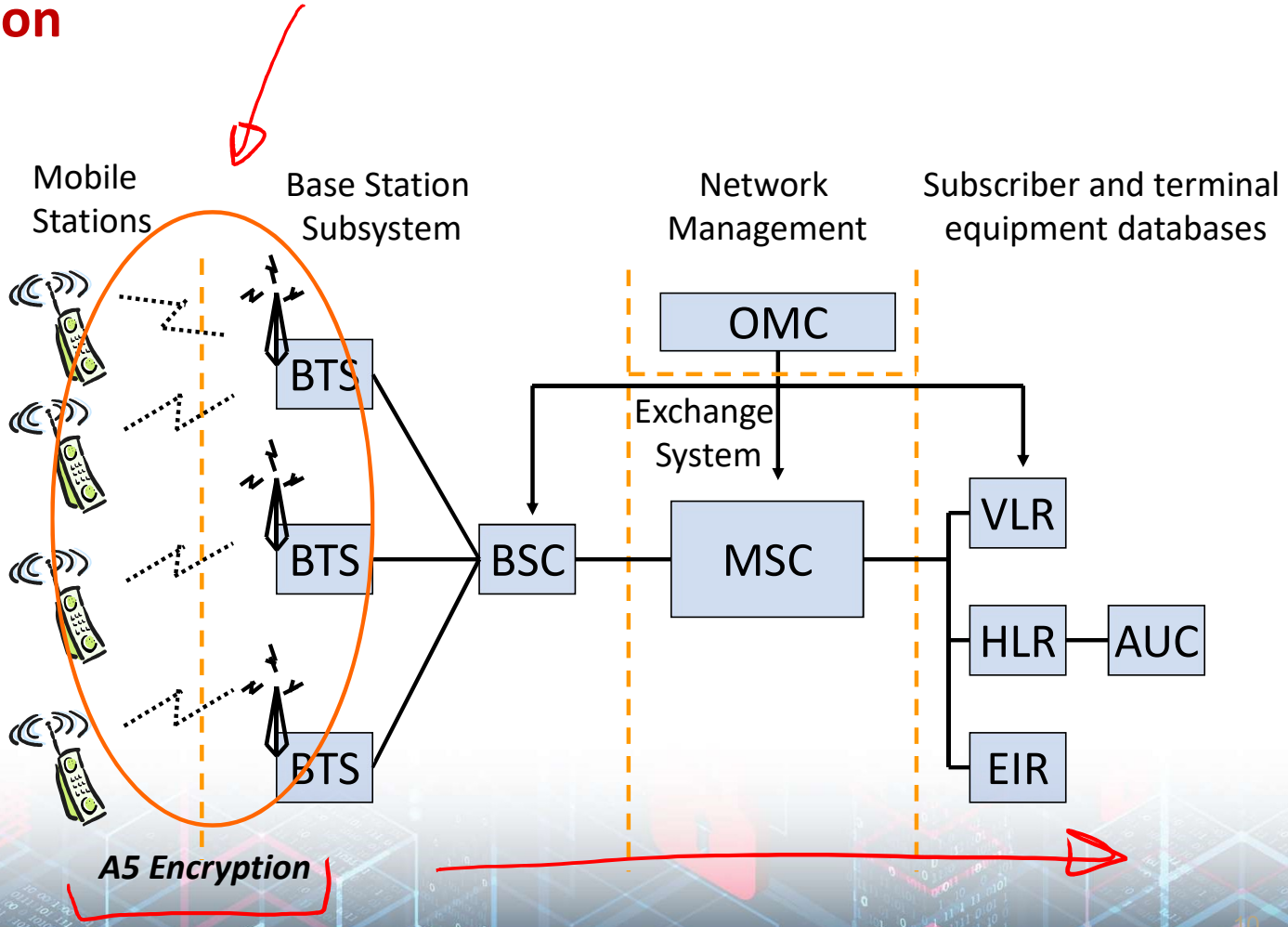
- Both A3 and A8 algorithms are implemented on the SIM. It is independent of hardware manufacturers and network operators.
- COMP128 is keyed hash function, used for both A3 and A8 in most GSM networks.



keyed hash function

SRES = first 32 bits
Kc = last 54 bits

A5 Encryption



Providing Confidentiality

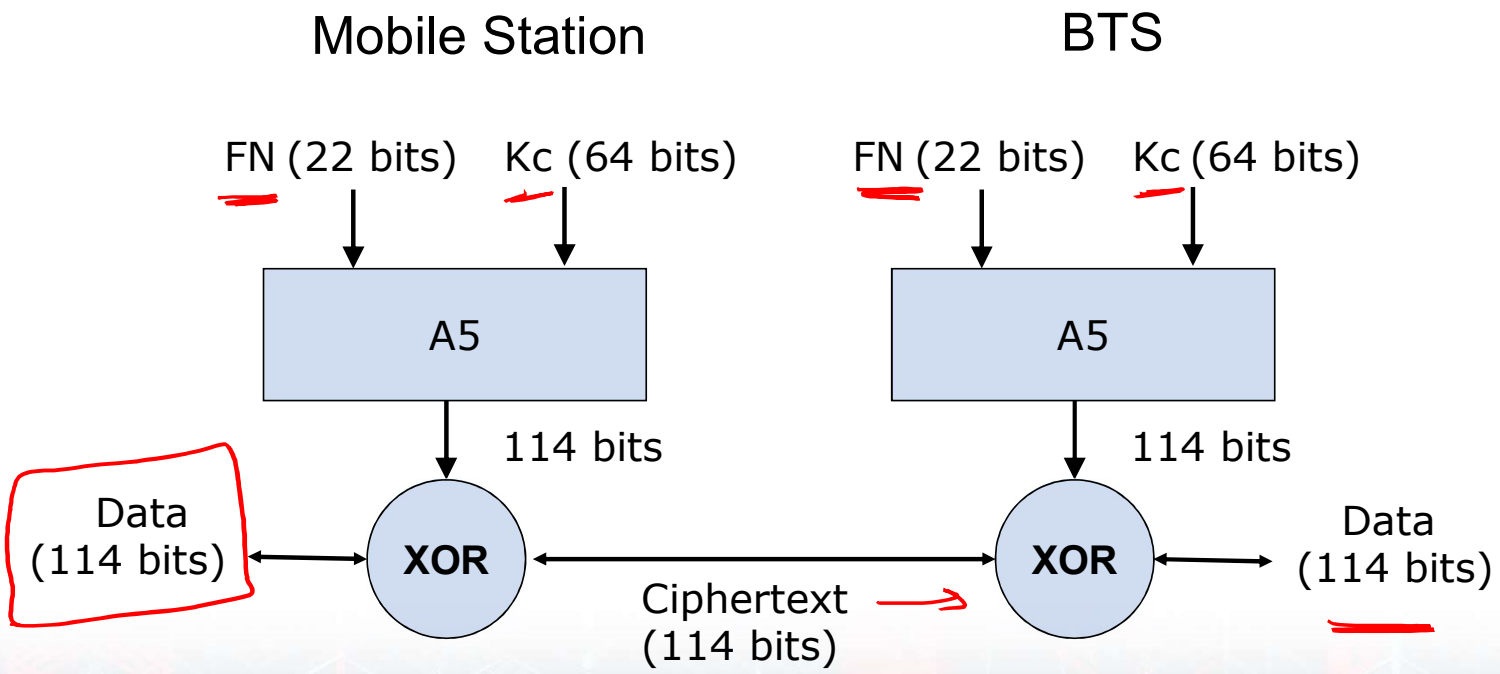
- After the authentication protocol, cipher key Kc is shared between the subscriber and the visited network.

- A5 is used as an over-the-air voice privacy algorithm

  - A5 is a stream cipher

  - Implemented very efficiently on hardware

Encryption Scheme



FN : Frame Number

Kc: Cipher Key

Providing Anonymity

- Protection of the subscriber's identity from eavesdroppers on the wireless interface
  - How to do it? In the real life, if you change you name frequently, nobody can trace your behavior. Is that right?
  - To use IMEI as seldom as possible.
  - In GSM, short-term temporary identifier are used. It is a random number and always changes.

- Usage of short-term temporary identifiers- TMSI

Subscriber Identity Protection

➢ TMSI – Temporary Mobile Subscriber Identity

- TMSI is used instead of IMSI as an a temporary subscriber identifier.
- TMSI prevents an eavesdropper from identifying of subscriber.
- VLR performs assignment, administration and update of the TMSI

Detection of Compromised Equipment

- International Mobile Equipment Identity (IMEI)
  - Identity allows to identify mobile phones
  - IMEI is independent of SIM
  - Used to identify stolen or compromised equipment

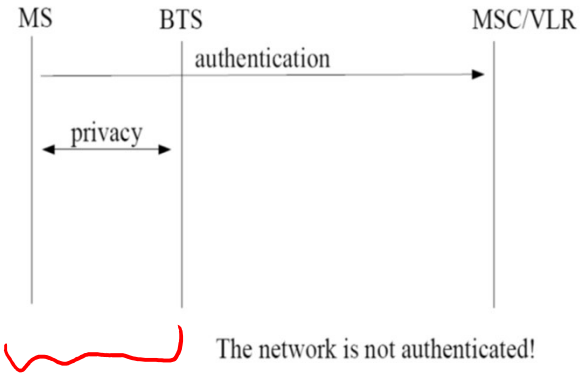
- Equipment Identity Register (EIR)
  - Black list – stolen or non-type mobiles
  - White list – valid mobiles
  - Gray list – local tracking mobiles

Attacks against GSM Security

- Attacks against anonymity
- Attacks against authenticity and confidentiality
  - Attacks against the cryptographic algorithms
  - Attacks against the GSM protocol

GSM Security Problems

- Cryptanalysis attacks against A3/A5/A8/COMP-128 algorithm
- Over-the-air interception using fake BTS
- Only air interface transmission is encrypted
- Ciphering key (Kc) used for encryption is only 54 bits long
- No messages authentication and integrity protection

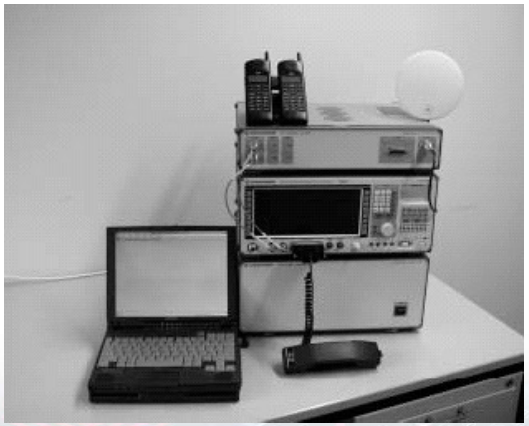


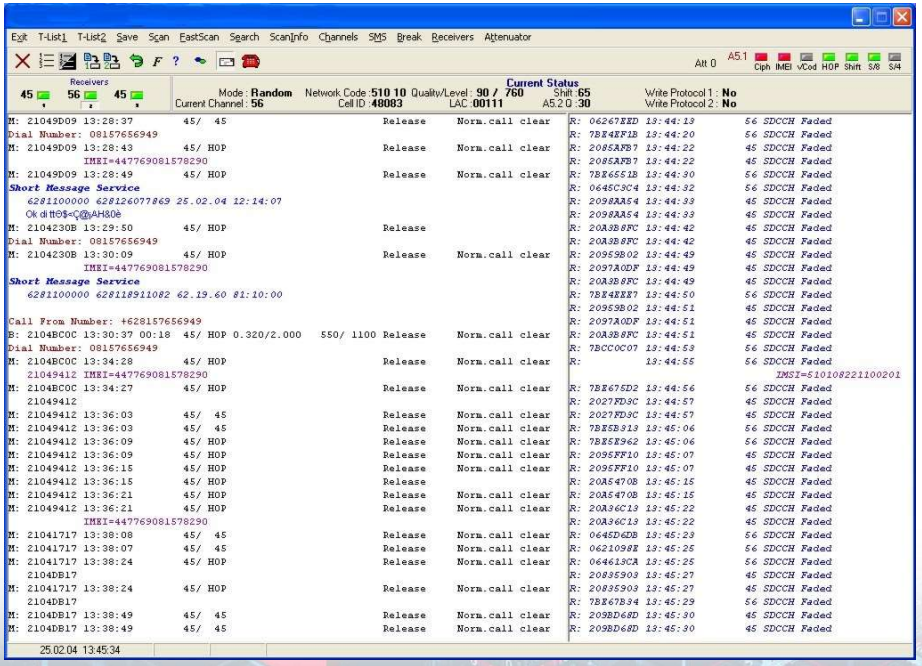
Attacks on GSM Security

- Attacks on A3/A8, A5/1
  - Through air interface
- False base station
  - GSM does one-way authentication (network authenticate user only)
- DoS
  - Jamming the signal
  - Preventing the MS from communicating

IMSI Catcher (Fake Base Station)

- IMSI-catchers are used legaly by law enforcement and intelligence agencies.

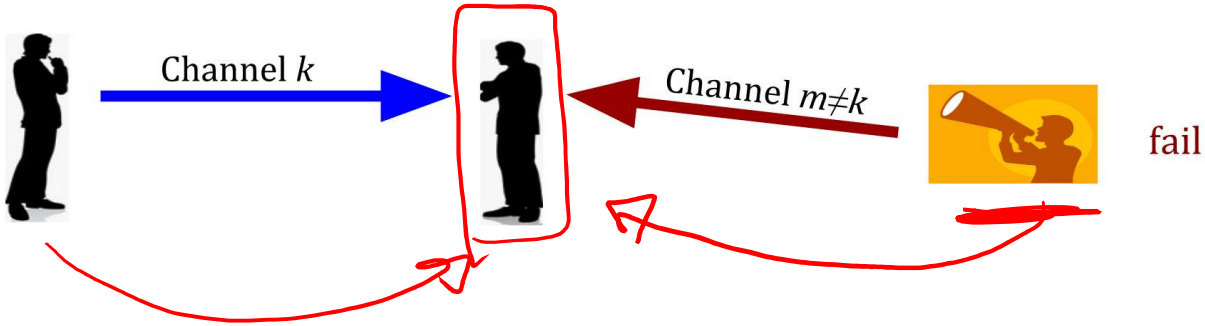




Attacks on GSM Security
Jamming

Jamming must use high power to decrease the SINR

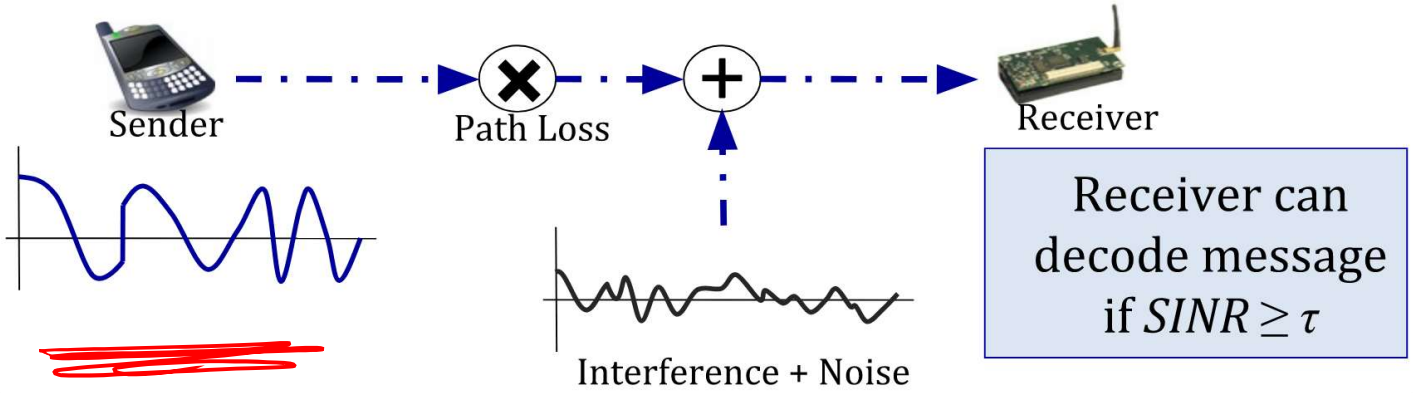
However, it must use the same channel “k”



Attacks on GSM Security (Cont.)
Jamming

Jamming is a physical layer DoS attack that aims to prevent wireless communication between two devices

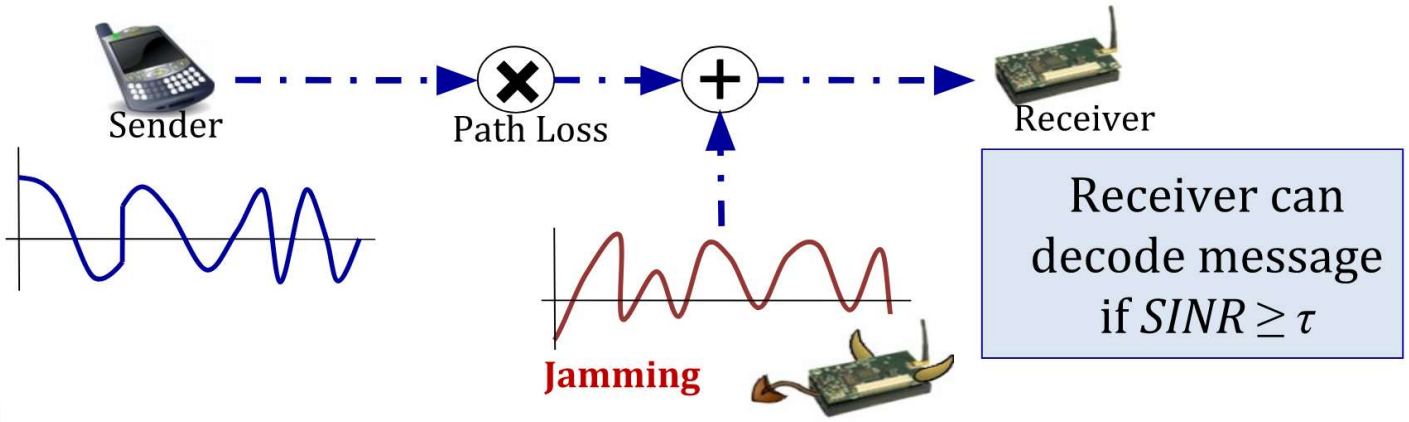
SINR: Signal to Interference and Noise Ratio



Attacks on GSM Security (Cont.)
Jamming

Jamming is a physical layer DoS attack that aims to prevent wireless communication between two devices

SINR: Signal to Interference and Noise Ratio



Jamming decreases *SINR*, causes ***decoding failure*** and ***packet loss***

Video summary

- GSM Authentication Algorithms A3 A8 Comp 128
- Encryption Algorithm (A5)
- Subscriber Identity Protection
- Attacks Against GSM