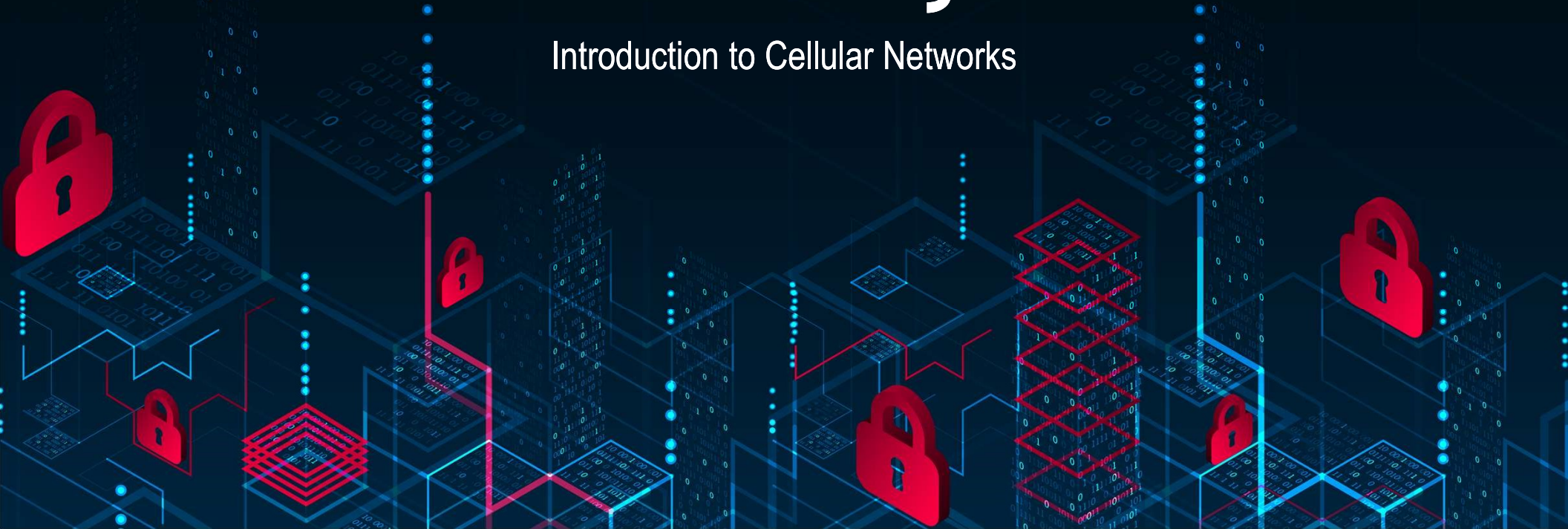


CPR E 431

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

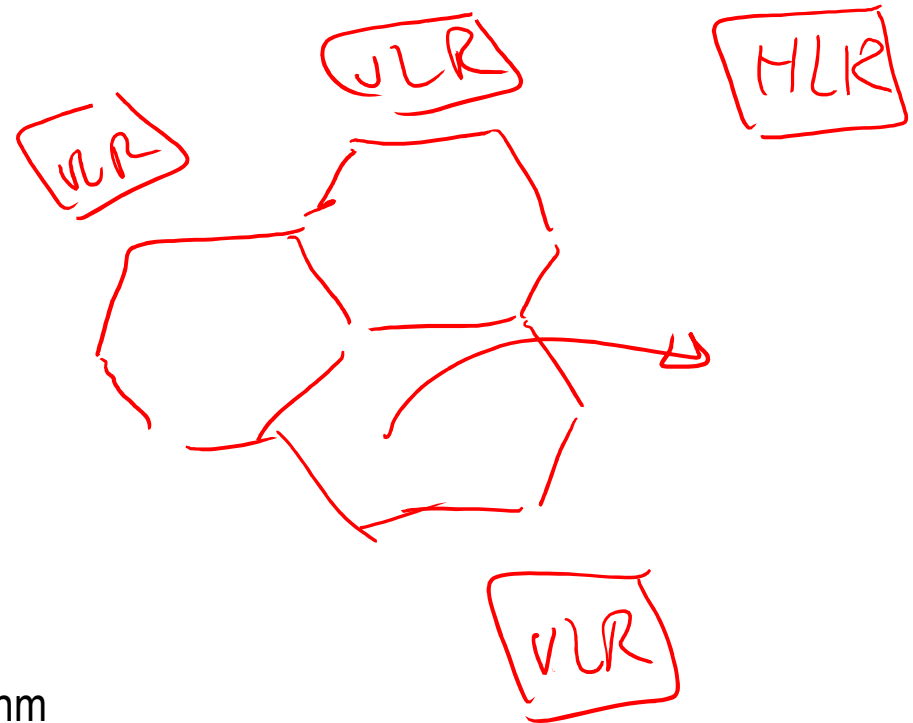
➤ Network Contains

- AuC : Authentication Center ✓
- HLR : Home Location Register ✓
- VLR : Visitor Location Register ✓

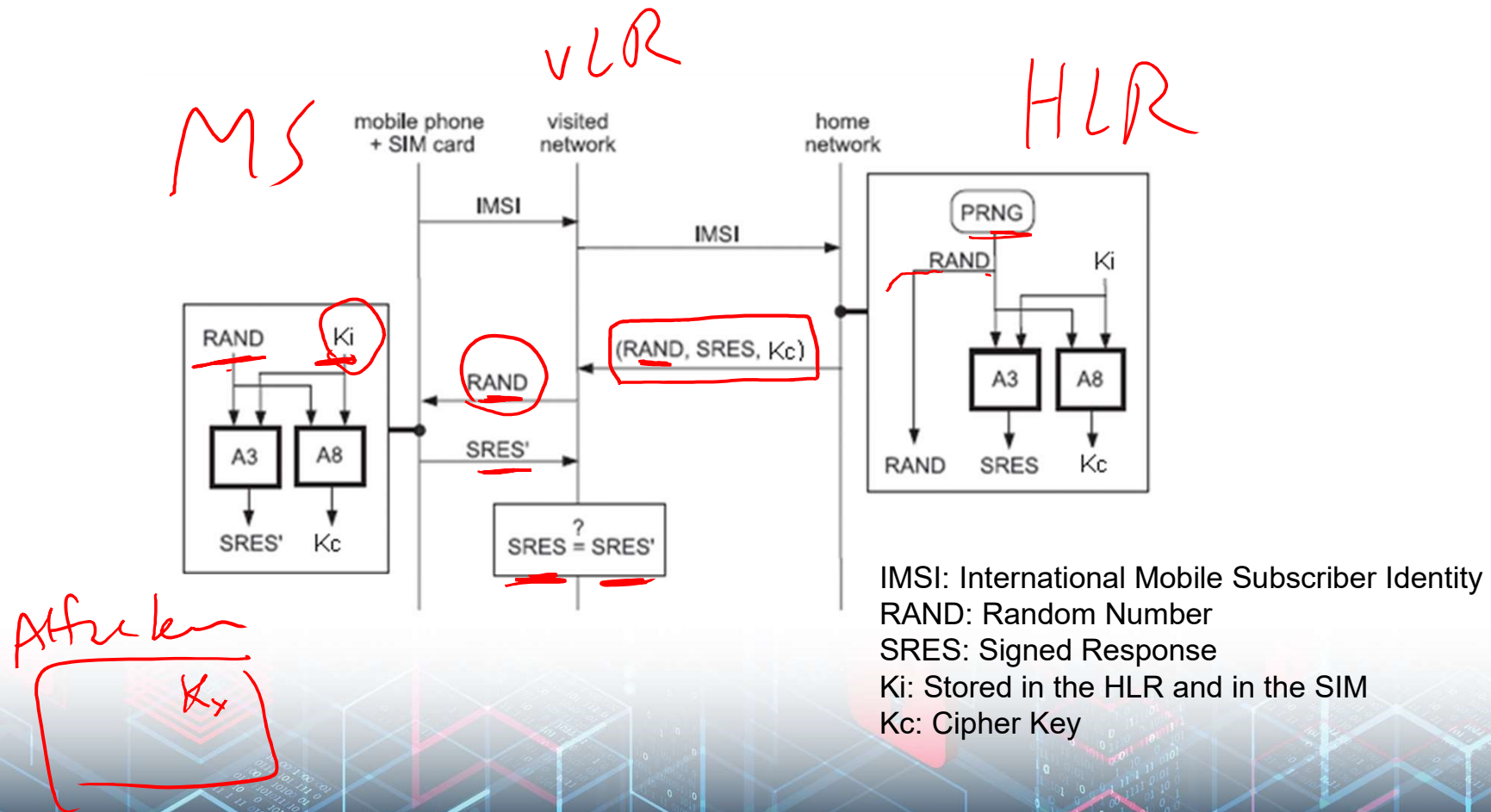
➤ Algorithms

- ➔ • A3: Mobile Station Authentication Algorithm
- ➔ • A8: Session (cipher) key generation Algorithm
- ➔ • PRNG: Pseudo-Random Number Generator

➤ Random number, keys and signed response



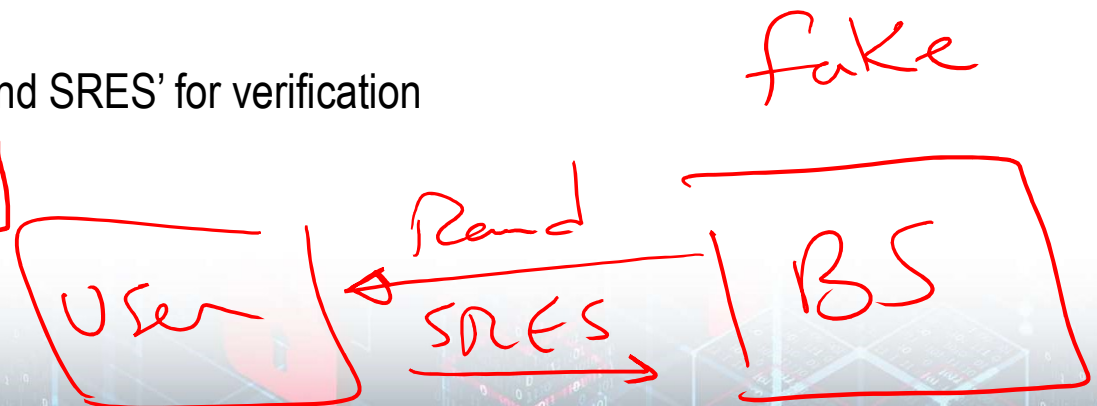
GSM Authentication Protocol



Authentication Procedure

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

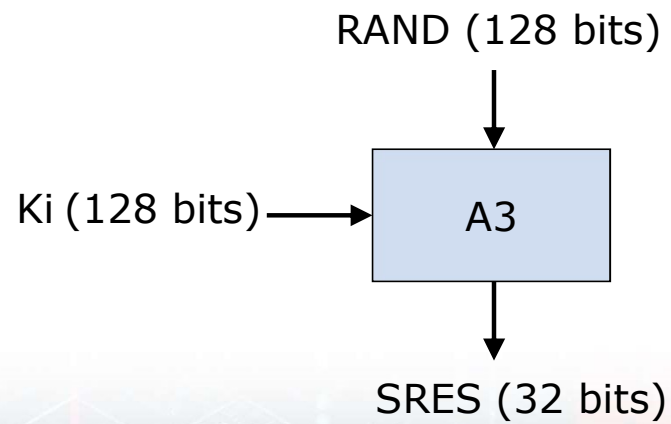
• Note: no base station authentication



A3 – Authentication Algorithm

➤ Goal

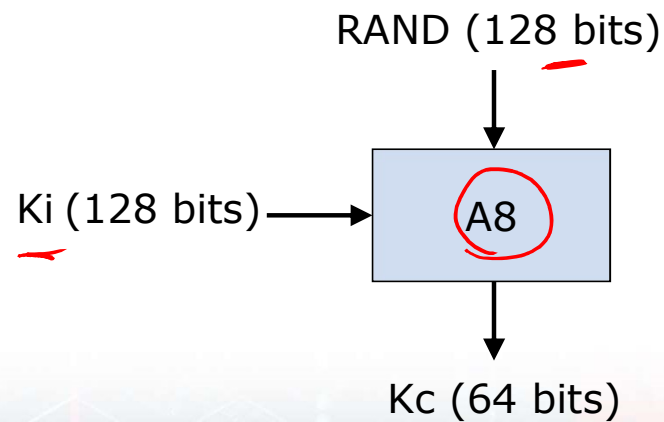
- Generation of SRES response to random number RAND
- Run-time of A3 < 500ms



A8 – Cipher Key Generation Algorithm

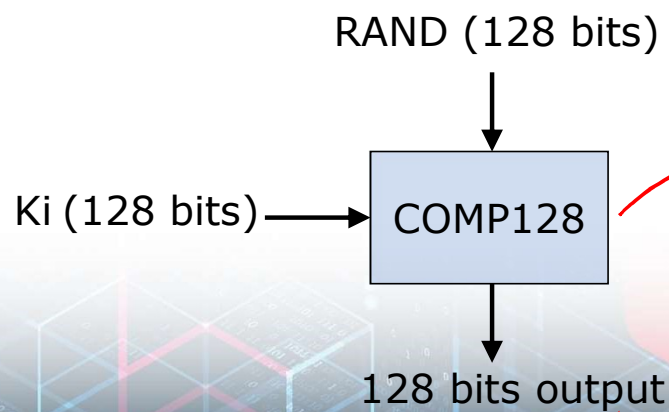
➤ Goal - Voice Privacy

- Generation of Cipher key – K_c
- A8 specifications never made public



Implementation of A3 and A8

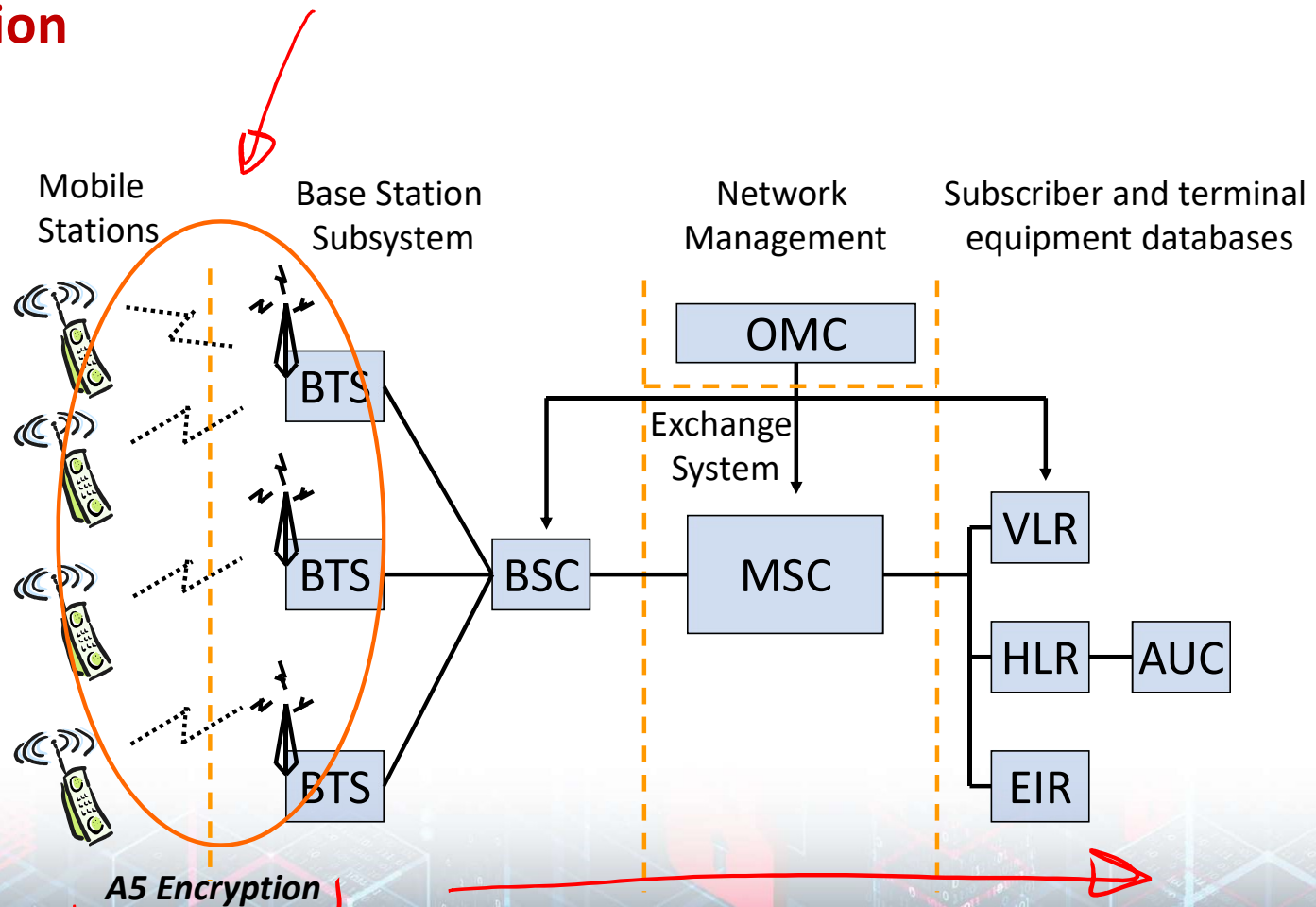
- Both A3 and A8 algorithms are implemented on the SIM. It is independent of hardware manufacturers and network operators.
- COMP128 is keyed hash function, used for both A3 and A8 in most GSM networks.



keyed hash func

SRES = first 32 bits
Kc = last 54 bits

A5 Encryption

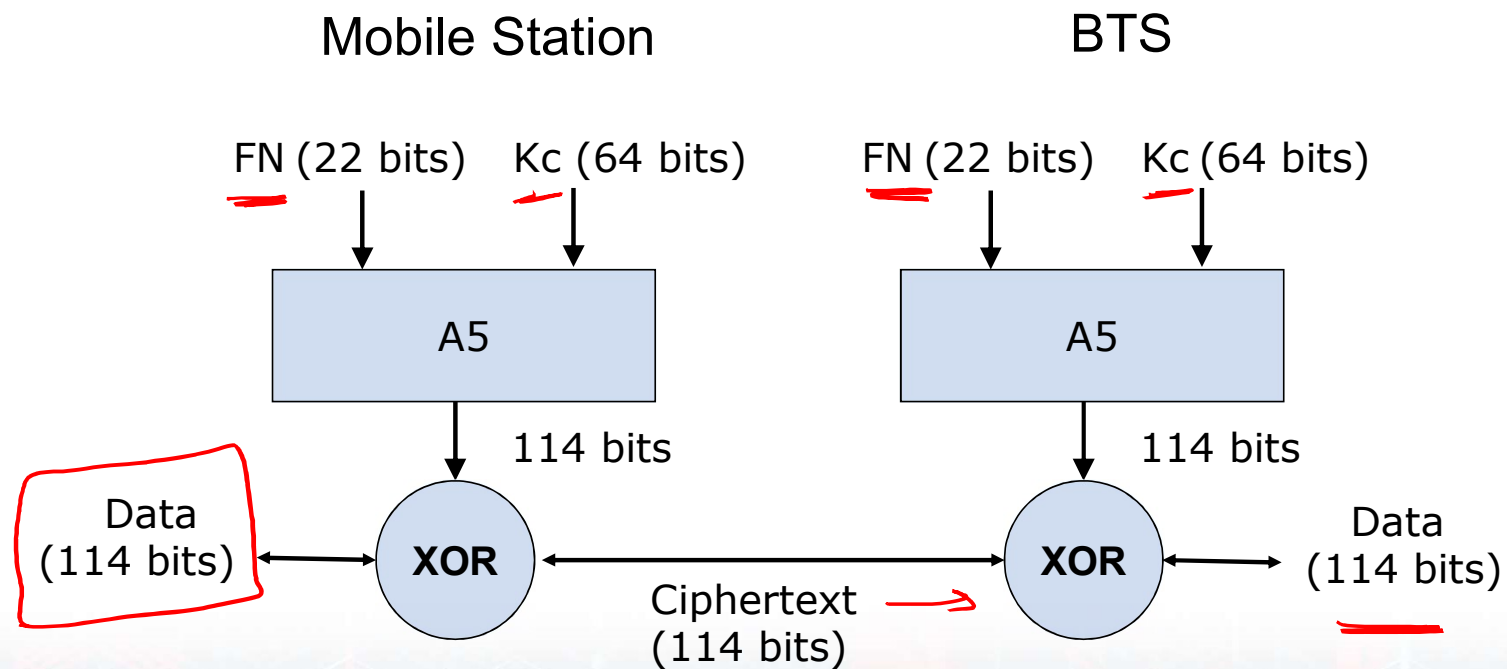


Providing Confidentiality

- After the authentication protocol, cipher key K_c 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 Mo2
 - Implemented very efficiently on hardware



Encryption Scheme



Providing Anonymity

IMSI → one time
only Authentication

➤ 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

IMSI 1 time 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



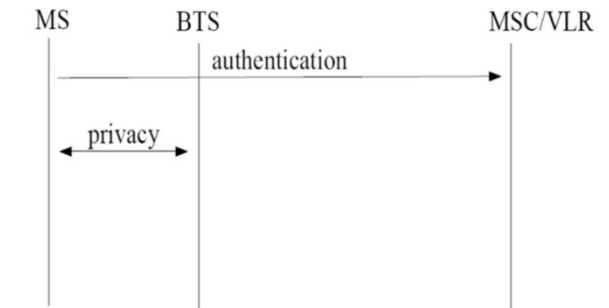
Attacks against GSM Security

- 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 (K_c) used for encryption is only 54 bits long
- No messages authentication and integrity protection



The network is not authenticated!

Encrypt

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 legally by law enforcement and intelligence agencies.



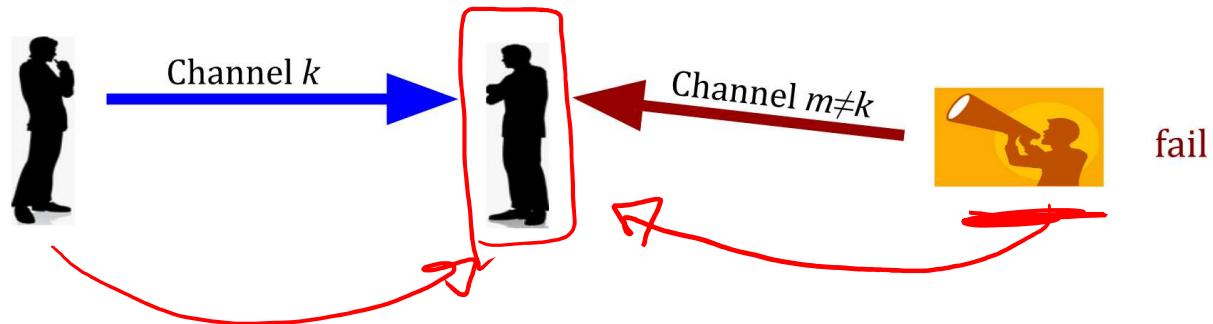
Egk T-list1 T-list2 Save Scan EastScan Search ScanInfo Channels SMS Break Receivers Attenuator									
Alt O A51 Cph IMEI Vcod HOP Shrt Sst SdA									
Receivers		Mode		Network Code		Current Status			
45	56	45		Random	510 10	Quality/Level: 90 / 760	65	Write Protocol 1:	No
Current Channel: 56					Cell ID: 48083	LAC: 00111	A52 Q 30	Write Protocol 2:	No
M: 21049D00	13:28:37	45/ 45		Release	Norm.call clear	Rx: 06267EED 19:44:13	56 SDCH Faded		
Dial Number:	08157656949					Rx: 208AFB1B 19:44:20	56 SDCH Faded		
M: 21049D00	13:28:45	45/ HOP		Release	Norm.call clear	Rx: 208ASB7B 19:44:22	45 SDCH Faded		
Dial Number:	08157656949					Rx: 208AB9F7 19:44:22	45 SDCH Faded		
M: 21049D00	13:28:49	45/ HOP		Release	Norm.call clear	Rx: 7B7655CB 19:44:30	56 SDCH Faded		
Short Message Service						Rx: 0645C3C4 19:44:32	56 SDCH Faded		
6281100000 628126077869 25.02.04 12:14:07 Ok dttos<C>@AH806						Rx: 209AA54 19:44:33	45 SDCH Faded		
M: 2104230B	13:29:50	45/ HOP		Release		Rx: 209BA54 19:44:33	45 SDCH Faded		
Dial Number:	08157656949					Rx: 20AB3BF7 19:44:42	45 SDCH Faded		
M: 2104230B	13:30:09	45/ HOP		Release	Norm.call clear	Rx: 209SB002 19:44:42	45 SDCH Faded		
JHE7=447769081578290						Rx: 209AADP 19:44:49	45 SDCH Faded		
Short Message Service						Rx: 20AB3BF7 19:44:49	45 SDCH Faded		
6281100000 628118911082 62.19.10 81:10:00						Rx: 7B74EBX7 19:44:50	56 SDCH Faded		
Call From Number:	+628157656949					Rx: 209SB002 19:44:51	45 SDCH Faded		
B: 2104BC0C	13:30:37 00:18	45/ HOP	0.320/2.000	550 / 1100	Release	Norm.call clear	Rx: 20AB3BF7 19:44:51	45 SDCH Faded	
Dial Number:	08157656949					Rx: 7BC0CC07 19:44:53	56 SDCH Faded		
M: 2104BC0C	13:34:28	45/ HOP		Release	Norm.call clear	Rx: 19:44:55	56 SDCH Faded		
Dial Number:	JHE7=447769081578290								
M: 2104BC0C	13:34:27	45/ HOP		Release	Norm.call clear				
Dial Number:	21049412								
M: 21049412	13:36:03	45/ 45		Release	Norm.call clear	Rx: 7B767FD2 19:44:56	56 SDCH Faded		
M: 21049412	13:36:03	45/ 45		Release	Norm.call clear	Rx: 2027FD3C 19:44:57	45 SDCH Faded		
M: 21049412	13:36:03	45/ HOP		Release	Norm.call clear	Rx: 2027FD3C 19:44:57	45 SDCH Faded		
M: 21049412	13:36:09	45/ HOP		Release	Norm.call clear	Rx: 7B75B913 19:45:06	56 SDCH Faded		
M: 21049412	13:36:15	45/ HOP		Release	Norm.call clear	Rx: 7B75EE62 19:45:06	56 SDCH Faded		
M: 21049412	13:36:15	45/ HOP		Release	Norm.call clear	Rx: 209EF7F0 19:45:07	45 SDCH Faded		
M: 21049412	13:36:21	45/ HOP		Release	Norm.call clear	Rx: 209EF7F0 19:45:07	45 SDCH Faded		
M: 21049412	13:36:21	45/ HOP		Release	Norm.call clear	Rx: 20A54708 19:45:15	45 SDCH Faded		
M: 21049412	13:36:21	45/ HOP		Release	Norm.call clear	Rx: 20A54708 19:45:15	45 SDCH Faded		
M: 21049412	13:36:21	45/ HOP		Release	Norm.call clear	Rx: 20A36C13 19:45:22	45 SDCH Faded		
M: 21049412	13:36:21	45/ HOP		Release	Norm.call clear	Rx: 20A36C13 19:45:22	45 SDCH Faded		
M: 21041717	13:38:08	45/ 45		Release	Norm.call clear	Rx: 064E262B 19:45:23	56 SDCH Faded		
M: 21041717	13:38:07	45/ 45		Release	Norm.call clear	Rx: 0621098E 19:45:25	56 SDCH Faded		
M: 21041717	13:38:24	45/ HOP		Release	Norm.call clear	Rx: 064613CA 19:45:25	56 SDCH Faded		

Attacks on GSM Security

Jamming

Jamming must use high power to decrease the SINR

However, it must use the same channel “k”

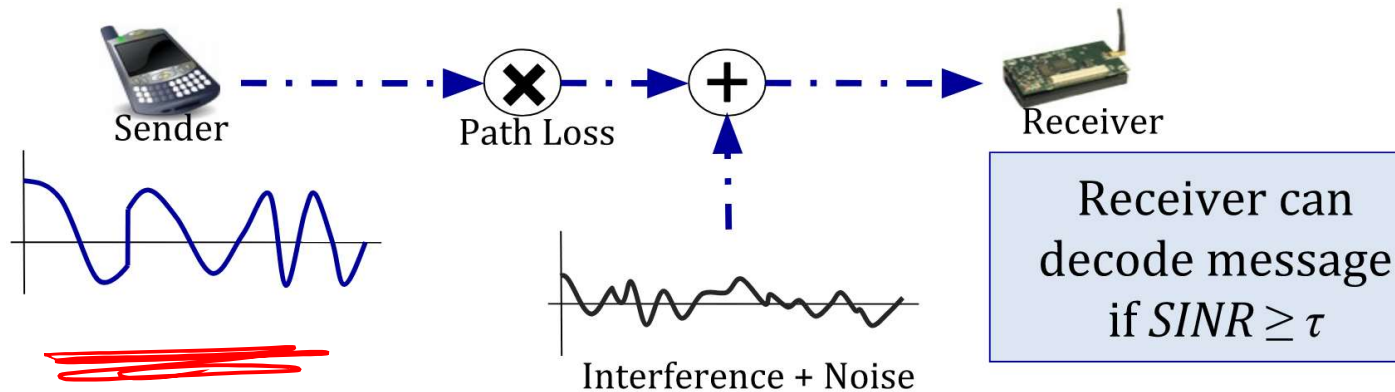


Attacks on GSM Security (Cont.)

Jamming

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

SINR: Signal to Interference and Noise Ratio

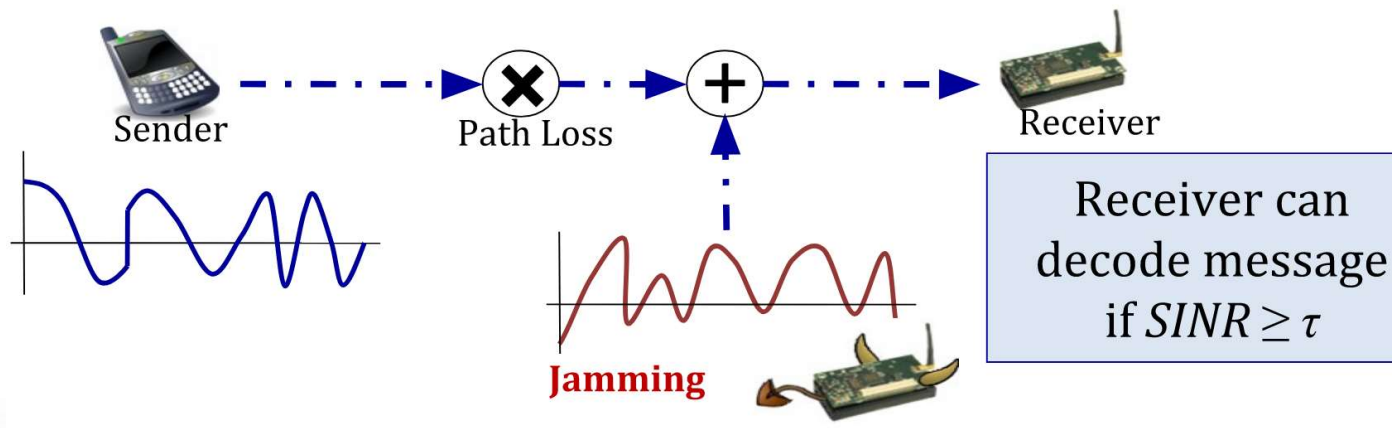


Attacks on GSM Security (Cont.)

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 A5 Comp 128

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

