GSM and 3G Security Summary and Vocabulary Help,

© Nicolas T. Courtois, 2006-2010
University College London

Telco	A national telephone company, in Europe used to be a part of a government agency PTT = the Postal Telegraph and Telephone
PSTN	Public Switched Telephone Network - analogue phone network
ISDN	Integrated Services Digital Network - digital phone standard, 64 kbit/s
PSPDN	Packet Switched Public Data Network – modern communication networks

0 G = Early analogue mobile phones

0 G	MTS: 1946-70s (half-duplex), IMTS: 1969-80s (full duplex, 2000$, 25 W),

1 G = Analogue mobile phones, no security

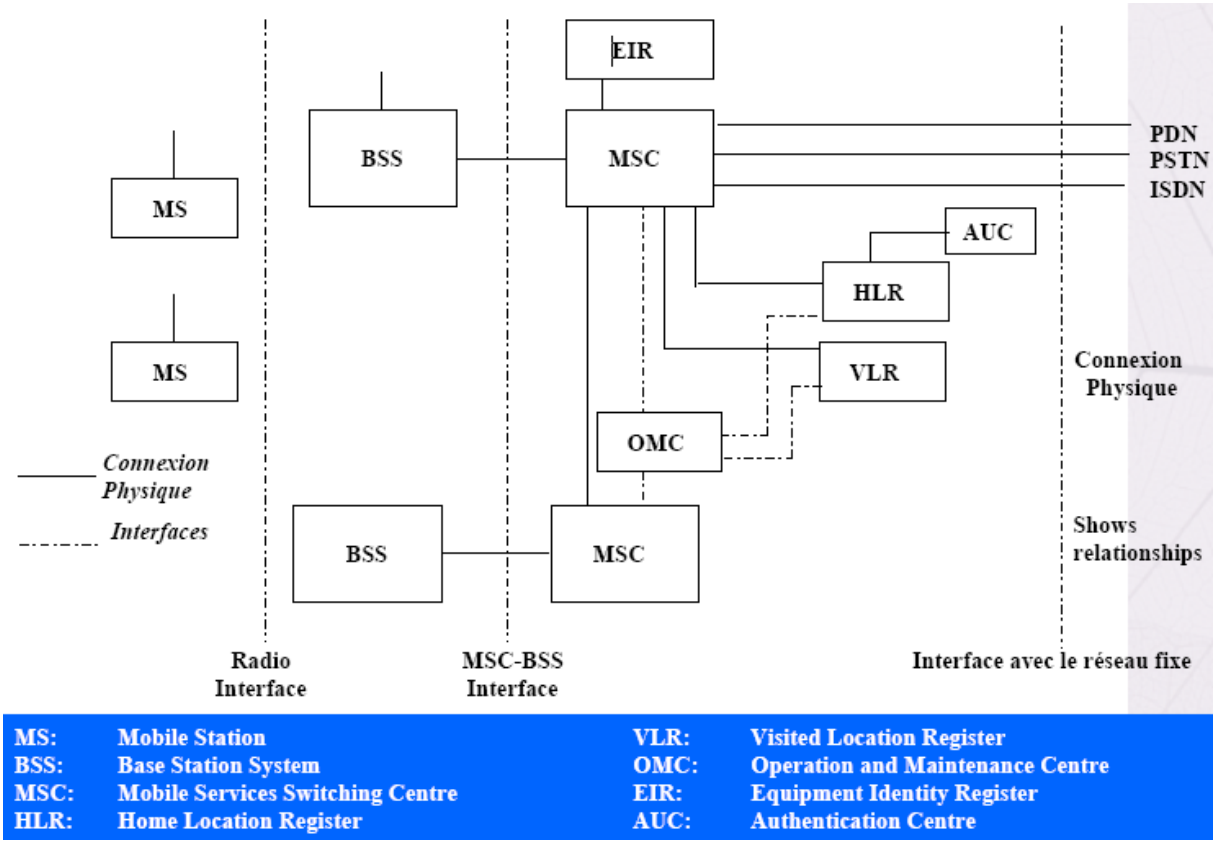
US 1 G	1990s, outdated, see slides by David Wagner from SAC 2002. US systems: There was no encryption, easy to eavesdrop, criminals played replay attacks and made free calls (2 % of all calls), US losses $650 million/year due to pirate calls
NMT	1981-2007, 450 MHz, Northern+Eastern Europe, better range than GSM (30 km), late models had analogue scrambling (two-band audio frequency inversion, prevents casual listeners). DMS Data and Messaging Service or NMT-Text, was used in Russia, Poland and Bulgaria, before SMS service started in GSM!
FDMA	Frequency DMA, multiple carrier bands at 450 and 850 MHz, 2.4 kbits/s

2 G = Digital mobile phones

Early US	All security was broken (XOR mask + CMEA , ORYX, CAVE), Cf. Wagner
GSM [EU, Asia,Aus]	Groupe Special Mobile [French, 1982] later pretended to be Global System for Mobile Communications [by ETSI, 1989, in English], 2W max, 13K bits/sec for speech 9.6 K for data (speech+ECC=22.8 k) on one TDMA channel out of theoretical capacity 270 kbits/s (time-shared).
TDMA	Time Division Multiple Access – air interface of GSM. 1 burst=0.577 ms.
CDMA [US]	Code-based Division Multiple Access, based on orthogonal sequences. Also set of 2G standards renamed cmdaONE, competitor of GSM, no smart cards, royalties=>Qualcomm<=chips. Better density !

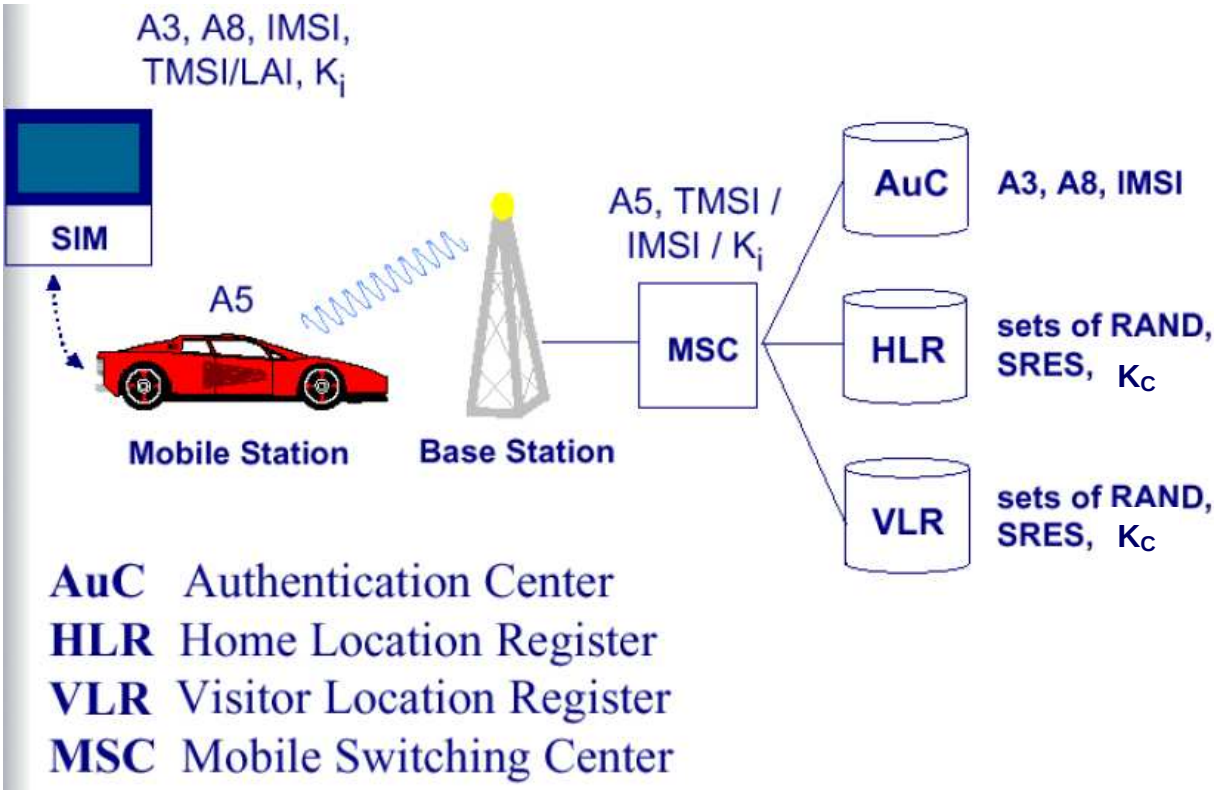
2.5 G and 2.75 G technologies

GPRS	General Packet Radio Service. Up to 8 time slots, with 9-21.4 Kbits/sec each (variable error correcting rate CS1-CS4), 3-5 slots used… (Class2-12) up to 48 Kbit/sec with Class 12 (serve more people - save money)
EDGE	Enhanced Data rates for GSM Evolution, 8 faster slots used, up to 8x48 = 384 kbit/s, EDGE Evolution: 1 Mbit/s, lower latency



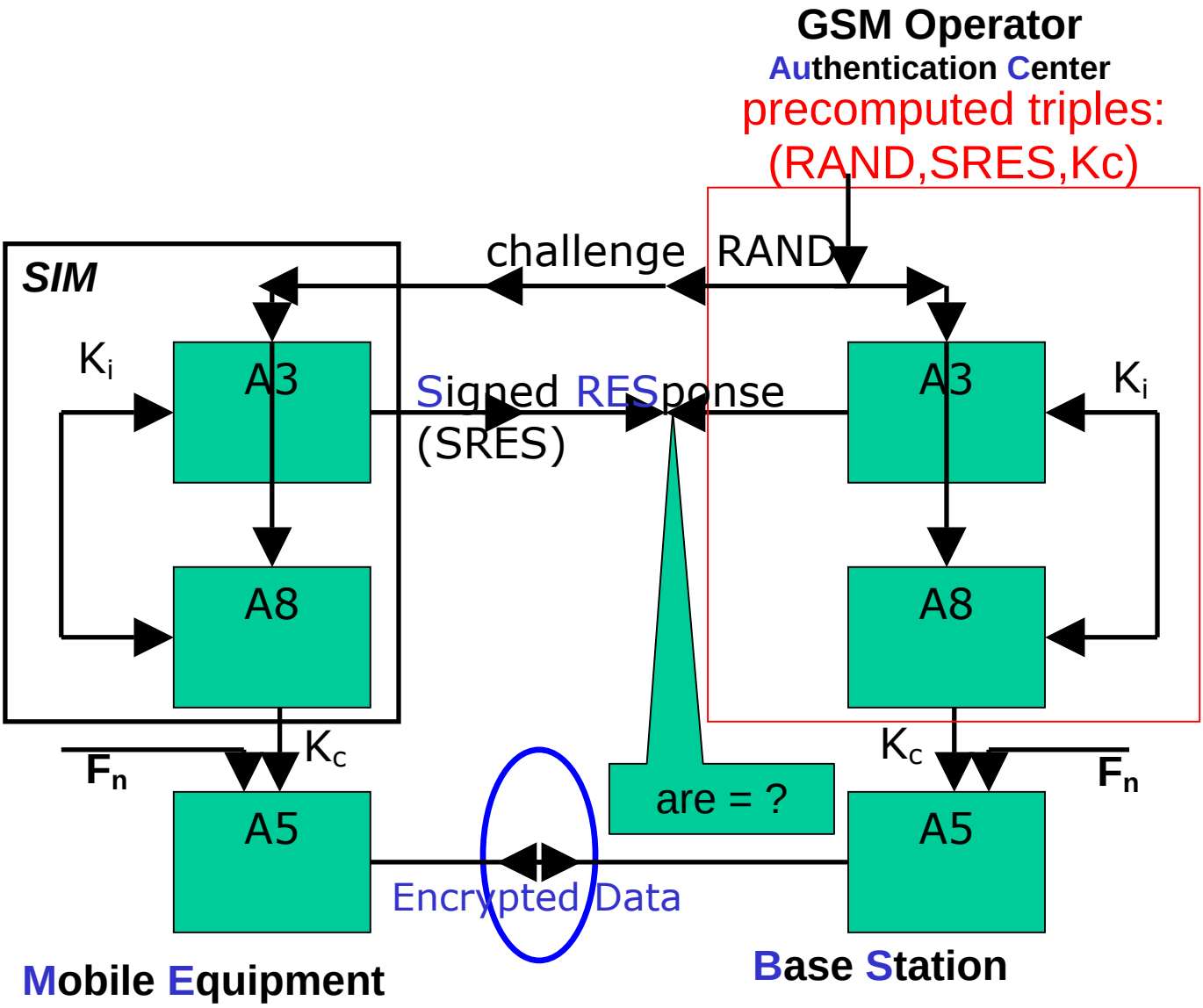
MS	Mobile Subscriber = ME+SIM
ME	Mobile Equipment
SIM	Subscriber Identity Module
IMEI	International Mobile Equipment Identity – unique for each ME
IMSI	International Mobile Subscriber Identity – unique for each SIM, 15 digits. Used in exceptional circumstances, when the BTS asks for it, then the MS receives encrypted TIMSI to be used later
TIMSI	Temporary pseudonym that is really used, even when roaming to another network, 5 digits, changed on a regular basis [another encrypted TIMSI]
LAI	Local Area Information – uniquely identifies one base station
EIR	Equipment Identity Register = List of IMEIs in one network
BTS	Base Transceiver Station
handover	Moving from one BTS to another (e.g. when walking)
BSC	Base Station Controller – manages handover, connected to multiple BTS and MSC
BSS	Base Station System=1 BSC + several BTS
roaming	Moving to another network operator (same or another country)
MSC	Mobile Switching Centre: manages the communications between different mobiles and PSTN
SGSN	Serving GPRS Support Node - delivers packets to MSs within its service area through multiple BTSs
OMC	Operation and Maintenance Centre (manages MSCs and the whole network).
AuC	Authentication Centre
HLR	Home Location Register. Part of AuC. -Knows where to connect incoming call (which network, which cell).

VLR	Visitor Location Register: in the host network (can be in another country)



AuC	-Generates in advance triples (RAND, SRES, Kc)
HLR	Knows where to connect an incoming call -Stores many triples (RAND, SRES, Kc)
VLR	In the host network (can be in another country). -Receives and stores the triples for each TIMSI.
Ki	Diversified unique MS key on 128 bits, known only to SIM and AuC. Generated from master key + IMSI + optional data. By the operator.
A3,A8	Proprietary authentication (MAC = keyed hash) algorithms implemented in the SIM, operator dependent. Share common 128-bit input, common key Ki on 128 bits. Can be the same algorithm with two different outputs. Example: COMP128 – very insecure provided as a weak example… Input: RAND on 128 bits Output A3: 32 bit MAC called SRES (Signed RESponse) Output A8: Kc on 64 bits, 54 really used in A5/1 (the strongest before A5/3=Kasumi=only in 3G phones, not yet used in GSM).
A5/0-3	Public voice encryption algorithms, implemented in the phone, the station chooses which to use. Initialised with Kc and IV = frame number on 22 bits. Produces only 114 bits of keystream for this IV. These bits are XORed to the encoded (voice+…) frame. (228 bits are sent in both directions).
A5/2	Excessively weak… though designed using 15.75 man x months and all members of SAGE stated that they were satisfied that [A5/2] was suitable to protect against eavesdropping on the GSM radio path'' - ETSI TR 278
A5/1	Almost secure enough… but not used correctly at all: Biham Crypto 2003

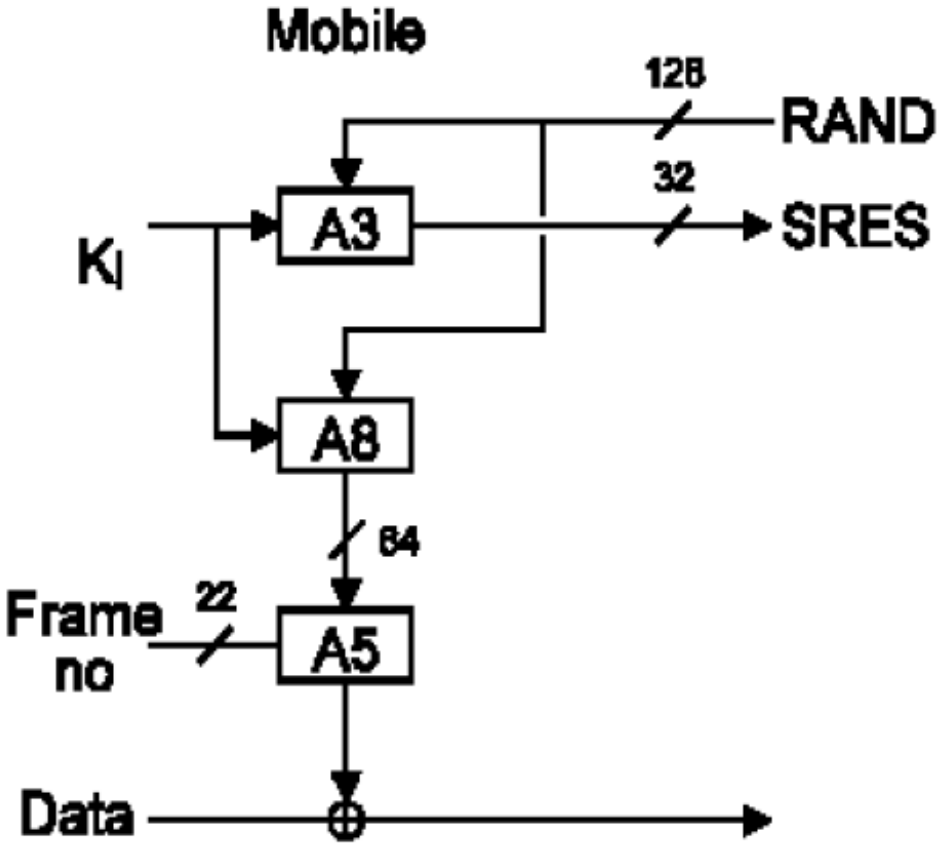
GSM Authentication and Encryption



- A3: Challenge-reply authentication 128->32 bits.
- A8: Session key Kc derivation - 64 bits - used for 1 phone call.
- A5/X: stream encryption of short frames of 114 bits.

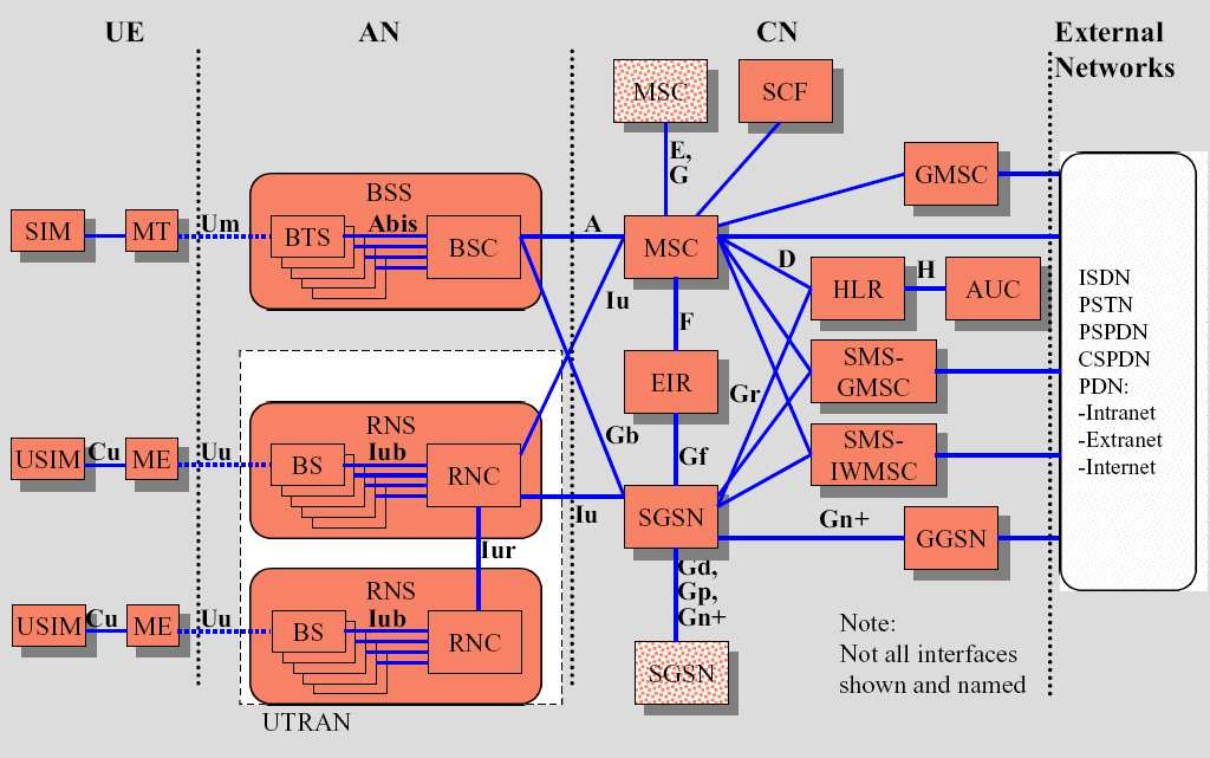
No authentication of the network -> phone. Fixed in UMTS.

SIM Card side and data/key sizes



- BS transmits to ME a 128-bit challenge RAND
- ME returns SRES on 32 bits
- K_i size: 56-128 bits, proprietary
- RAND and K_i are combined with A8 to get a 64-bit key K_c.
- this key K_c + frame number on 22 bits are used to encrypt blocks of 114 bits.
- Redundant data frames are encrypted + stream cipher => ciphertext-only attacks. GSM is BROKEN!

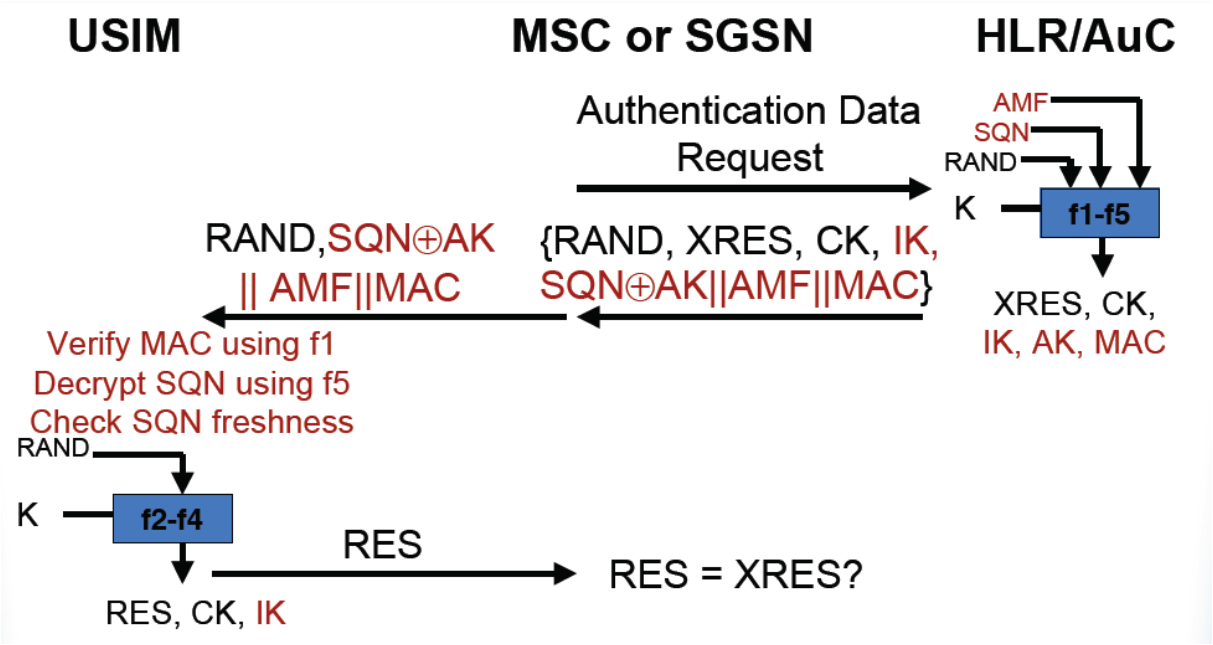
3G Architecture, extends 2G, compatibility and seem-less roaming



3G vocabulary

UMTS	Universal Mobile Telecommunications System, or 3GPP, main 3G mobile phone system. [Competitor: CDMA 2000]. Permanent 2Mbit/sec (pico cell, antenna on the building in front of you) and otherwise 144 Kbits/sec.
W-CDMA	Wideband Code Division Multiple Access, the air interface of UMTS, royalties=>Qualcomm
HSDPA, 3 G+	Extension of UMTS canal DCH for mobile broadband, now 3.6 Mbit/s and even 7.2 Mbit/s (Release 6) at some locations.
SGSN	GPRS Support Node
GGSN	Gateway GPRS Support Node
SMS-GMSC	Gateway MSC For Short Message Service, A function of an MSC capable of receiving a short message from an SC, interrogating an HLR for routing information and SMS info, and delivering the short message to the VMSC or the SGSN of the recipient MS.

3G security



A5/3 = Kasumi	Voice encryption algorithm + integrity algorithm, 128-bit keys, also added to the GSM standard (which explains the name) CK=cipher key on 128 bits IK =integrity key on 128 bits <= freshness, limited usage
AKA	Authentication and Key Agreement (the whole 3G security protocol)
MAC	f1_K(SQN || RAND || AMF) - on 64 bits
SQN	Sequence number of 48 bits
AMF	Authentication Management Field on 16 bits
AK	Anonymity key on 128 bits
AUTN	128 bits: network authentication token = SQN xor AK || AMF || MAC
Quintet	(RAND, XRES, CK, IK, AUTN)
USIM algos	Operator specific algorithm for f1,f2,f3,f4,f5 One example is MILENAGE, based on AES, but usually proprietary

Crypto comparison GSM vs. 3G

GSM			UMTS		
Description	Bits	Alg	Description	Bits	Alg
Ki Subscriber authentication key	128		K Subscriber authentication key	128	
RAND random challenge	128		RAND random challenge	128	
XRES exepected result	32	A3	XRES expected result	32-128	f2
Kc cipher key	64 max	A8	Ck cipher key	128	f3
			IK integrity key	128	f4
			AK anonimity key	48	f5
			SQN sequence number	48	
			AMF authentication management field	16	
			MAC message auth. Code	64	f1
Example : algorithm COMP128-1			Example : algorithm Milenage		