České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE – 14.přednáška

Zabezpečení komunikace v mobilních sítích

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz

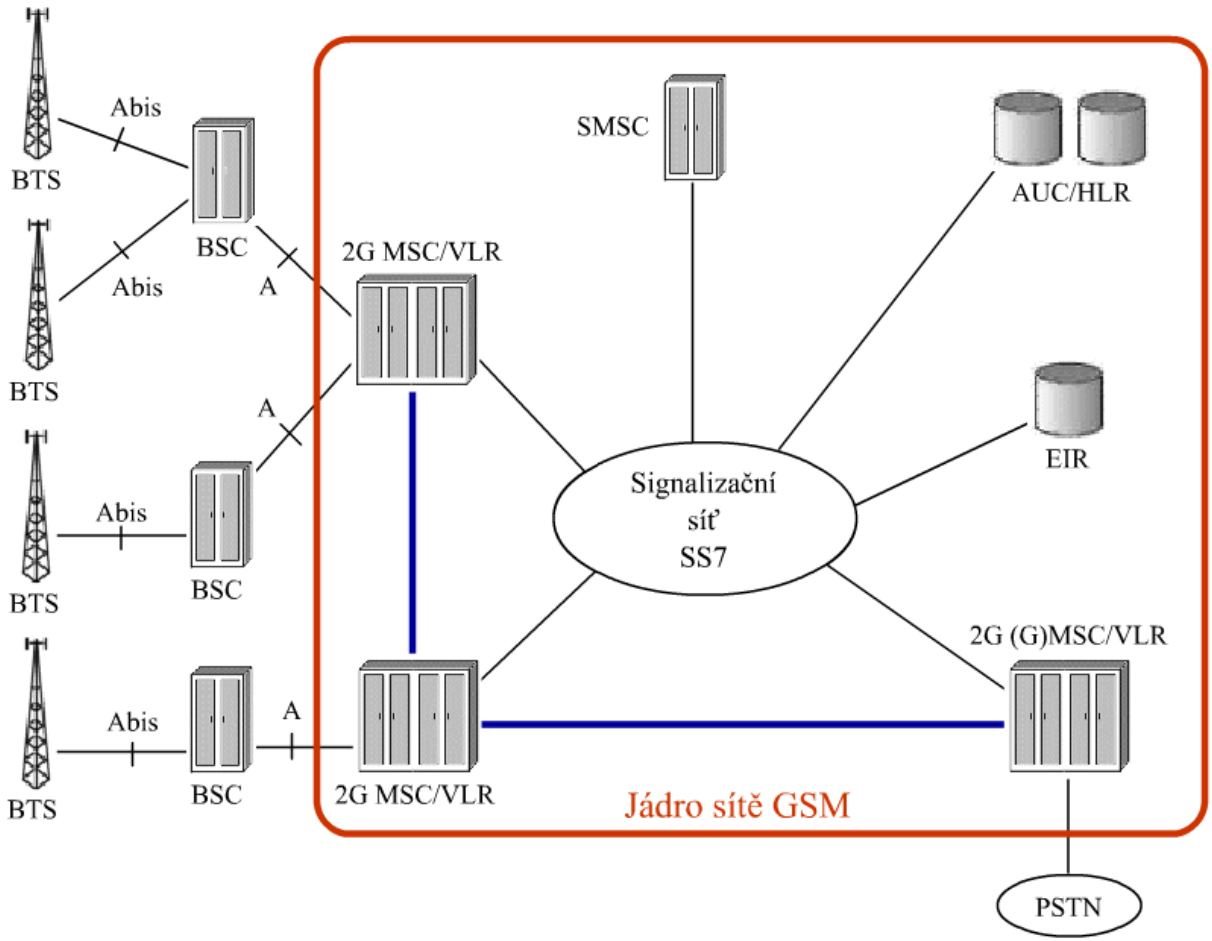
Osnova

- 2G – GSM, GPRS/EDGE
- 3G – UMTS
- 4G – LTE, LTE-A

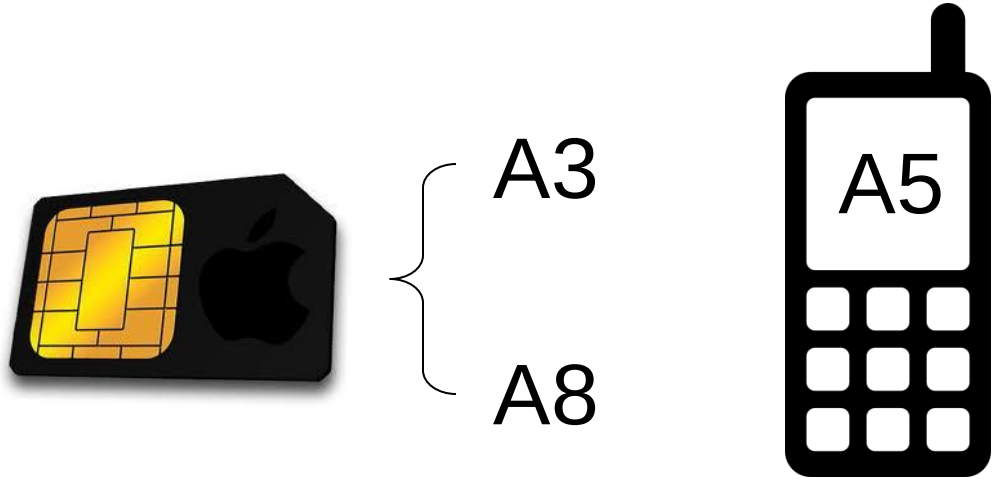
- Anonymita
- Autentizace
- Šifrování
- Integrita

GSM / GPRS

Struktura GSM sítě



Kryptografické algoritmy v GSM



Algoritmy, které jsou používány pro šifrování v mobilní síti GSM:

- A3 - autentizační algoritmus
- A5 - šifrovací algoritmus
- A8 - generátor klíče K_c pro hlasovou komunikaci

SIM obsahuje ještě tajný klíč K_i, který je uložen i v AuC.

Kryptografické algoritmy v GSM

- navrženy v ETSI (European Telecommunications Standards Institute) skupinou SAGE (Security Algorithms Group of Experts)
- původní algoritmy byly utajované, ale unikly na veřejnost
- A3
  - algoritmus pro autentizaci MS
  - **Vstup:** klíč K_i128b , náhodné číslo 128b
  - **Výstup:** otisk 32 b – SRES
  - takřka vždy realizován pomocí algoritmu COMP128
  - COMP128 byl součástí návrhu specifikace GSM sítě

Kryptografické algoritmy v GSM

- A8
  - algoritmus pro generování klíčů pro šifrování rádiového rozhraní
  - většinou pomocí šifry COMP128
  - **Vstup:** klíč K_i 128b, náhodné číslo RAND
  - **Výstup:** klíč K_c 64b,
  - K_c je používán dokud MSC nerozhodne o reautentizaci zařízení
- A3 a A8 jsou implementovány v SIM kartě
  - operátor si je může implementovat po svém
  - autentizace probíhá v domovské síti → místní síť nemusí znát tyto algoritmy, přesto se autentizace povede

Kryptografické algoritmy v GSM

- COMP128 není veřejný
- princip odhalen při používání SIM karet a později unikla kompletní specifikace (1998)
  - http://www.iol.ie/~kooltek/a3a8.txt
- v jednom cyklu vygeneruje jak SRES tak K_c
    - horních 32b SRES
    - spodních 54b + 10 nul K_c
    - efektivní délka klíč K_c je pouze 54b

Bezpečnostní model GSM

IMSI – International Mobile Subscriber Identity

- identifikace účastníka
- uloženo na SIM kartě
- skládá se ze 3 částí:
  1. Mobile Country Code (MCC) - 230
  2. Mobile Network Code (MNC)

T-mobile	01	
O2 CZ	02	
Vodafone	03	
U:fon	04	
SŽDC	98	(Správa železniční dopravní cesty)
Vodafone	99	

  3. MSIN - Mobile Subscriber Identity Number („telefonní číslo“)

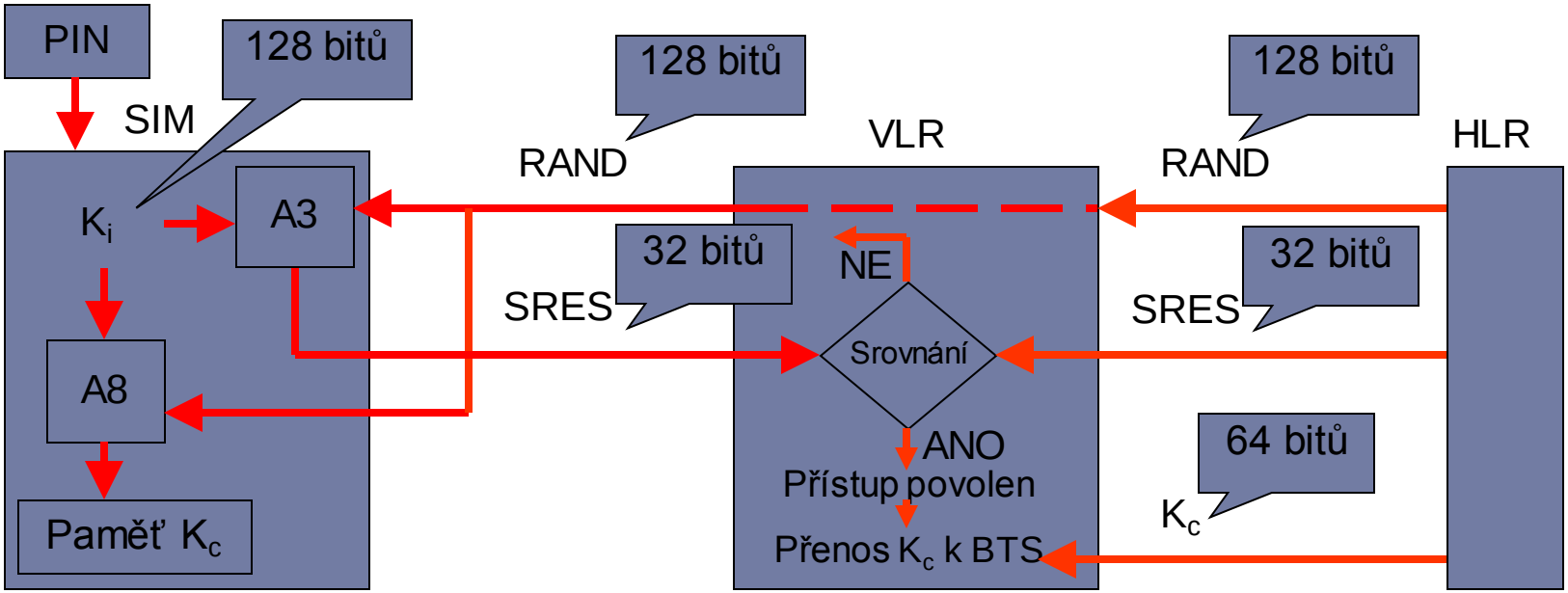
Bezpečnostní model GSM

- IMSI je globálně jednoznačný
  - při komunikaci mezi MS-síť se nepoužívá IMSI
  - bylo by možné sledovat, kde se nachází konkrétní uživatel
- používá se TMSI (Temporary IMSI)
- v datových sítích se používá P-TMSI (Packet TMSI)
  - pouze lokální platnost (pouze v rámci LA/RA), kde je účastník zaregistrován)
  - vazba IMSI-TMSI/P-TMSI udržována ve VLR/SGSN
  - TMSI je používána při požadavcích na:
    - paging
    - aktualizaci lokační oblasti
    - spojení
    - ukončení spojení…
- TMSI/P-TMSI snižuje možnost monitorování a sledování účastníků

Autentizace v GSM

- Kdo se účastní autentizace:
  - SIM karta
  - AuC (Authentication Center) – v domácí síti
- jednosměrná autentizace MS→síť
- založeno na tajném klíči K_i - 128 bitů
- K_i uložen pouze na SIM a v AuC
- **autentizace se odehrává vždy v domácí síti**
  - autentizační algoritmus je nezávislý na samotné mobilní síti, ve které probíhá
  - autentizace funguje i v cizích sítích
- autentizace typu „challenge-response“
- využívá algoritmus A3

Autentizace v GMS - algoritmy A3 a A8



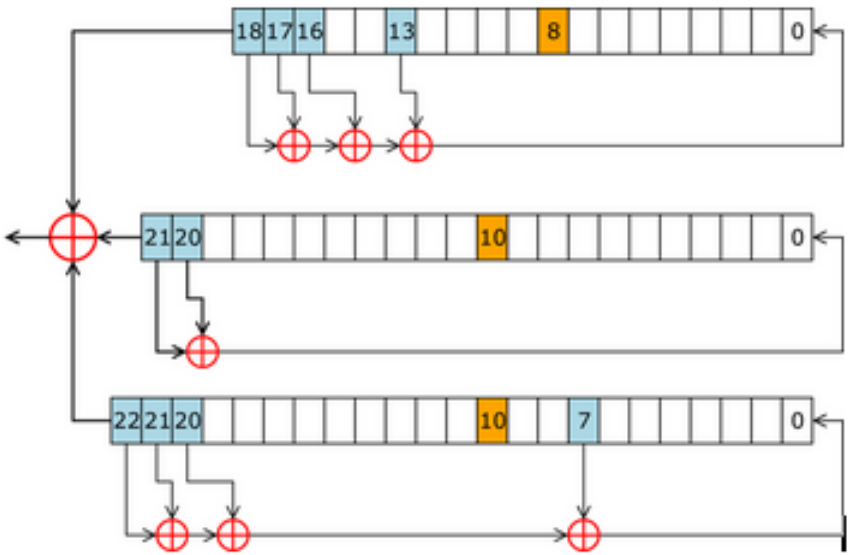
- A3/8, A38, COMP128 – různé názvy pro jeden algoritmus
- A3 ani A8 nejsou specifikovány v doporučeních ETSI
- (RAND,SRES, K_c) – autentizační triplet

Utajení v GSM

- šifrování na rádiovém rozhraní mezi MS a BTS (U_m)
- jediné šifrované rozhraní v celé GSM síti
- šifrovací algoritmus A5 je uložen v MS
  - stejný pro všechny operátory
- klíč je generován algoritmem A8 uloženým na SIM
  - algoritmus A8 si může operátor zvolit
- vstup do A5:
  - relační klíč K_c = A8(RAND, K_i) délky 64 bitů
  - K_c - nemění se často (pouze při autentizaci)
  - číslo TDMA rámce (22 bitů)
- výstup: 2x 114 bitů

Utajení v GSM

- A5/1 obsahuje of 3 *posuvné registry*
  - X: 19 bitů ($x_{18}, x_{17}, x_{16}, \ldots, x_0$)
  - Y: 22 bitů ($y_{21}, y_{20}, y_{19}, \ldots, y_0$)
  - Z: 23 bitů ($z_{22}, z_{21}, z_{20}, \ldots, z_0$)



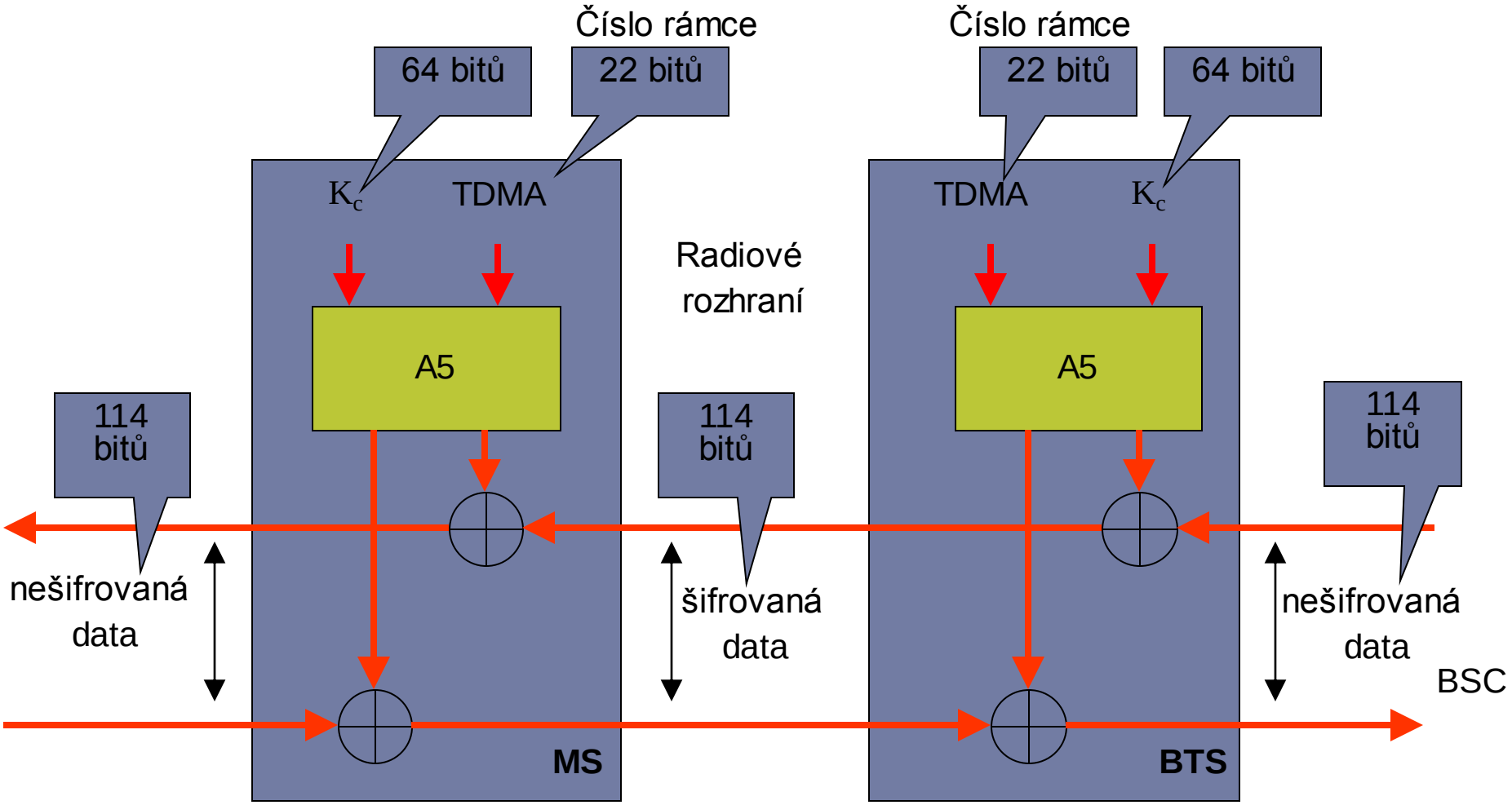
- klíčem je počáteční hodnota registrů
- každá buňka obsahuje 1 bit
- v každém kroku se registr posune nebo zůstane stát
- proud klíče vzniká XORem výstupu tří registrů

Varianty A5

Existuje několik verzí algoritmu A5, které poskytují různou úroveň zabezpečení:

- A5/0 – neposkytuje žádné zabezpečení
- A5/1 – původní algoritmus A5 používaný v Evropě
  - – prvních deset bitů klíče je nulových
  - – efektivní délka klíče – 54 bitů
- A5/2 – kryptograficky oslabená varianta algoritmu vytvořená pro export a používaná v USA
- A5/3 (Kasumi) – nový šifrovací algoritmus vytvořený jako součást 3rd Generation Partnership Project (3GPP)

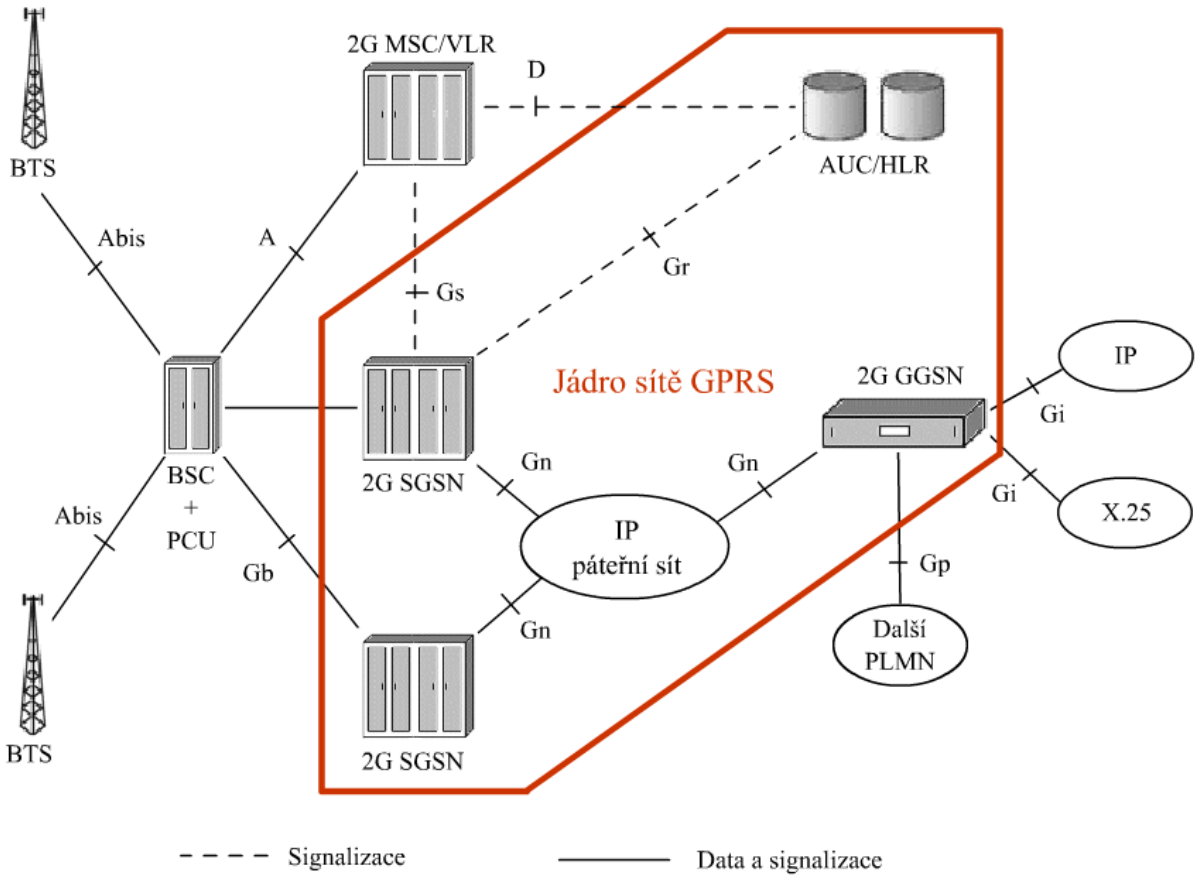
Použití algoritmu A5 v GSM



GSM - shrnutí

- anonymita – dobrá
- autentizace – špatná
  - pouze jednosměrná – možnost existence fake-BTS
  - neexistuje schéma pro výměnu klíčů
  - předsdílený klíč (K_i)
- šifrování – špatné
  - krátký klíč - 54b
  - slabý algoritmus – lze prolomit (rainbow tables)
  - data pro autentizaci včetně klíče K_C jdou přenášena v otevřeném tvaru mezi mobilními sítěmi
  - uživatel nepozná jestli je hovor šifrován, nebo ne
- integrita - žádná

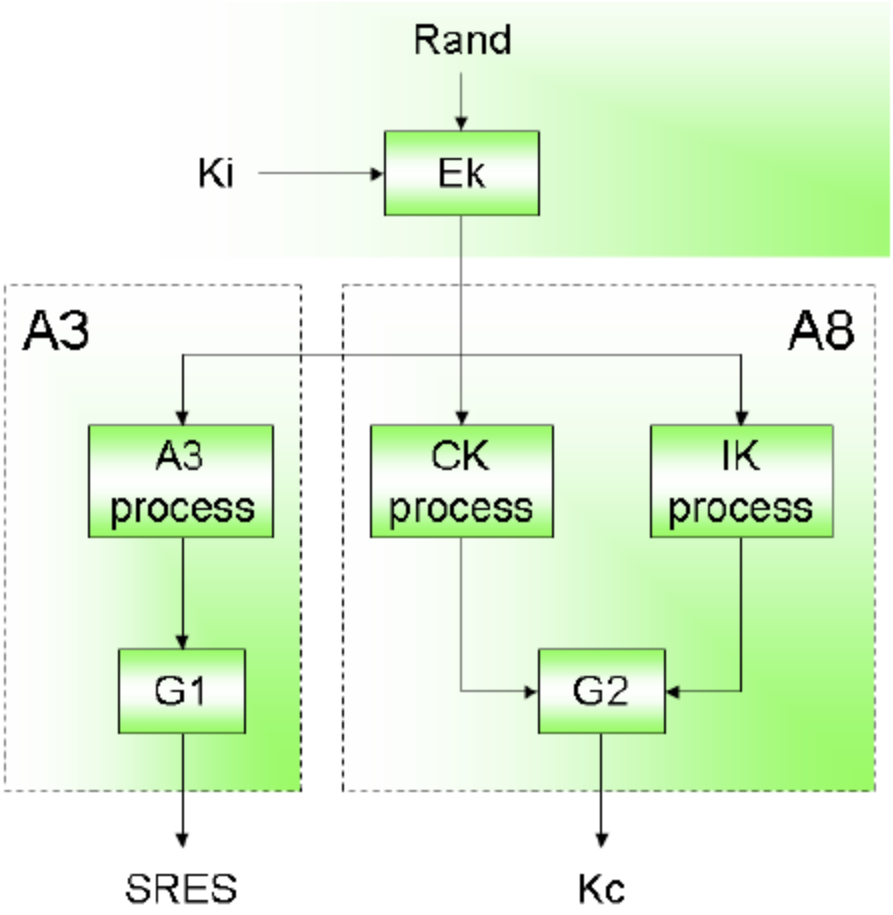
Struktura GSM sítě s GPRS



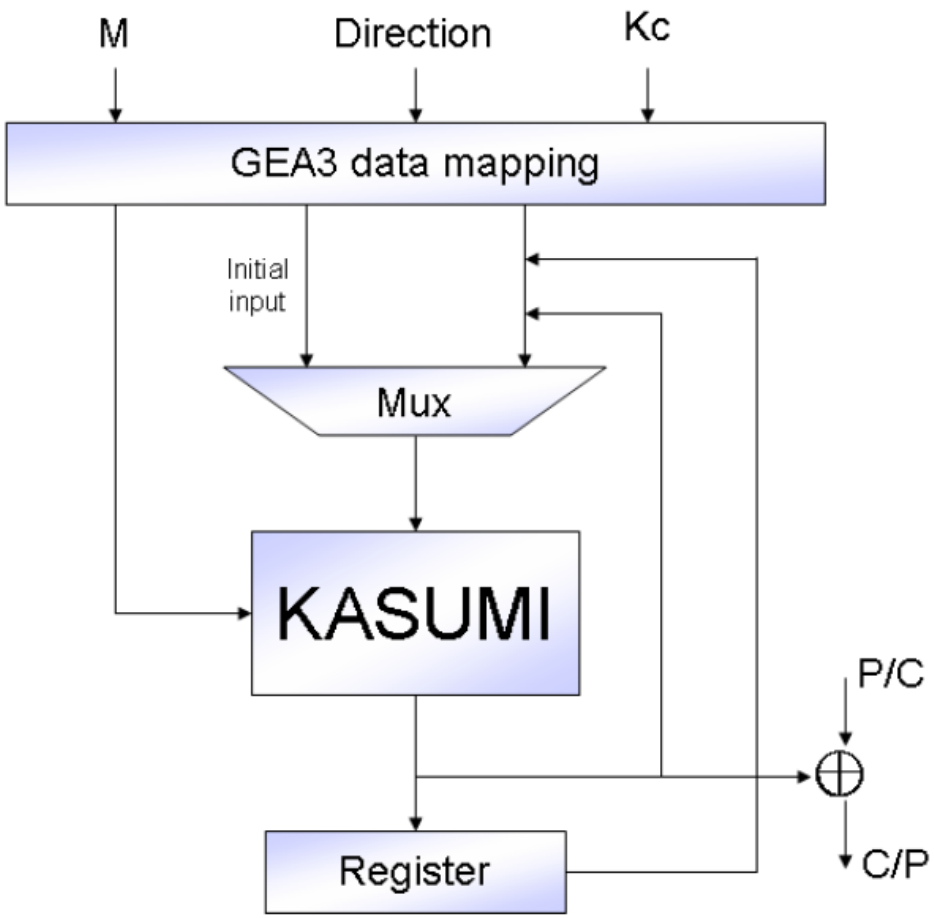
Rozdíly v zabezpečení GSM a GPRS/EDGE

- GPRS – General Packet Radio Service
  - podporuje přenos s přepínáním paketů (PS)
  - hlasové hovory probíhají s přepínáním okruhů (CS) stejně jako v GSM
  - GPRS data mohou využívat více time slotů najednou
- Šifrování na rádiovém rozhraní
  - nový algoritmus – GEA3 (bloková šifra KASUMI v OFB režimu)
  - vytvořen v ETSI
  - doposud tajný
  - GPRS provoz je šifrován až do SGSN, protože BTS nemůže pracovat s provozem využívajícím více TS (time-slot)
- Autentizace
  - liší se od autentizace v GSM (A3/A8) – založeno na Rijndael
  - místo AuC figuruje SGSN
  - oddělená autentizace pro CS (circuit-switch) a PS (packet-switch) provoz

Implementace A3 a A8 v GPRS

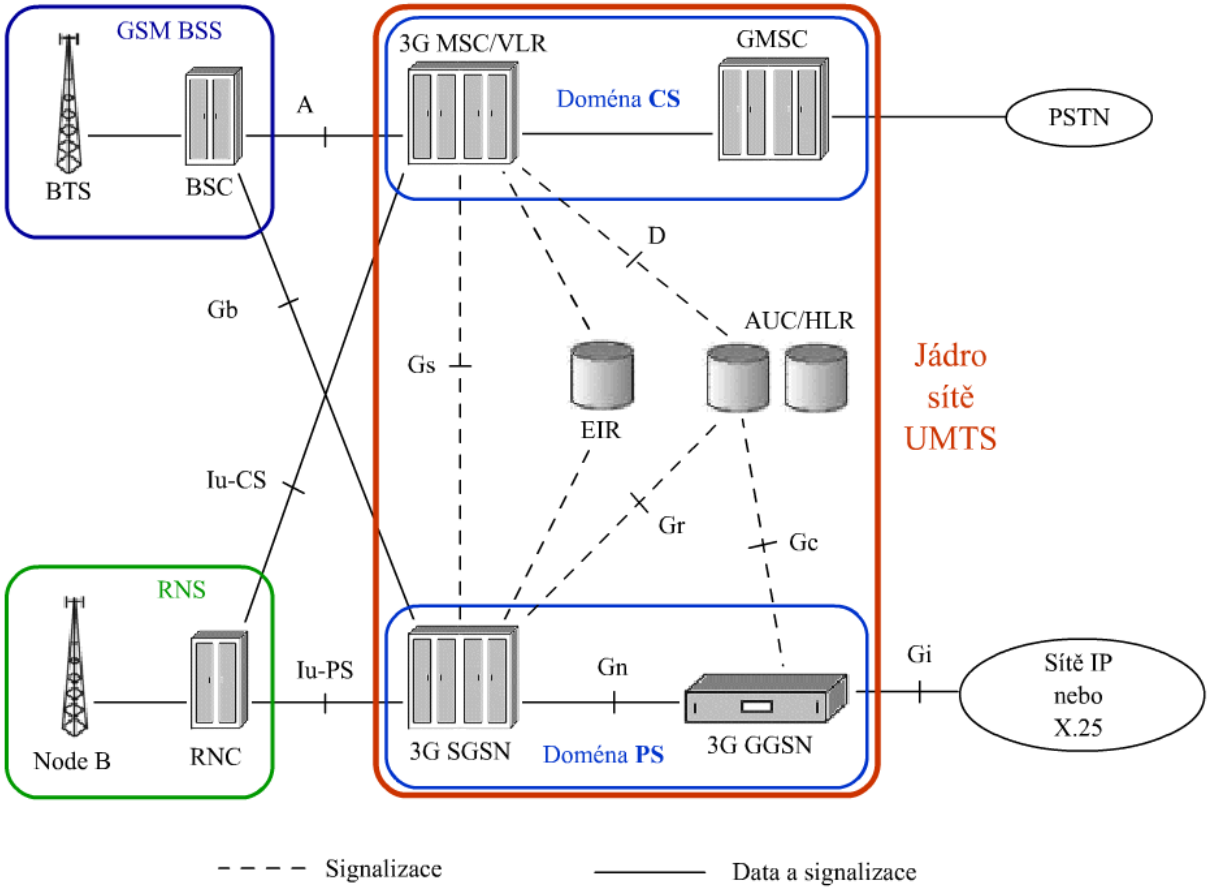


Implementace GEA3



UMTS

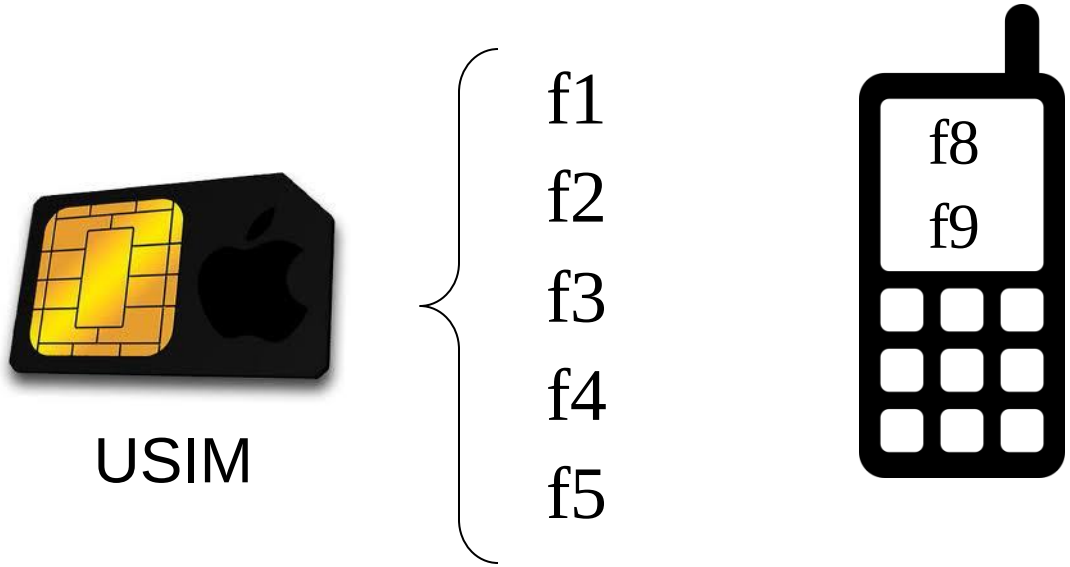
Struktura sítě UMTS



Zabezpečení UMTS vs. GSM

- UMTS vznikl jako otevřený standard
- 3GPP (3rd Generation Partnership Project)
  - http://www.3gpp.org
- 3GPP TS 33.102 - 3G Security - Security Architecture
  - UMTS sítě vznikají a existují vedle stávajících GSM sítí → bezpečnostní model vychází z bezpečnostního modelu GSM

Šifrovací algoritmy v UMTS



Karta USIM obsahuje ještě tajný klíč K, který je uložen i v AuC.

3G – šifrovací algoritmy

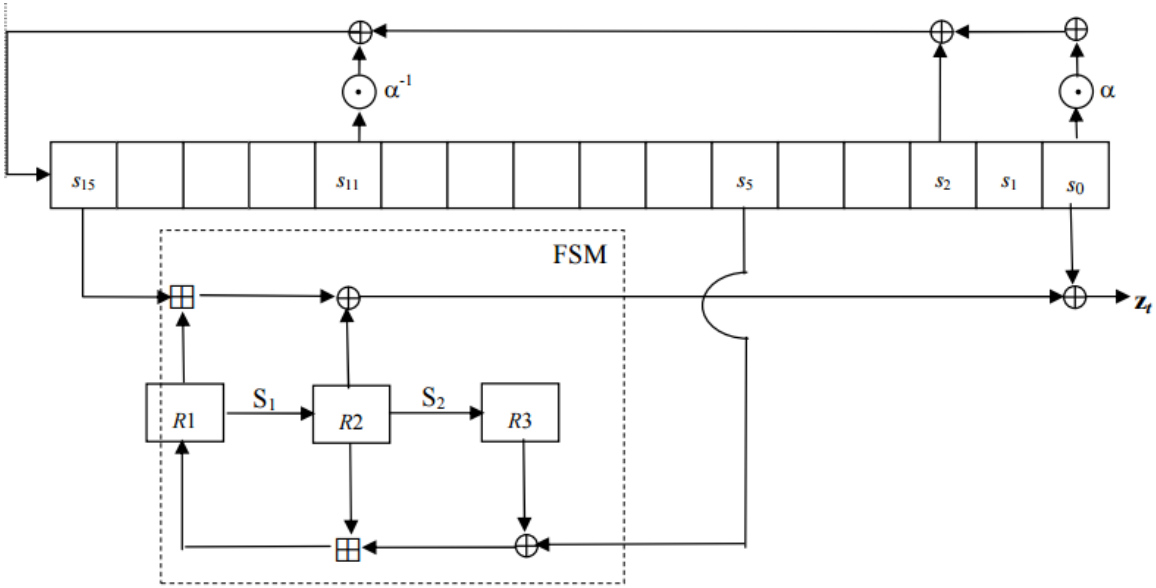
- KASUMI
  - UEA1 – UMTS encryption algorithm 1
  - UIA1 – UMTS integrity algorithm 1
- SNOW 3G
  - UEA2 – UMTS encryption algorithm 2
  - UIA2 – UMTS integrity algorithm 2

3G – šifrovací algoritmy - KASUMI

- bloková šifra pro f8, f9
- délka bloku 64 bitů
- délka klíče 128 bitů
- 8 rund
- publikoval M.Matsui (Mitsubishi) v roce 1996
- březen 2000
  - 3GPP přijalo KASUMI jako povinný algoritmus pro utajování a zajištění integrity dat pro W-CDMA sítě

3G – šifrovací algoritmy – SNOW 3G

- proudová šifra
- operace v GF(2^8)
- S_1 – založen na rundové funkci z Rijndaelu (SubBytes a MixColumn)
- S_2 – založen na Dicksonově polynomu $g_{49}(x)$
  ($g_{49}(x) = x \oplus x^9 \oplus x^{13} \oplus x^{15} \oplus x^{33} \oplus x^{41} \oplus x^{45} \oplus x^{47} \oplus x^{49}$) tak, že $S_2 = g_{49}(x) \oplus 0x25$
- Klíč – 128b
- IV – 128b



Algoritmy f1,f1*,f2,f3,f4, f5,f5*

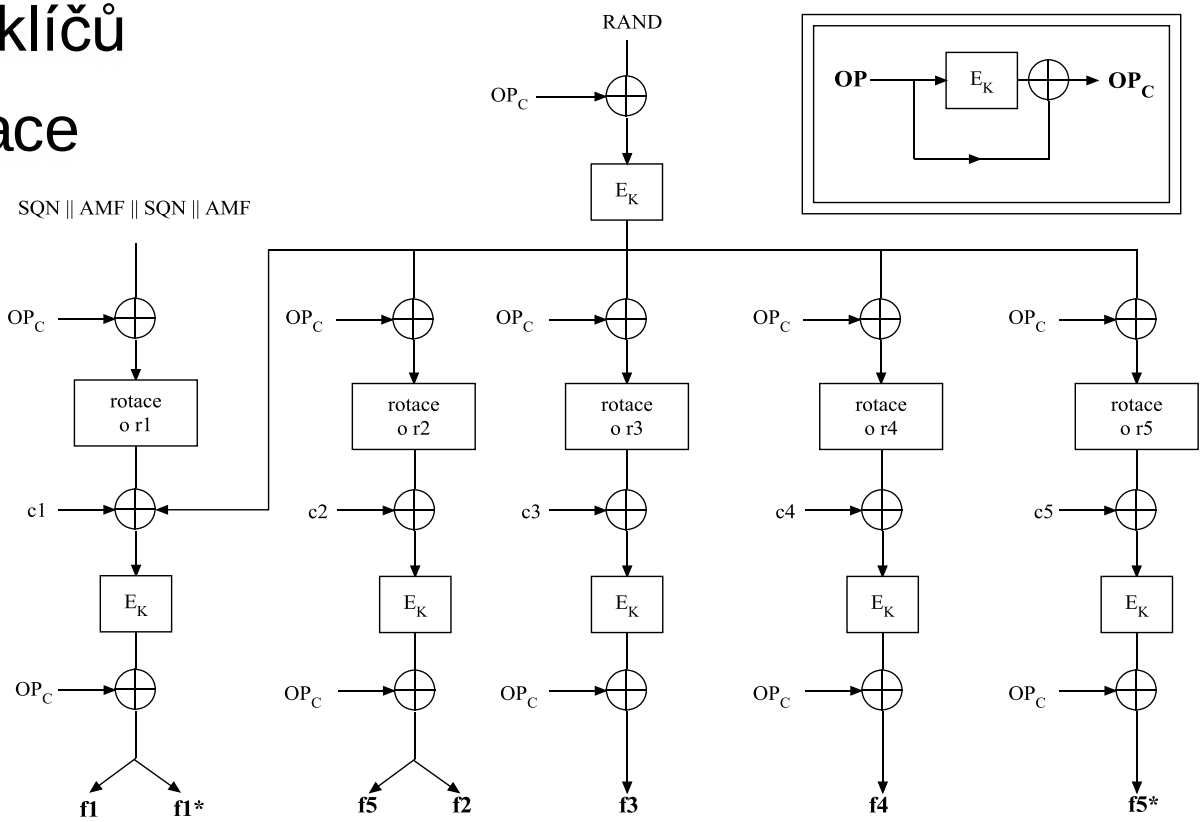
Souhrnně nazývány MILENAGE

f1,f2 – autentizace

f3,f4,f5 – generování klíčů

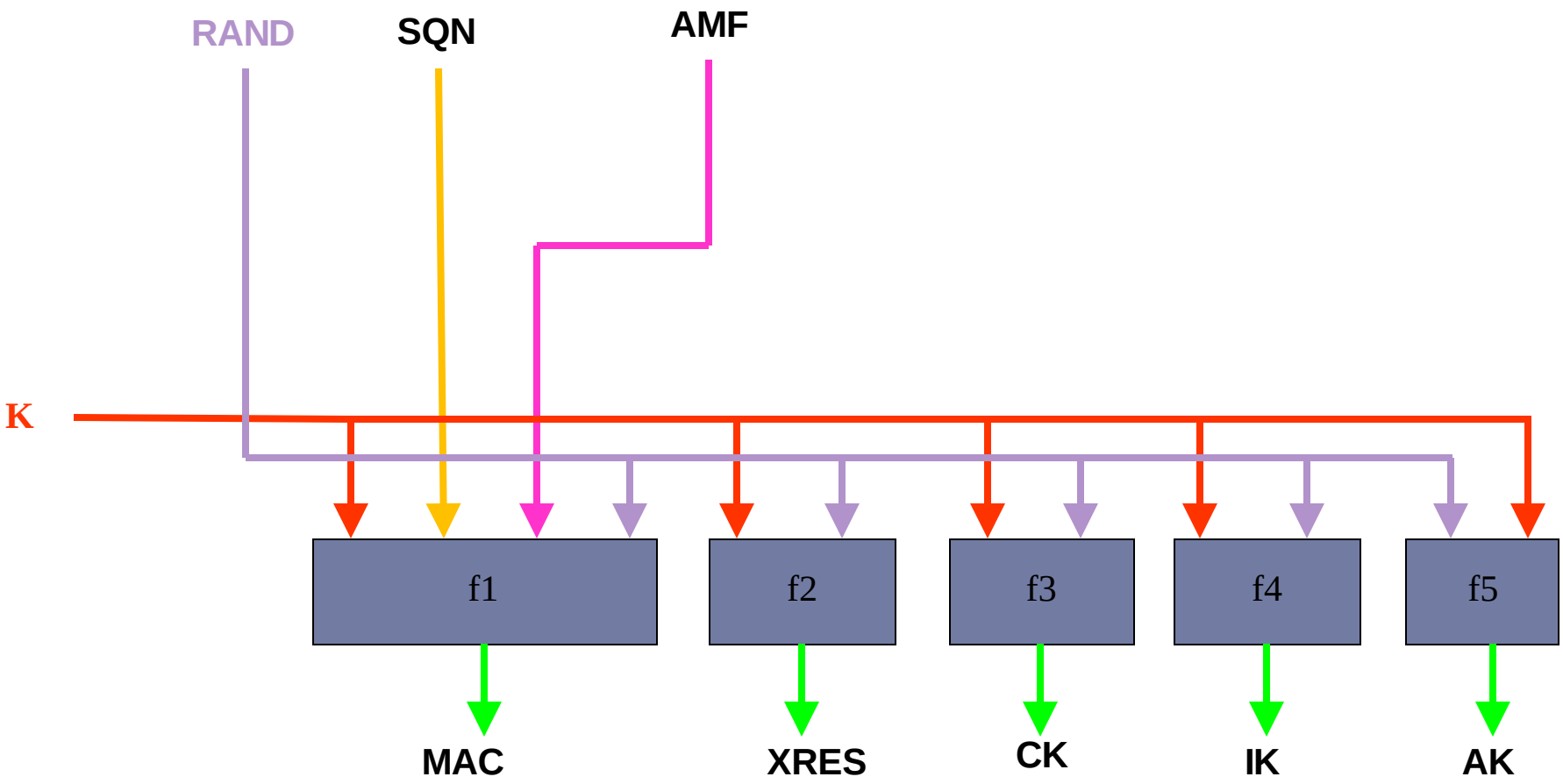
f1*,f5* - resynchronizace

základem je Rijndael



Šifrovací algoritmy v UMTS

Generování MAC a AUTN v AUC



Šifrovací algoritmy v UMTS - zkratky

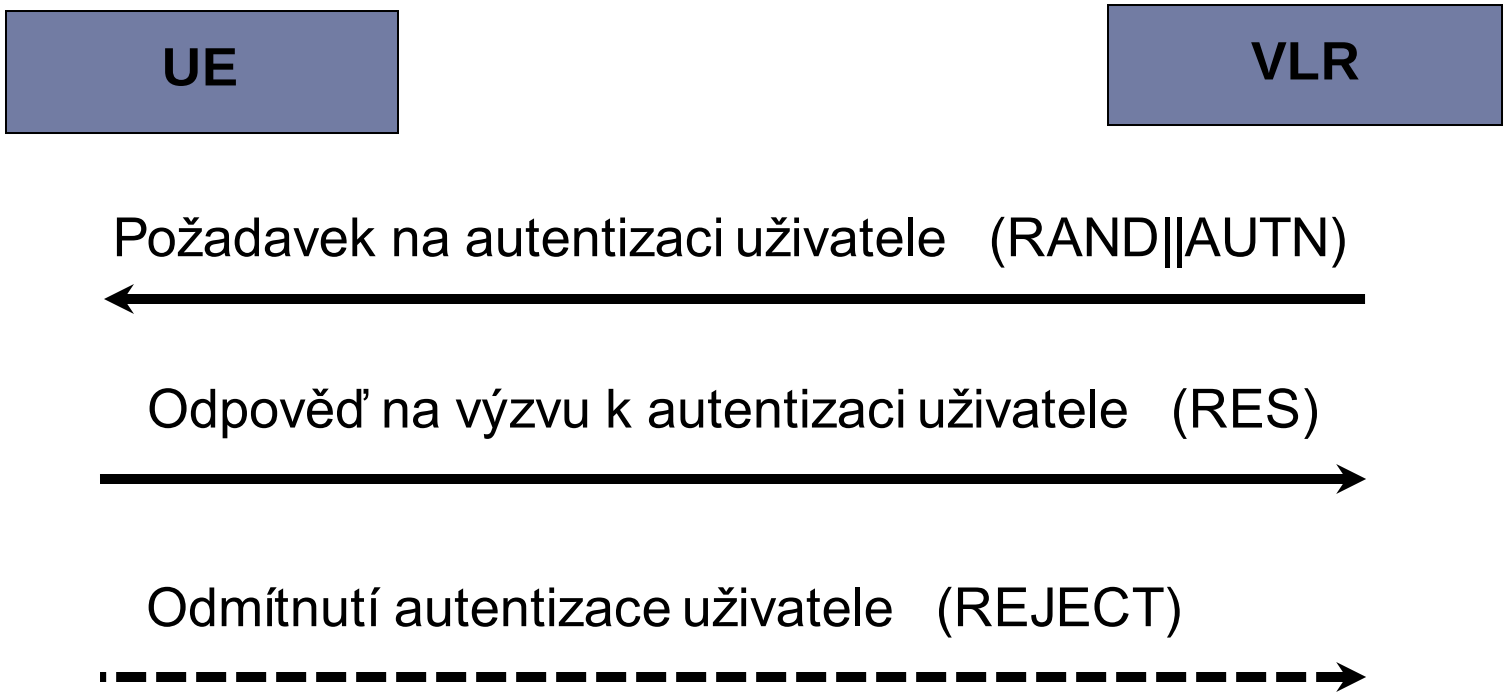
- RAND – Náhodná výzva
- SQN – Sekvenční číslo
- AMF – Authentication Management Field
  - součást autentizačního tokenu

- MAC – Message Authentication Code $MAC = f1(SQN||RAND||AMF)_K$
- XRES – Expected Response $XRES = f2(RAND)_K$
- CK – Cipher Key $CK = f3(RAND)_K$
- IK – Integrity Key $IK = f4(RAND)_K$
- AK – Anonymity Key $AK = f5(RAND)_K$
  - slouží k skrytí sekvenčního čísla

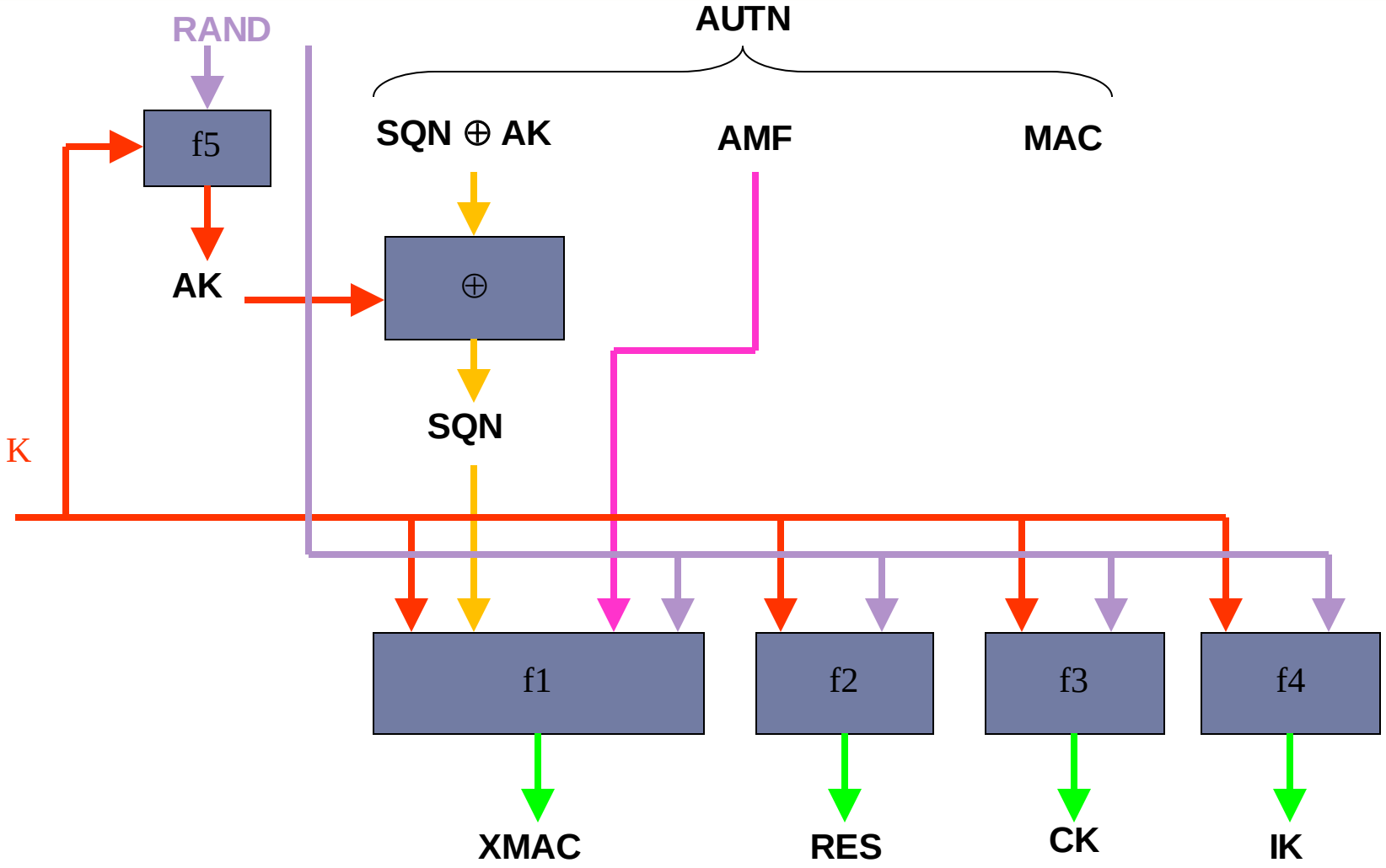
- AUTN – autentizační token $AUTN := SQN \oplus AK||AMF||MAC$

- AV – autentizační vektor $AV := RAND||XRES||CK||IK||AUTN$

Autentizace UE a výměna klíčů



Generování XMAC a AUTN v UE

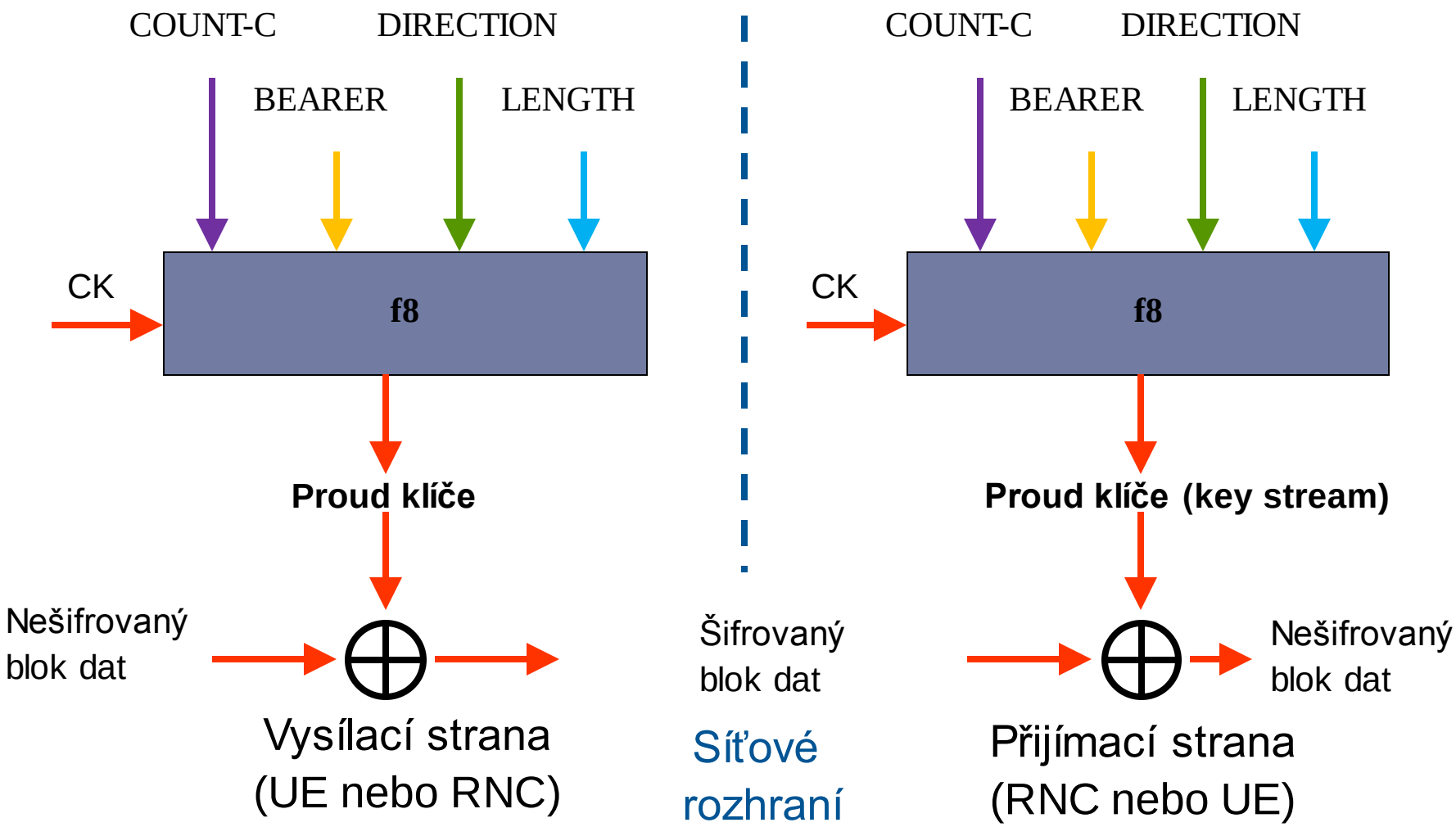


Dokončení autentizace UE a AUC

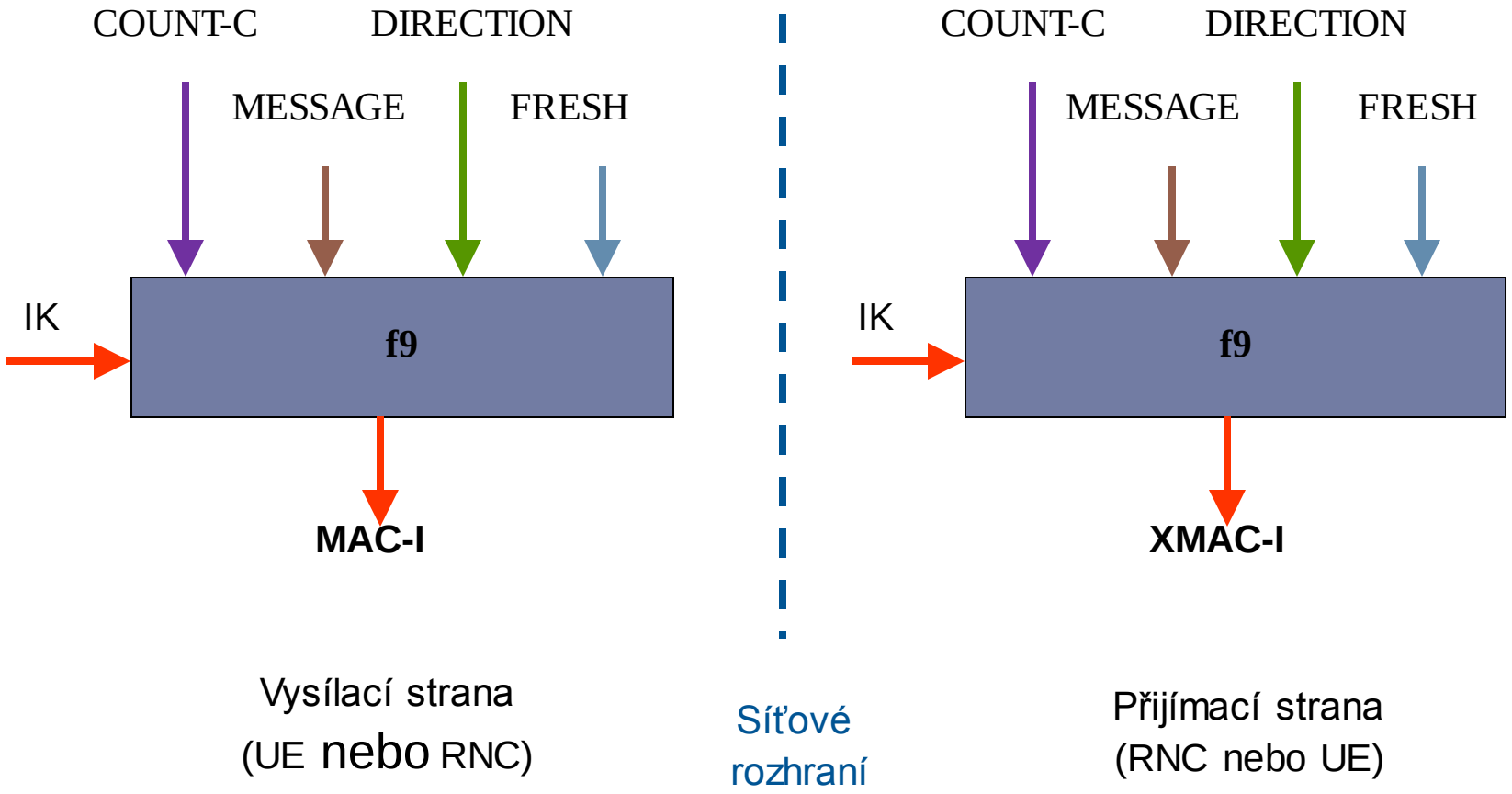
- $AK = f5(RAND)_K$
- $SQN = (SQN \oplus AK) \oplus AK$
- $XMAC = f1(SQN||RAND||AMF)_K$
  - porovnání přijatého MAC (z AUTN) a vygenerovaného XMAC
  - musí se rovnat, pokud ne -> REJECT

- Ověření zda SQN je ve správném rozsahu
  - SQN > SQN_{MS}
  - SQN_{MS} - nejvyšší dříve přijaté akceptované SQN

Šifrovací algoritmy v UMTS – f8 (utajení)



Šifrovací algoritmy v UMTS – f9 (integrita)



UMTS - shrnutí

- autentizace stejná jako v GSM
  - vzájemná mezi sítí a mobilní stanicí
  - algoritmy f1,f2
  - Založená na tajném klíči K, uloženém pouze na USIM a v AUC v domácí síti

- srovnání GMS x UMTS
  - GSM autentizační triplet (RAND, SRES ,K_c)
  - UMTS kvintet (RAND, XRES, CK, IK, AUTN)
    - IK – klíč pro zajištění integrity
    - AUTN - autentizační token pro autentizaci sítě

UMTS - shrnutí

- anonymita – stejná jako v GSM
- šifrování – lepší než v GSM
  - lepší algoritmus, dostatečně dlouhé klíče
  - hlas šifrován pouze mezi UE a NodeB
  - data šifrována mezi NodeB a 3G SGSN
  - algoritmy f8,f9
- integrita – lepší než v GSM
  - algoritmy f1

- kompatibilita UMTS a GSM
  - uživatelé GSM mají v sítích UMTS zabezpečení na úrovni GSM

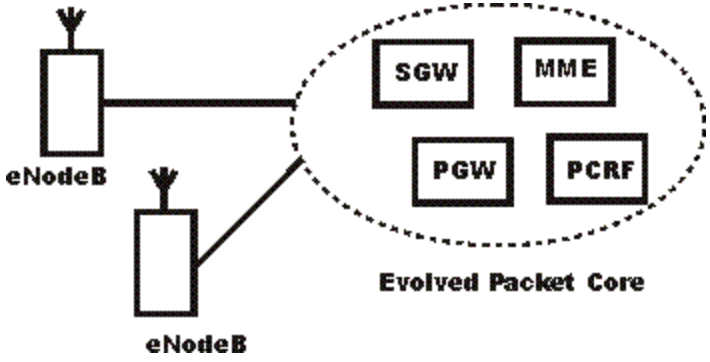
LTE / LTE-A

LTE – Long Term Evolution

- 3GPP
- nízká latence
- vysoká přenosová rychlost - x*10 Mbit/s
- OFDMA, SC-FDMA
- Přenosová pásma používaná v ČR
  - FDD
    - LTE band 1 – 2100MHz – Vodafone
    - LTE band 3 – 1800MHz – Vodafone, O_2, T-M
    - LTE band 7 – 2600MHz – Vodafone, O_2, T-M
    - LTE band 8 – 900MHz – Vodafone
    - LTE band 20 – 800MHz – Vodafone,T-M, O_2
  - TDD
    - především Asie

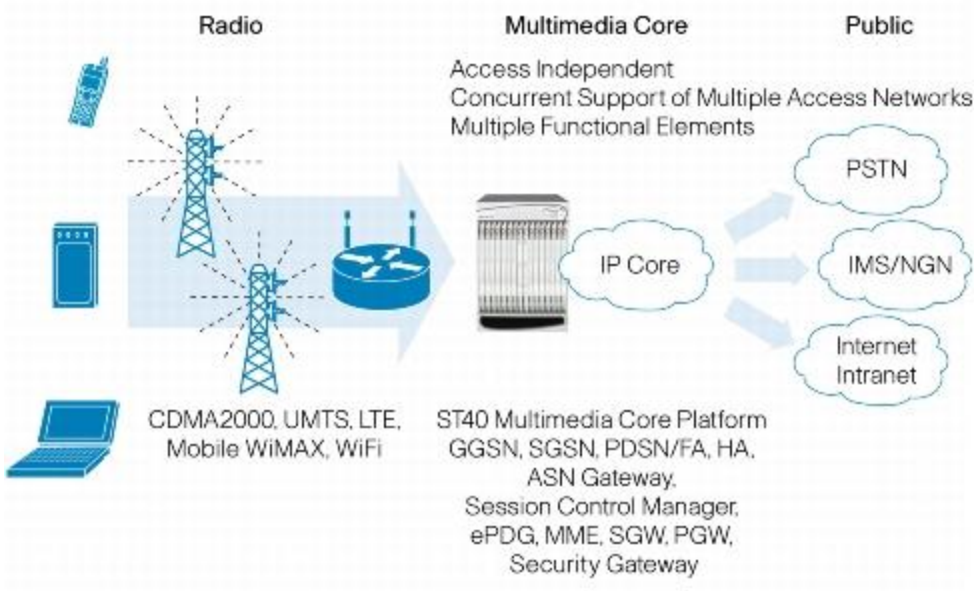
LTE – Long Term Evolution

- EPC – Evolved Packet Core
  - souhrnné označení pro jádro sítě
- eNB – Evolved NodeB
  - základnová stanice v LTE
- SGW – Serving Gateway
  - prvek oddělující
- PGW – Packet Gateway
  - Brána do dalších IP sítí
- MME – Mobility Management Entity
  - řízení přístupové sítě a UE, poskytuje dočasné identity UE, řeší intra-LTE handover
- PCRF – Policy and Charging Rules Function
  - dynamické řízení toků, podklady pro účtování



LTE – Long Term Evolution

- HeNB – Home eNB
  - eNB pro femto buňky
- SeGW – Security Gateway
  - součást SGW
  - odděluje HeNB od zbytku sítě
  - terminace IPsec tunelů



Cisco ASR 5000

LTE - zabezpečení

- velmi podobné UMTS
- stejná autentizace
- jiný šifrovací algoritmus
- neexistence end-to-end security, pouze mezi UE a sítí
  - pro zajištění E2E bezpečnosti nutné použít protokoly vyšších vrstev – TLS, SSH, IPsec, OpenVPN
- signalizace je částečně chráněna v EPC
  - protokol DIAMETER – podporuje zabezpečení

4G – šifrovací algoritmy

- SNOW 3G
  - EEA1 – EPS Encryption Algorithm 1
  - EIA1 – EPS Integrity Algorithm 1
  - identické s UEA2 reps. UIA2
- ZUC
  - EEA3 – EPS Encryption Algorithm 3
  - EIA3 – EPS Integrity Algorithm 3
    - ZUC – proudová šifra

EPS = Evolved Packet System

Dotazy

- Building fake (rogue) base station
  - Cost estimate 10 000 euros
  - Can capture IMSI
  - Gathered information might be used in networks with more loose authentication
  - Counter: Temporary identifier TMSI, changed when subscriber location updated
    - TMSI not entirely prevents IMSI capture since IMSI has to be sent once
  - Also other attacks (e.g. mentioned SIM –cloning)

- Cell change in GSM network

1. Phone sends audibility reports to BTS
2. BTS adds own information and sends to BSC
3. BSC cell change request to MSC (if necessary)
4. MSC resource allocation request to new BSC, that waits for MS to arrive
5. New BSC send acknowledgement to MSC that sends cell change command to old BSC, this forwards it to MS
6. MS breaks connection to old base station and continues with new one

How to hook up a phone to my fake base station?

- Item 5: Cell change command from the network -> Attacker may simulate command and force the phone to change
  - No authentication for base stations -> Device can not know communicating with a rogue base station