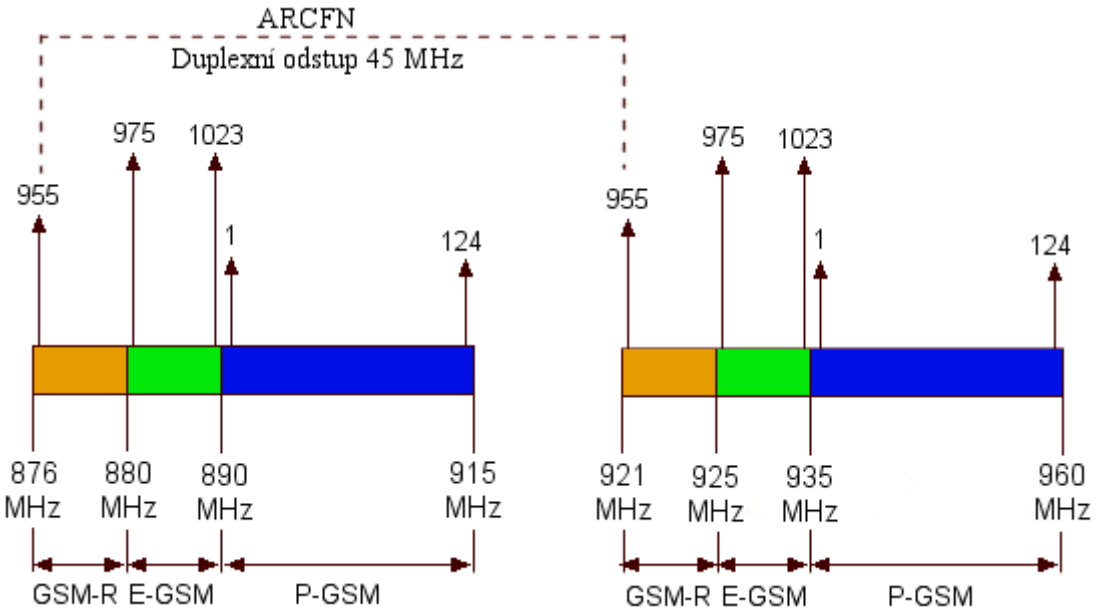
Stručně o GSM

Technické parametry systému GSM určeného pro provoz mobilních telefonů jsou závazně určeny souborem norem GSM, který v roce 1989 vypracoval Evropský telekomunikační standardizační úřad (ETSI, *European Telecommunication Standard Institute*) jako mezinárodně akceptovatelný digitální telefonní standard.

Jde o digitální celulární(buňkový) systém, využívající časového multiplexu (TDMA) a frekvenčního multiplexu (FDMA). Systém využívá sdílení kanálů v pásmech určených jak pro vysílání od mobilní stanice MS směrem k základnové stanici BTS (**tzv. uplink**)používá se pásmo 890-915 MHz, tak v pásmu určeném pro distribuci signálu od základnové stanice směrem k účastníkům (**tzv. downlink**), používá se pásmo 935-960 MHz.

V pásmu GSM 900 MHz se využívá pro downlink 125 kanálů (každý o šířce 200 kHz), v pásmu DCS (GSM) 1800 MHz je 374 kanálů šířky 200 kHz. Kmitočty, na kterých vysílá BTS a mobilní stanice, jsou svázány *duplexním odstupem* (45 MHz pro pásmo 900 MHz, 95 MHz pro 1800 MHz). To znamená, že mobilní stanice vysílá vždy na kmitočtu o 45 MHz resp. 95 MHz nižším, než vysílá BTS.

Dále vznikla novější varianta GSM, označená **E-GSM (Extended-GSM)**, kde je rozšířeno frekvenční pásmo standardní P-GSM (Primary-GSM) na 880-915/925-960 MHz (ARFCN jako u P-GSM a navíc 975-1023) a zmínit je třeba i variantu **GSM-R (Railway GSM)**, kterou odsouhlasili provozovatelé železnic jako jednotný komunikační systém pro použití v železniční dopravě. Pro tuto službu ETSI vymezila pásmo 876-880/921-925 MHz (odpovídá ARCFN 955-974).



Základnová stanice BTS může kdykoliv změnit číslo kanálu (frekvenci), na kterém se uskutečňuje spojení. Každý z těchto kanálů může obsloužit až 8 účastníků s využitím časového sdílení TDMA(časový multiplex). V poslední době se zavádějí technologie umožňující rychlejší přenos dat s využitím většího počtu logických kanálů pro jediného účastníka (síť GPRS, *General Packet Radio Service*, určená pro přenos datových paketů, a síť HSCSD, *High Speed Circuit Switched Data,* určená přednostně pro rychlý přenos dat). Tyto technologie souvisejí s další vývojovou fází systému GSM, zvanou GSM Phase 2+ a s postupným přechodem na připravovanou třetí generaci mobilní komunikace, totiž UMTS (*Universal Mobile Telecomunications System).*

Vliv časového sdílení (TDMA) na úroveň signálu

Časové sdílení kanálu GSM znamená, že každý účastník vysílá signál pouze po krátký časový úsek, tzv. *timeslot,* čemuž odpovídá průběh signálu označovaný jako *burst.* Tento timeslot má časovou délku 577 μs a je součástí delšího úseku, zvaného *rámec* čili *frame*, trvajícího osminásobek timeslotu, tedy 4,615 ms. Znamená to, že každému účastníkovi je vyhrazen jeden úsek (timeslot) z celého rámce. Jestliže je základnová stanice plně zatížena a obsluhuje tedy právě všech 8 účastníků na každém kanálu (režim *Full Rate*), je z výstupu kontejneru s technologií GSM dodáván do antény maximální výkon (tento výkon lze však dálkově regulovat s ohledem na nastavení optimálních provozních podmínek). Tato situace je však pouze hypotetická. Sousední buňky totiž dokážou odlehčit provoz na přetížené buňce tím, že část účastníků převezmou na sebe (Hannover). Pokud se počet účastníků zmenší, úměrně tomu se zmenší i výkon dodávaný do antény, popř. se daný kanál vypne.

Pozn. 1: Počet účastníků se může zvětšit na 16 (Informace NRL č.4/2000) v případě, kdy se použije pro přenos pouze každý druhý timeslot (režim Half Rate). Tím dojde ke snížení bitové rychlosti, což nepatrně sníží kvalitu hovorového signálu. Režim Half Rate vyžaduje jednak podporu ze strany mobilního telefonu a jednak podporu ze strany sítě. Operátoři v ČR prozatím podporu Half Rate nepřipravují. Naopak některé technologie využívají současně více timeslotů, čímž lze zvýšit bitovou rychlost (výše zmíněné technologie GPRS a HSCSD).

Pozn. 2: Délka rámce 4,615 ms odpovídá frekvenci 217 Hz. To je kmitočet, který se při přihlašování mobilní stanice do sítě GSM někdy indukuje v nízkofrekvenčních obvodech rádiových přijímačů, nízkofrekvenčních zesilovačů, telefonních přístrojů apod. Výsledkem je přerušované „vrčení" a praskání v reproduktoru či ve sluchátku. Tento jev se někdy projevuje na okamžik i u počítačových monitorů posuvem nebo deformací obrazu.

Jediný kanál, který *vysílá stále*, je tzv. nultý kanál. Na něm je distribuován signalizační timeslot, který komunikuje se všemi telefony najednou a zajišťuje např. sestavení hovoru nebo přenos textových zpráv. Provozní zatížení dané základnové stanice nelze zjišťovat pouze v kmitočtové oblasti, nýbrž je nutné je posuzovat i v časové oblasti. Takové měření lze částečně zajistit speciálním osciloskopem. Jde však o okamžitý údaj, který se může změnit mnohokrát za sekundu. Na spektrálním analyzátoru se jev projevuje jako "poskakující spektrální čáry".

Dálková regulace výkonu

Norma GSM 05.05 předepisuje možnost dálkové regulace výkonu koncových stupňů kontejnerů GSM síťovým operátorem *(Power Control)*, a to minimálně v šesti krocích po 2 dB, celkem tedy může operátor změnit výstupní výkon o 12 dB, tedy zhruba 16 krát, může ho však pouze *snížit*. Pokud tedy bude instalovaný výkon na kanál např. 4 W, může za určitých okolností operátor snížit tento výkon na 4/16 W = 250 mW. Řídící jednotka základnové stanice (BSC, *Base Station Controller*) může dále snižovat výstupní výkon až v patnácti krocích po 2 dB, čili celkem o 30 dB (tedy tisíckrát). Pokud bychom v takové situaci měřili intenzitu elektromagnetického pole u antény, naměřili bychom o několik řádů nižší výkon než maximální možný. Maximální instalovaný výkon vysokofrekvenčních koncových modulů je dán technickými parametry modulu a v žádném případě ho nelze překročit.

Důvodem regulace vyzařovaného výkonu jak u BTS, tak u mobilních stanic je mimo jiné potřeba zamezit vzájemným interferencím mezi jednotlivými kanály, které jsou častou příčinou poruch mobilního spojení zejména v hustě osídlených aglomeracích. Operátoři se proto snaží nastavit optimálně jak frekvence kanálů mezi jednotlivými BTS, tak i jejich výkon.

Obdobný způsob regulace funguje i u *mobilních telefonů*. Maximální výkon je zde regulován ve 14 krocích od 1 mW (1800 MHz) resp. 3,2 mW (900 MHz) do 1 W resp. 2 W. V praxi se však maximálních výkonů uvedených v normě GSM 05.05 vůbec nedosahuje. Pro pásmo 900 MHz je maximální okamžitý výkon, přiváděný na anténu mobilní stanice, typicky 0,6 W a méně. To znamená, že *střední výkon* vyzařovaný z antény mobilní stanice je *nižší než 0,1 W* . V městských zástavbách a v místech mikrobuněk stačí zpravidla pro provoz stanice minimální nastavená výkonová úroveň (řádově miliwatty).

Význam některých zkratek v GSM

BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
DTX	Discontinuous Transmission
ETSI	European Telecommunication Standard Institute
FDMA	Frequency Division Multiple Access
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HSCSD	High Speed Circuit Switched Data
MS	Mobile Station
SMS	Short Message Service
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunications System

Megapixel

Počet bodů, které zvládne fotmobil vyfotit, se udává v megapixelech. Počet megapixelů snadno zjistíte tak, že vynásobíte obě hodnoty rozlišení fotoaparátu a vydělíte milionem. Např. fotomobil, který vytváří snímky s rozlišením 640 × 480 bodů má 0,3072 Mpx. Současný standard je 5 Mpx, lepší fotomobily mají klidně i 12 Mpx.

Jack

Konektor pro připojení sluchátek. Určitě ho najdete na svém počítači nebo MP3 přehrávači. Někteří výrobci mobilů bohužel používají jiný konektor, aby vás donutili používat sluchátka vlastní výroby.

Ekvalizér

Nastavení hudebního přehrávače, které určuje, jak mají být zvýrazněné jednotlivé složky hudby (např. basy nebo výšky).

POP3

Protokol pro stahování e-mailů.

GPRS

Typ datových přenosů v mobilních telefonech. Jedná se o téměř nejstarší technologii, proto je pomalá. Zato ale GPRS můžete používat prakticky všude, kde je mobilní signál.

EDGE

Typ datových přenosů v mobilních telefonech. Jedná se o vylepšené GPRS, takže je podstatně rychlejší. Bohužel EDGE nenajdete všude, naši operátoři pokrývají především velká města.

UMTS

Nazývané též sítě třetí generace (3G). Umožňují videohovory a rychlé datové přenosy. Pokrytí signálem je spíše symbolické, v Česku pouze u operátora O2 v Praze a Brně.

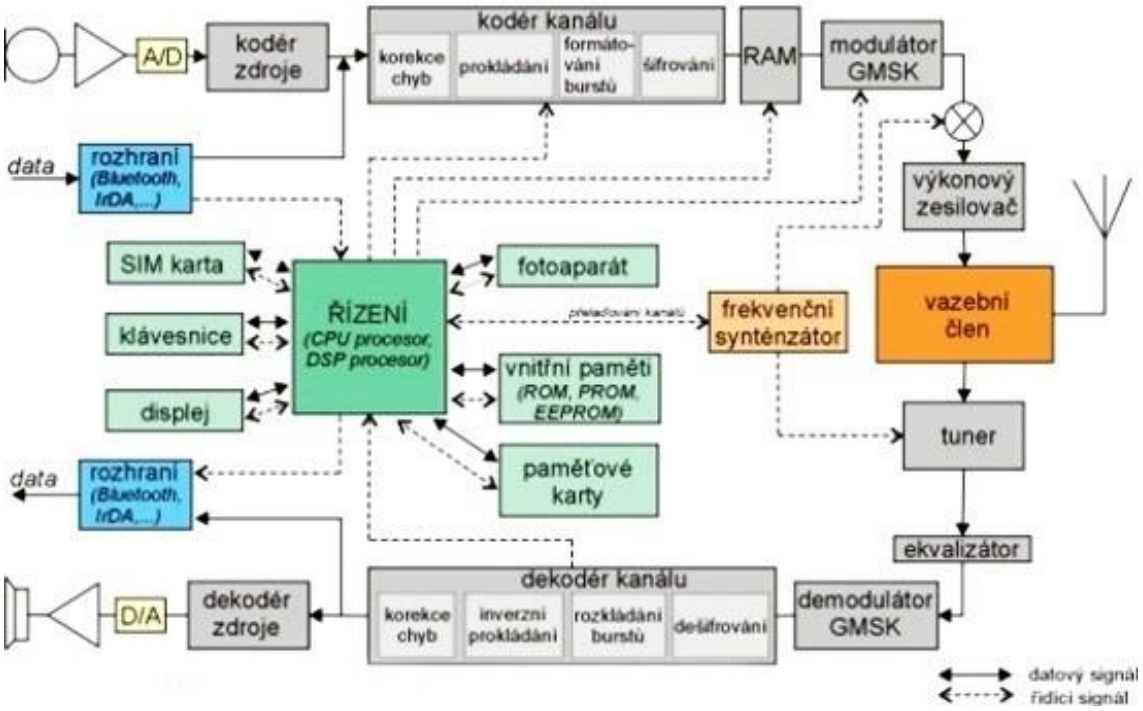
HSDPA

Zrychlená verze UMTS umožňuje stahovat data rychlostmi v řádu megabitů za sekundu.

Mobilní telefon GSM

Mobilní telefon je běžnou součástí života. Rozmach a dostupnost mobilních telefonů nastal zavedením 2. generace mobilních sítí GSM (Global systém for Mobile) v r. 1993. V současné době v České republice výrazně převyšuje počet mobilních telefonů počet obyvatel. Podle prodaných aktivních karet SIM se předpokládá asi 13 milionů mobilních telefonů a uživatelů služeb mobilních operátorů (T-Mobile, O2, Vodafone).

Blokové schéma mobilního telefonu GSM



Popis funkce mobilního telefonu podle blokového schématu

Bloky mobilního telefonu:

Vysílací a přijímací VF část
- A/D převodník
- kodér zdroje
- kodér kanálu
- modulátor
- výkonový zesilovač
- vazební člen
- anténa
- dekodéry

Vstupní – výstupní rozhraní

- klávesnice
- displej
- sluchátko
- mikrofon
- bluetooth
- paměťové karty

Řízení a paměti

- mikroprocesor
- řídící signály
- paměti RAM a EEPROM
- operační systém

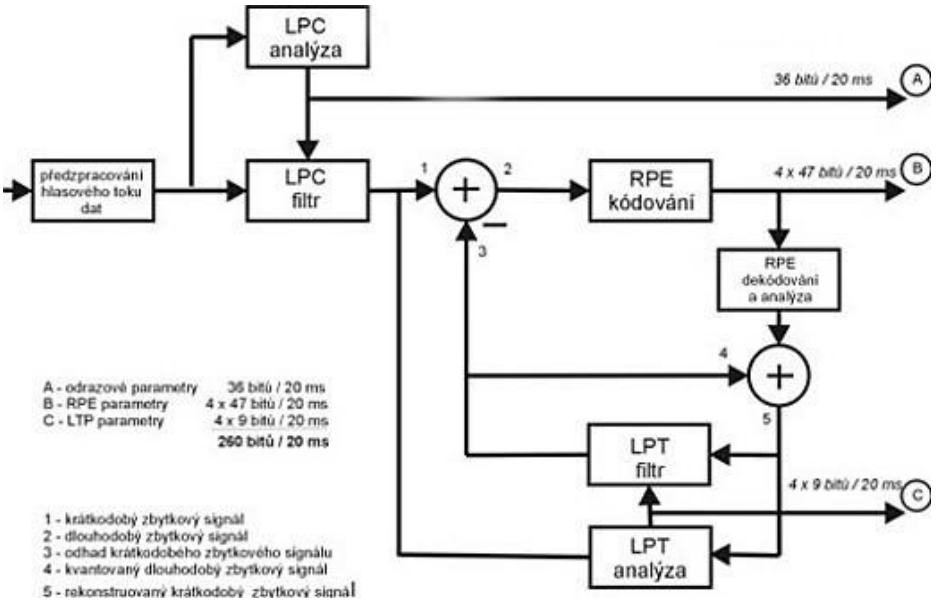
Napájení
- baterie
- externí zdroj

SIM karta (identifikační modul účastníka)

Popis základních bloků:

- A/D převodník
Lidský hlas je pomocí mikrofonu a NF zesilovače převeden na elektrický analogový signál v pásmu 300 – 3400 Hz. Tento analogový signál se převede pomocí A/D převodníku na signál digitální. Převodník A/D je třináctibitový se vzorkovací frekvencí 8000 Hz. V telefonech GSM se 8000 vzorků/s rozdělí na 50 úseků po 20 ms. Z každého 20 ms úseku se získá 160 vzorků.
Do kodéru zdroje odchází datový tok o velikosti 104 kbit/s. Datový tok je dán vzorkovací frekvencí a počtem kvantizačních bitů (8000 Hz . 13bit = 104000 bit/s)

- kodér zdroje
Funkcí kodéru je zkoprimování (stlačovat, zhušťovat) 104000 bit/s datového toku na kapacitu přenosového kanálu o velikosti 13000 bit/s. Kodér odstraňuje redundanci (nadbytečnou a nepotřebnou část informace.



Typy kodeků užívaných v mobilních telefonech GSM:

- FR (GSM Full - Rate)

Z kodéru vystupuje každých 20 ms paket o velikosti 260 bitů. Do každého vstupuje zkomprimovaný datový tok o velikosti 13000 bit/s. (260bit/0,02 s = 13000 bit/s) Způsob kódování – kodek RPE – LPT(Regulatror Pulse Excitatio – Long Term Prediction) RPE pracuje s pravoúhlou excitací. Je to vlastně generátor s proměnlivou střídou. LPT provádí dlouhodobý odhad koeficientů filtrů, který spočívá ve využití korelací (vzájemná závislost) mezi sousedními periodami základního tónu hovorového signálu k predikaci hodnoty signálu v následující periodě.

- EFR (GSM Edhadhanced Full – Rate)

Z kodéru vystupuje paket o velikosti 260 bitů s datovým tokem 13 kbit/s. Využívá kodek ACELP (Algebraie – Code – Excited Linear Prediction) s využitím generátoru algebraického kódu.

- VAD (voice activity detection)

Kodek neprovádí kódování pokud uživatel nehovoří nebo neposlouchá

- Kodér kanálu:

Jeho úkolem je zabezpečit bezchybný přenos. Vkládá do signálu další bity, aby v případě poruchy bylo možno rekonstruovat signál. Blok kodéru vykonává funkce:

- korekci chyb
- prokládání
- šifrování

Korekce chyb:
Provádí rozdělení paketu o velikosti 260 bitů z kodéru zdroje do tří skupin podle velikosti:

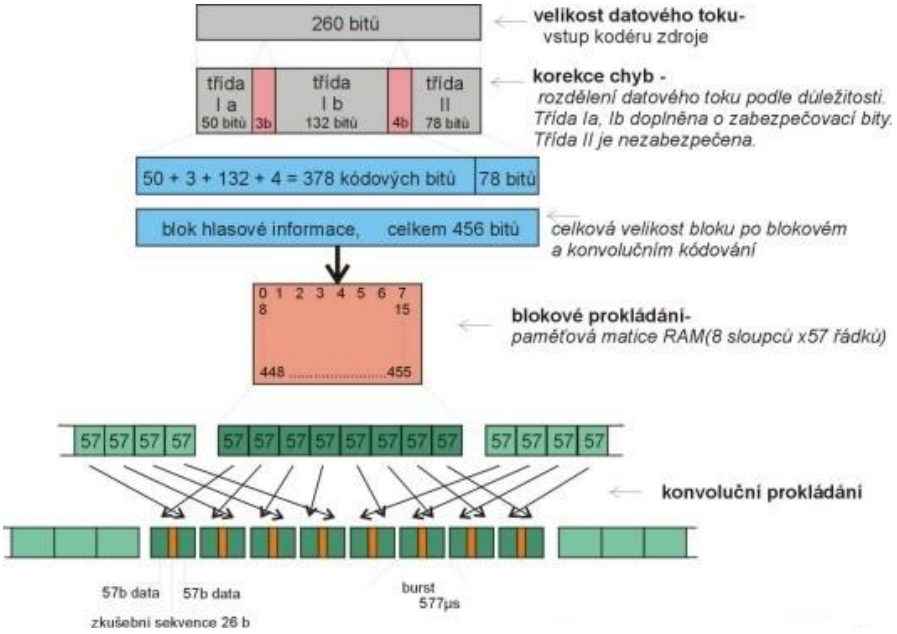
1. skupina – **1a** jedná se o prvních 50 nejvýznačnějších bitů, které jsou doplněny o 3 bity CRC (Cyclic redundacy cheek) kódu.

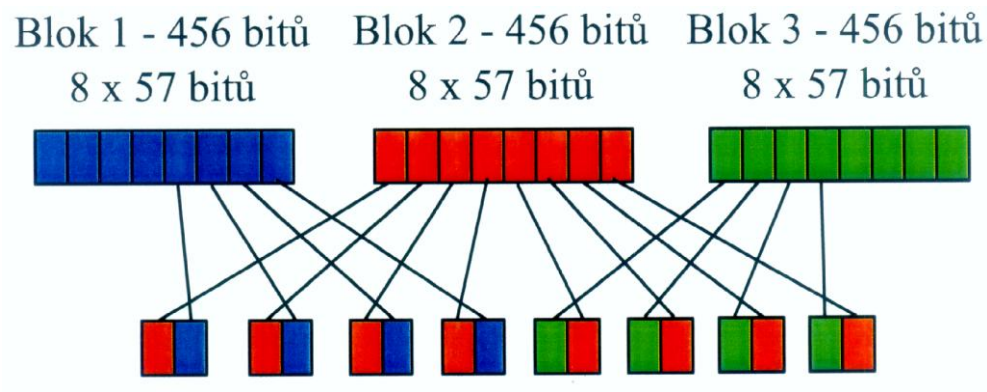
2. skupina –**1b** obsahuje 132 méně významných bitů. Je zabezpečena 4 bity CRC kódu. Skupiny **1a** a **1b** jsou přivedeny na vstup konvolučního kodéru s účinnosti 1. Je to poměr vstupního a výstupního signálu. Každý bit je kódován do dvou bitů podle určité kombinace.

3. skupina obsahuje 78 bitů, které jsou méně významné. Nejsou chráněny CRC konvolučním kódem. Paket se zvětší z 260 bitů na 456 (50 + 3 + 132 + 4) x 2 + 78 = 456 konvolučním kódováním je 13 kbit/s signál kodéru zdroje navýšen na 22,8 kbit/s

456 bitů /0,02 s = 22,8 kbit/s

Prokládání:
Blokové prokládání zapisuje 465 bitový datový tok do řádků a čte ze sloupců. Tím vznikne matice o á sloupcích a 57 řádcích, která se zapíše do paměti RAM.





- Šifrování

Pro zabránění odposlechu hovoru je každá informace šifrována. Po přihlášení mobilního telefonu do sitě GSM je vygenerován klíč o délce 64 bitů.Tento klíč s číslem TDMA tvoří vstup pro algoritmus. Algoritmus vygeneruje pseudonáhodnou posloupnost. Na tuto posloupnost a na 114 bitové bursty(burst je základní jednotka v systému GSM jehož velikost je 156, 25 bitů s délkou trvání 0,577 s) jsou aplikovány operace XOR. Tím dojde k zašifrování přenášených dat.

- Modulátor

Moduluje užitečný signál na nosnou frekvenci v pásmech GSM (900 a 1800 Mhz). V systémech

GSM je používaná GMSK digitální modulace. *Jedná se o dvoustavovou modulaci pracující na principu klíčování frekvenčním posuvem*. Pokud na vstupu GMSK modulátoru dojde ke změně 0 na 1 dojde k posunutí nosné vlny. Modulátor zůstane na této nosné tak dlouho, dokud nedojde k další změně logické hodnoty. Blok modulátoru obsahuje směšovač a oscilátor.

Směšovač - modulovaný signál převede do VF pásma a příslušného kanálu.

Oscilátor - plní funkci frekvenčního syntetizátoru. Ten pro získání diverzity se 217 x za sekundu přeladí.

Pro pásmo GSM 900 je pracovní rozsah 890 – 900kHz

Pro směr downlink BTS – MS je rozsah 935 – 960 MHz

GSM 900 tvoří 2 x 124 fyzických kanálů s 200 kHz odstupem nosných frekvencí. Každý fyzický n kanál obsahuje 8 časových kanálů (timeslotů). Jeden timeslot přenáší jeden hovor. Odstup duplexních párů je 45 MHz. Mezera mezi pásmem pro uplink a downlink je 20 MHz.

- Výkonový zesilovač:

Maximální výkon v klasických ručních mobilních telefonech je 2 W. Minimální výkon je 20 mW. Sílu signálu a jeho kvalitu vyhodnocuje stanice BSC, která vyhodnocuje a určuje výkonové úrovně stanice BTS a mobilního telefonu, porovnáním poměru S/N.

- Vazební člen (anténní přepínač):

Zesílený signál z výkonového zesilovače je přiveden do vazebního členu, který přivádí signál na anténu, určenou pro vysílání i příjem.

- Anténa:

Je všesměrová pro vysílání a příjem signálu. Přijímá a vysílá signály GSM v pásmech 900, 1800, 1900 MHz.

Typy antén:

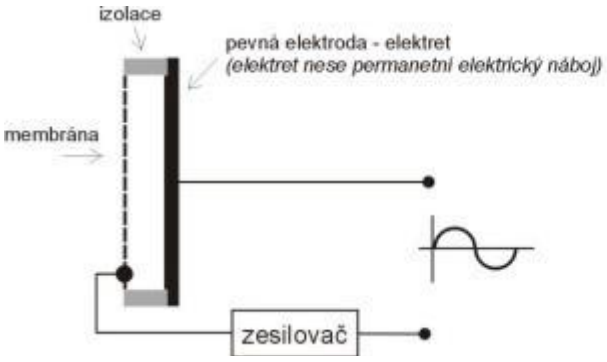
- prutové (monopólové) antény

- šroubovicové antény

- plošné antény

- Vstupní / výstupní rozhraní

Mikrofon – používá se elektretový mikrofon



Princip:- pohyb membrány v elektrickém poli
- V rytmu pohybu membrány se mění kapacita kondenzátoru a tedy i elektrické napětí mezi deskami. Pro zesílení napěťových změn a napájení obsahuje mikrofon tranzistor FET.

- Sluchátko:

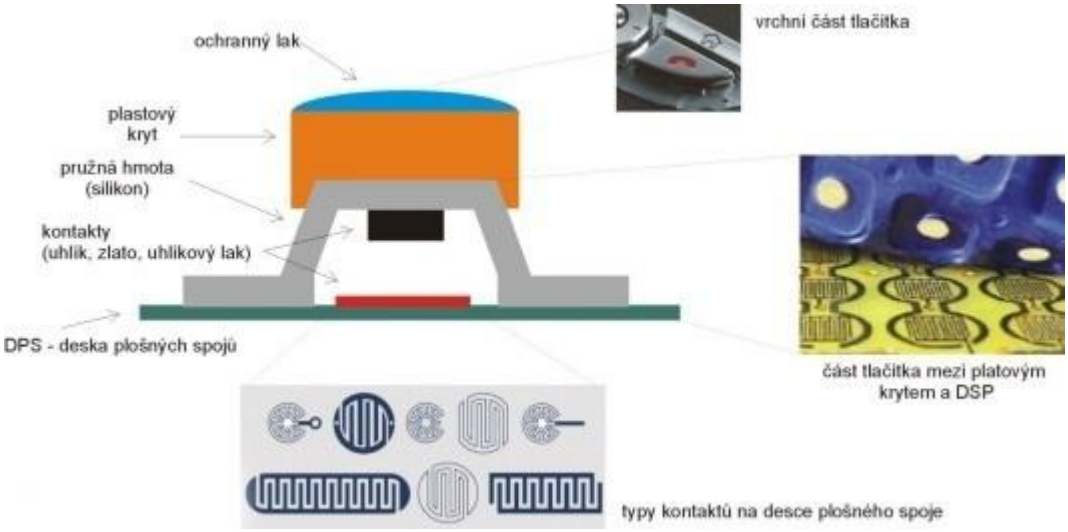
Je používán elektrodynamický princip, jehož základem je membrána, cívka a magnet. Cívkou protéká modulovaný proud a vzájemným působením magnetického pole cívky a permanentního magnetuje cívka vtahována (vytahována) ze vzduchové mezery a tím dochází k pohybu membrány.

- Displej:- Základem je LCD.
Princip – spočívá v polarizaci tekutých krystalů v elektrickém poli přivedeným napětím.Podle natočení krystalů světlo prochází nebo neprochází.
Používané displeje: TFT jsou to aktivní barevné displeje, kde každý pixel je tvořen třemi tranzistory. Pixely vyzařují základní červenou, zelenou a modrou barvu.

***- Klávesnice*:** - je vstupní zařízení složené z kláves.
Obsahuje:

- numerickou klávesnic(čísla písmena, znaky)
- kurzorová tlačítka (pohyb v menu telefonu)

V současné době se používají v mobilních telefonech pryžové klávesnice.



složení tlačítka klávesnice.

- Infraport: - je bezdrátové připojení mobilního telefonu k osobnímu počítači. Pro přenos se používá infračervéné světlo.

***- Bluetooth*:** - je bezdrátové připojení mezi mobilním telefonem a okolními zařízeními. Jedná se o rádiový přenos. Pracovní pásmo je 2,4 GHz.

- Paměťová karta: - rozšiřuje volnou paměť mobilního telefonu a slouží pro uložení a přenos dat.

Druhy paměťových karet:
a) SD b) mini SD c) mikro SD d) MMC e) MS f) xD

***- Řízení a paměti*:** - řízení je prováděno mikroprocesorem, který je řízen krystalem. Řídí a koordinuje okolní prvky typu n klávesnice, displej. Komunikuje se SIM kartou, paměťmi

EEPROM, RAM, SRAM, FLASH a řídí dodávku energie. Pracuje se všemi druhy signálů (řídící, datové, napájecí a analogové).

***- Akumulátor*:** - je obnovitelný zdroj energie.

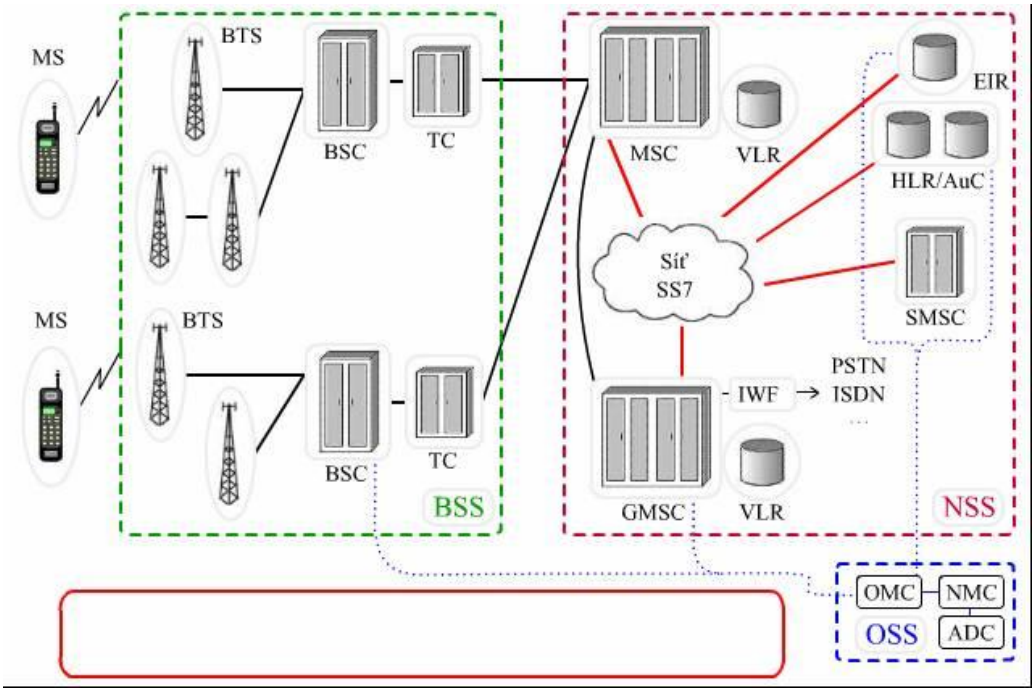
Používané akumulátory:

- Ni-Cd (nikl-kadmium)
- Ni-Mh (nikl-metalhydrit)
- Li-Ion (Lithium- Iontové)
- Li-pol (Lithium-Polymer)

***- SIM karta*:** - je vyměnitelná součást mobilního telefonu. Jedná se o čip na kterém jsou uloženy informace o uživateli a data potřebná pro provoz v síti GSM. Se stále zmenšující se elektronikou a stálou integrací součástek jsou mobilní telefony vybavovány jinými hardwarovými bloky. Většina mobilních telefonů je vybavena fotoaparátem nebo videokamerou, rádiovým přijímačem, MP3 … a tak tvoří multifunkční zařízení.

Základní struktura systému GSM

Na následujícím obrázku je ve formě tzv. síťového (blokového) schématu znázorněna celková struktura systému GSM. Zobrazený systém je rozdělen na tři subsystémy a jsou zde uvedeny i významy jednotlivých zkratek.



- **Mobilní uživatelské stanice - MS (Mobile Station)**

Mobilní telefon je v podstatě transciever (vysílač/přijímač) komunikující se základnovou stanicí BTS doplněný řídícími obvody (mikroprocesor) a vstupně/výstupními zařízeními (klávesnice, display, sluchátko, mikrofon, porty). Mobilní stanice je jednoznačně identifikována pomocí čísla **IMEI** (International Mobile Equipment Identity), uloženého v

její paměti. Sám účastník je identifikován pomocí **SIM** karty (Subscriber Identification Module).

Dle specifikací GSM se mobilní stanicí rozumí jednak vlastní mobilní zařízení (vysílač/přijímač), navíc také předplatitelský identifikační modul SIM (Subscriber Identification Module) - ten umožňuje unikátní identifikaci uživatele v rámci celé sítě GSM.

- **Mobilní zařízení (Mobile Equipment)** obsahuje rádiový přijímač/vysílač, pomocí kterého komunikuje se základnovými stanicemi. Mezi další bloky náleží předmodulační a podetekční obvody, mající na starost zdrojové a kanálové kódování, dále mikroprocesorové obvody a další pomocné bloky. Uživatel přichází do styku s klávesnicí, displejem, sluchátkem a mikrofonem. Pro některé účely, především komunikaci MS s dalším zařízením je nutné použít další rozhraní.
- **Karta SIM (Subscriber Identification Module)** je nutnou součástí mobilní stanice a ta je bez této karty nepoužitelná (s výjimkou tísňového volání 112). V obvodech této karty jsou uloženy specifické údaje o právoplatném majiteli karty, dále jeho čtyřmístné identifikační číslo PIN (Personal Identification Number) a neměnné identifikační číslo PUK (Personal Unblocking Key). Hlavním smyslem SIM karty je ověření a identifikace uživatele a služeb jemu přístupných. Karta je přenosná a lze ji použít s libovolným mobilním telefonem. SIM dále uchovává následující údaje :
  - IMSI (International Mobile Subscriber Identity)
  - Autentikační klíč (Ki)
  - Šifrovací klíč (Kc)
  - TMSI (Temporary Mobile Subscriber Identity)
  - LAI (Location Area Identity)

Podle maximálního vysílacího výkonu se mobilní stanice dále dělí do pěti výkonnostních skupin.

GSM Class	1	2	3	4	5
max. výkon	20W	8W	5W	2W	0,8W

Uvedené výkony jsou maximální pro danou třídu, v praxi je výkon adaptivně nastavován. Většina dnešních příručních mobilních stanic spadá do kategorie GSM Class 4.

- **Subsystém základnových stanic - BSS (Base Station Subsystem)**

Jedná se o subsystém, se kterým prostřednictvím rádiového rozhraní komunikují jednotlivé mobilní stanice MS. Samozřejmě není možná komunikace jednotlivým mobilních stanic přímo mezi sebou. Mobilní stanice nepatří do BSS ani do žádného z dalších subsystému, ale jsou samostatnou součástí systému GSM.

Základními stavebními prvky subsystému BBS jsou následující zařízení:

- **Základnové stanice BTS (Base Transciever Station)**
- **Základnová řídicí jednotkaBSC (Base Station Controller)**
- **Transkodér TC (TransCoder)**

V systému GSM obvykle obsahuje jeden svazek 9 buněk, používají se však i svazky s menším počtem buněk. Uvnitř každé buňky je umístěna základnová stanice (není-li využito principu sektorizace), která zajišťuje komunikaci s mobilní stanicí. Tato komunikace probíhá přes rádiové rozhraní (Air interface), označované jako rozhraní Um nebo I/F.

Několik základnových stanic je společně řízeno jedinou základnovou řídicí jednotkou BSC. Jednotlivé BTS mohou spolu s BSC vytvářet hvězdicovou, kaskádní, stromovou i jinou topologii. Základnové stanice se dělí do osmi výkonových tříd s výkony 2,5; 5; 10; 20; 40; 80;1 60; 320 Wattů a komunikace s BSC je často realizována radioreléovými spoji. Stejně jako v případě komunikace BSC - MSC však může být použito optického nebo metalického vedení.

Základnové řídicí jednotky BSC výrazně odlehčují ústředně MSC tím, že vykonávají funkce handoveru (v systému GSM typu MAHO), přidělování kanálů (dynamické) a částečně také plní funkce přepojovací. Mezi BTS a BSC se nachází rozhraní Abis. Na rádiovém rozhraní (Um) má telefonní kanál přenosovou rychlost 13 kbit/s, na rozhraní Abis již 16kbit/s. Rozhraní mezi základnovou řídicí jednotkou a ústřednou MSC se nazývá rozhraní A. Mobilní ústředna však z důvodu kompatibility s externími sítěmi používá telefonní kanály s rychlostmi 64 kbit/s. Proto je nutností zařdit mezi BSC a MSC transkódovací jednotku TC (TransCoder), která má na starost přizpůsobení rychlostí. Tato jednotka může být umístěna jednak na straně BSC nebo na straně MSC, což je z ekonomických důvodů výhodnější.

- **Síťový spojovací subsystém - NSS (Network Switching subsystem)**

Jde vlastně o systém mobilních resp. radiotelefonních ústředen. Na rozdíl od klasických telefonních ústředen však celý tento systém vykonává kromě obvyklých přepojovacích funkcí ještě mnoho dalších činností, vyplývajících z mobility účastníků (určování polohy, handover, přidělování kanálů apod.).

Základními stavebními prvky subsystému NSS jsou následující zařízení:

- **Mobilní radiotelefonní ústředna MSC (Mobile Switching Centre)**
- **Domovský lokační registr HLR (Home Location Register)**
- **Návštěvnický lokační registr VLR (Visitor Location Register)**
- **Centrum autentičnosti AuC (Authentication Centre)**
- **Identifikační registr mobilních stanic EIR (Equipment Identity Register)**
- **Jednotkou spolupráce s externími sítěmi IWF (Inter-Working Functionality)**
- **SMS Centrum**

Síťový spojovací subsystém plní v systému GSM především spojovací funkce, obdobně jako je uskutečňuje klasická telefonní ústředna. Tuto funkci plní v subsystému NSS mobilní radiotelefonní ústředna MSC. Jde zde o běžný typ telefonní ústředny, která je však doplněna o další funkce plynoucí z mobility přepojovaných účastnických stanic. Tato ústředna je nadřazena nad systémem řadičů BSC a jedna nebo více z nich plní funkci tzv. Gateway MSC a umožňuje propojení mobilní sítě GSM s externími telekomunikačními sítěmi, fixními nebo mobilními. Za tímto účelem je potřeba ústřednu vybavit jednotkou spolupráce s externími sítěmi IWF (Inter-Working Functionality)

Subsystém NSS dále realizuje celou řadu specifických úloh, spojených s mobilitou účastníků. Součástí každé sítě GSM je domovský lokační registr HLR, což je v podstatě hlavní databáze, ve které jsou uložena veškerá důležitá data o uživatelích sítě.

Obsahuje důležitá čísla IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Subscriber ISDN Number), zpřístupněné služby a dále například údaje týkající se polohy uživatele. V síti jednoho operátora je vždy minimálně jeden HLR, může jich být i více. Součástí registru HLR je i centrum autentičnosti AuC (Authentication Centre), což je chráněná databáze, obsahující klíče pro ověřování totožnosti účastníků. Toto centrum má dále na starost šifrovací klíč, podle kterého se šifruje každý účastnický signál přenášený rádiovým rozhraním.

Tento klíč je unikátní pro každého účastníka a je proměnný v čase. Na registr je dále napojen identifikační registr mobilních stanic EIR. V této databázi jsou uložena čísla IMEI (International Mobile Equipment Identity) mobilních stanic, které jsou autorizovány k použití v dané síti, dále čísla ukradených MS a je zde i seznam stanic, které jsou označeny jako porouchané, případně nesplňující určitá požadovaná specifika. Velmi důležitou roli hraje také návštěvnický lokační registr VLR, který přechodně uchovává a obnovuje data o uživatelích, v dané chvíli se nacházejících v oblasti příslušné MSC. Obsahuje podobné informace jako HLR , ale pouze dočasně, tzn. že jakmile účastník opustí oblast, data jsou vymazána.

K přenosu signalizace mezi jednotlivými zařízeními je použita signalizační síť SS7 a jsou definovány následující rozhraní:

- **B** mezi MSC a VLR
- **C** mezi MCS a HLR
- **D** mezi registry VLR A HLR
- **E** mezi dvěma ústřednami MSC
- **F** mezi MSC a EIR
- **G** mezi HLR a AuC

- **Operační a podpůrný subsystém - OSS (Operational and Support Subsystem)**

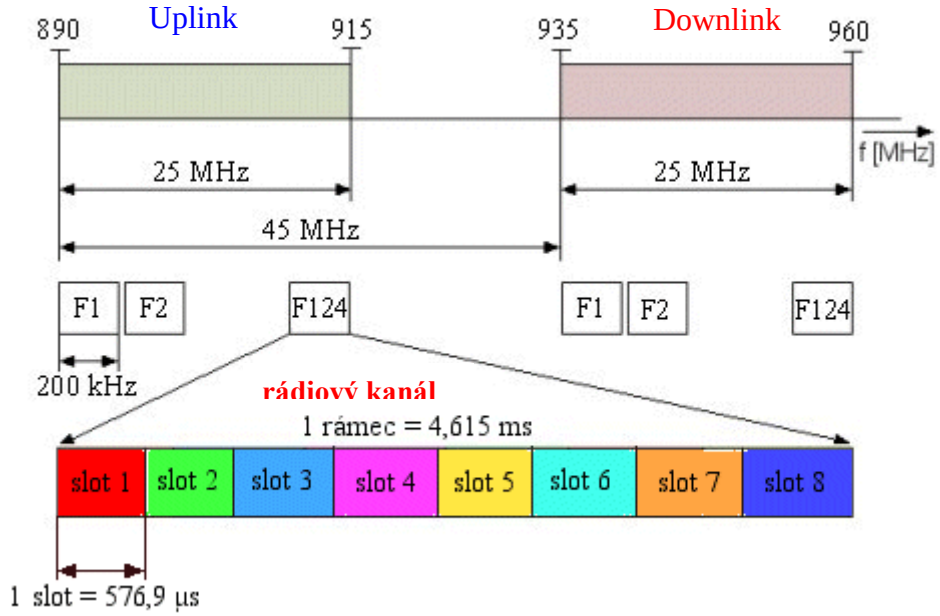
Cílem tohoto subsystému je zajišťovat řádnou činnost a údržbu celé sítě GSM. Je zde prováděn monitoring, diagnostika a opravy poruch systému a mnoho dalších úkonů. Další funkcí tohoto bloku je také administrativní podpora.

Systém GSM dále spolupracuje s externími složkami.

- **Uživatelé systému, účastníci (subscribers)**: Ti přicházejí do styku se systémem pouze prostřednictvím svých mobilních stanic MS.
- **Operátoři:** Budují a provozují systém GSM. Pod dohledem regulačních orgánů se starají o stránku technickou, administrativní i finanční.
- **Externí telekomunikační sítě:** K těmto sítím náleží především veřejná komutovaná telefonní síť PSTN (Public Switching Telecommunication Network) a digitální sítě integrovaných služeb ISDN (Integrated Services digital Network), dále například sítě PSPDN (Packet Switched Public Data Network), PLMN (Public Land Mobile Network) nebo družicové telekomunikační systémy.

Rádiové rozhraní systému GSM

Na každém rádiovém kanálu je metodou TDMA vytvořeno 8 časových slotů, přičemž každý interval představuje 1 uživatelský kanál. Celkem je tedy u standardního systému GSM 900 k dispozici 8 x 124 = 992 duplexních kanálů (3000 u varianty GSM 1800). To ovšem platí při zdrojovém kódování "plnou rychlostí", tzv. full rate. Zavedením dokonalejšího a účinnějšího zdrojového kódování half rate je potom možno docílit přenosu 16 hovorových kanálů na jedné nosné vlně. Uvedený způsob přenosu s kombinovaným frekvenčním a časovým multiplexem se pak označuje zkratkou **FDMA/TDMA**.



Každý digitalizovaný hovorový kanál má po zakódování v kodéru zdroje přenosovou rychlost 13 kbit/s. Ta se dále po přidání ochranných bitů, prováděném při kanálovém kódování, zvýší na 22,8 kbit/s.

Sdružením takových osmi kanálů a přidáním dalších pomocných a signalizačních bitů dojdeme k celkové přenosové rychlosti signálu připadajícího na jednu frekvenci o hodnotě 270,883 kbit/s. Odpovídající perioda jednoho bitu je potom 3,692 µs a efektivní přenosová rychlost na jeden kanál 33,854 kbit/s. Jako optimální modulační metoda byla vybrána pro systém GSM gaussovská modulace MSK, tj. **GMSK** s normovanou šířkou pásma předmodulační gaussovské dolní propusti B x T = 0,3.

Odolnost proti selektivnímu úniku je zajištěna tzv. ekvalizací. Při ekvalizaci je do přenosového řetězce na straně přijímače zařazen filtr, který kompenzuje vlastnosti přenosového kanálu na přijímací straně. Proto je v každém slotu vysílána tréninková posloupnost (známá posloupnost bitů) a v přijímači se deformovaný signál porovná se správným signálem a podle výsledku se nastaví parametry ekvalizačního filtru.

Ekvalizace je málo účinná v prostředích, kde vznikají dlouhé výpadky signálu a proto základnová stanice v každém časovém slotu mění kmitočet komunikace (mobilní stanice se jí

přizpůsobují). Použitá ekvalizace spolu se strukturou rámců umožňuje používat mobilní stanice až do rychlosti 250 km/h, což je i maximální rychlost pro úspěšný handover.

Mobilní stanice neustále sleduje kvalitu rádiových kanálů nejen z hlediska intenzity signálu ale také z hlediska bitové chybovosti BER. Měří se až 6 sousedních základnových stanic a na základě těchto údajů BSC nebo MSC rozhoduje o handoveru.

Zabezpečení systému GSM proti zneužití

Úvod **Ověření totožnosti** **Šifrování**

Úvod

V systému GSM je třeba, stejně jako v jiných telefonních sítích zabránit nejen odposlechu, ale také zneužití ztraceného telefonu, volání na cizí účet a podobně. Bezpečnost v sytému GSM je obecně rozdělena do dvou hlavních kategorií. První z nich je ověření totožnosti účastníka, mobilní stanice a SIM karty, druhou kategorií je samotný proces šifrování přenášených dat.

Ověření totožnosti uživatele SIM karty probíhá pomocí zadávání číselných kódů PIN (PIN2) a PUK. Ověření totožnosti mobilní stanice může probíhat (záleží na operátorovi) pomocí IMEI (International Mobile Equipment Identity), což je číslo uložené v mobilní stanic a dále v registru EIR. Do registru VLR je zasláno toto číslo, které je pak ověřeno a zařazeno do jednoho ze seznamů:

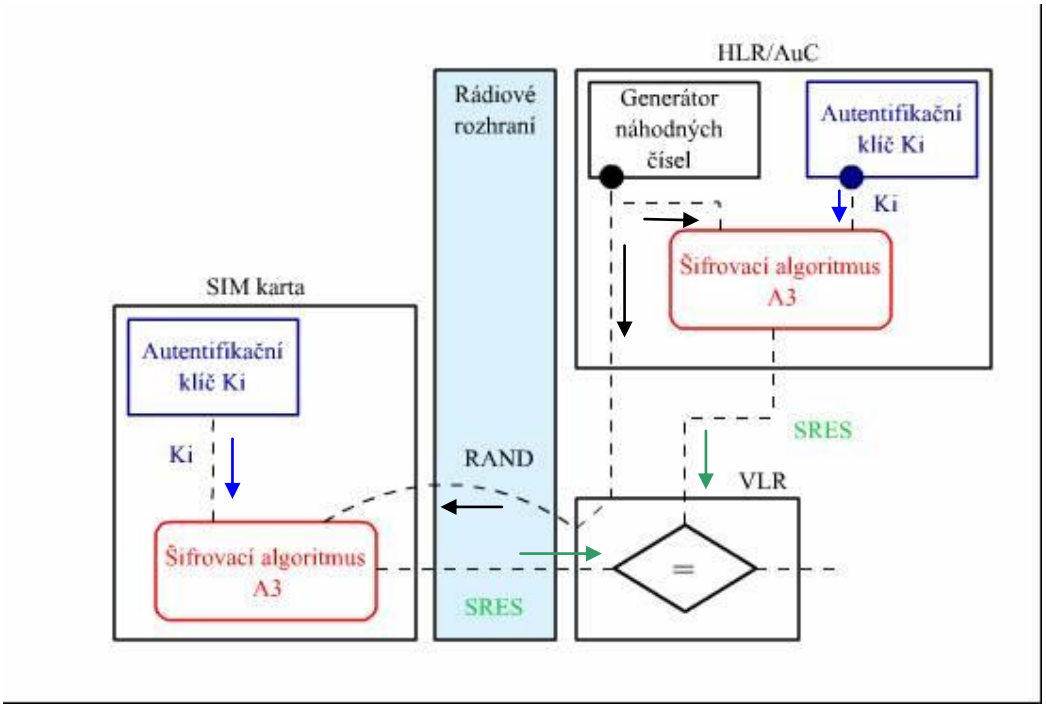
- White list ("bílý seznam") - stanice, jímž je přístup povolen
- Black list ("černý seznam") - kradené mobilní stanice
- Grey list ("šedý seznam") - porouchané stanice, nebo stanice nepodporující určité specifikace

Jediné slabé místo při přenosu jakýchkoli dat systémem GSM se nachází v jeho rádiové části. Data přenášená mezi mobilní stanicí a základnovou stanicí na jedné straně umožňují téměř neomezenou volnost uživatele mobilního telefonu, na straně druhé však znamenají potenciální nebezpečí odposlechu nebo například telefonování na účet majitele. Systém GSM proto používá řadu mechanizmů, jak tomuto předejít. Jedná se o použité protokoly a formáty dat, digitální modulaci GMSK, neustálé přelaďování stanice na různé frekvence, kanálové kódování a výše popsané ověření totožnosti účastníka a mobilní stanice. Další důležité procesy (ověření totožnosti SIM karty a samotné šifrování dat) jsou popsány v samostatných kapitolách.

Proces ověření totožnosti SIM karty

Po zapnutí požádá mobilní stanice o přístup do sítě. Zašle tedy své **IMSI** (International Mobile Subscriber Identity) a toto je jediný okamžik, kdy je používáno toto číslo **IMSI.** Anonymita je poté zajištěna přidělením tzv. dočasné identifikace **TMSI** (Temporary Mobile

Subscriber Identity), která je uložena na SIM kartě a v registru VLR. Způsob, jakým probíhá ověření totožnosti SIM karty je znázorněn na následujícím obrázku.

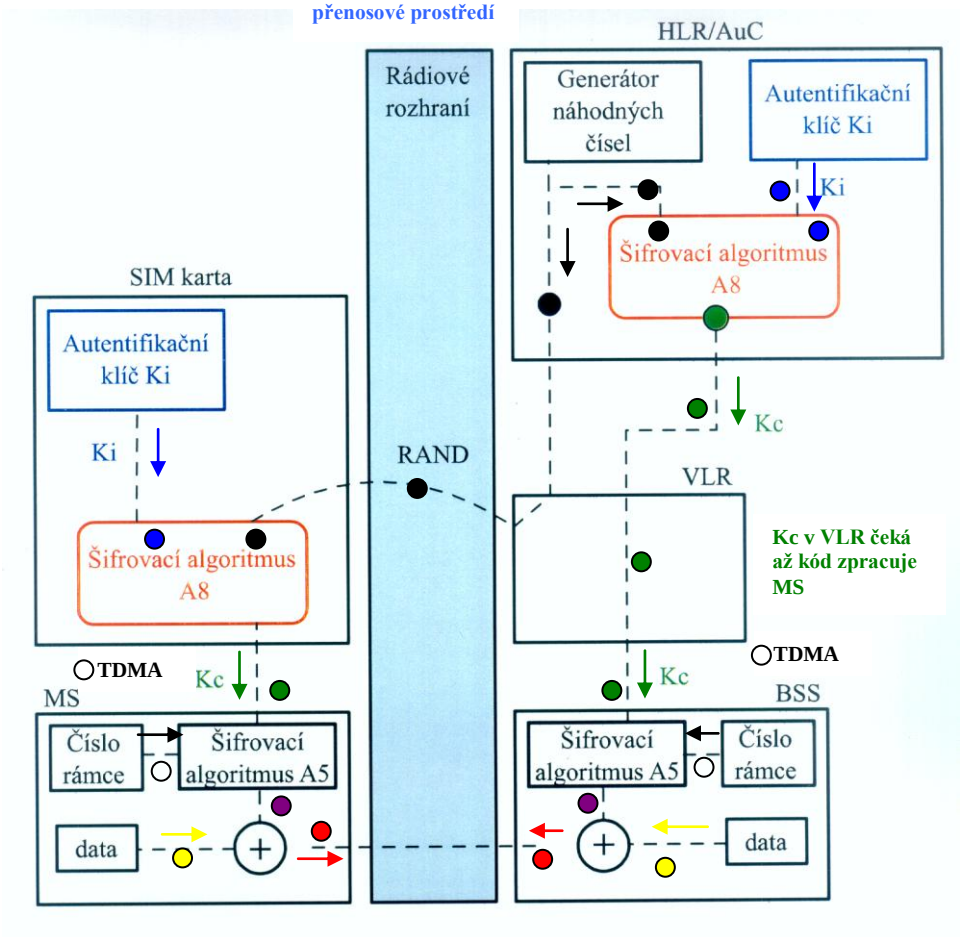


V registru HLR (AuC) je vygenerováno náhodné číslo **RAND**. Na základě tohoto čísla je pak s pomocí autentifikačního klíče Ki podle šifrovacího algoritmu A3 spočítána odezva SRES (Signed Response) na toto náhodné číslo . Zároveň je podle šifrovacího algoritmu A8 (označovaný též A38) vygenerován šifrovací klíč Kc (viz. šifrování).

Tato trojice (RAND - 128 bitů, SRES - 32 bitů a Kc - 64 bitů) je předána do registru VLR, kde je po dobu spojení uchována. Registr VLR dále přepošle náhodné číslo **RAND** mobilní stanici, která v SIM kartě na základě znalosti klíče Ki a čísla **RAND** spočte odpověď SRES. Tato odpověď je poslána zpět do VLR, kde je porovnána s odpovědí vygenerovanou v HLR a určí, zda stanice má přístup do sítě. Algoritmus A3 a klíč Ki jsou tedy zabezpečeně uloženy jednak v registru HLR a také v SIM kartě. *Při komunikaci* tedy rádiovým rozhraním prochází pouze náhodné číslo RAND a odpověď SRES. Algoritmus A3 je vytvořen tak, aby bylo relativně snadné spočítat SRES z údajů Ki a RAND, ale velmi náročné vypočíst Ki z údajů RAND a SRES.

Šifrovací proces

Šifrování probíhá tak, že je na základě klíče (kombinace znaků) pomocí šifrovacího algoritmu vygenerována bitová posloupnost. Tato šifrovací posloupnost se pak přičítá k přenášené bitové posloupnosti. Proces šifrování v systému GSM je popsán následujícím obrázkem.



V registru HLR (AuC) je vygenerováno náhodné číslo **RAND 128 bitů**. Na základě tohoto čísla je pak s pomocí autentifikačního klíče Ki podle šifrovacího algoritmu A8 vygenerován šifrovací klíč Kc (zároveň je pomocí algoritmu A3 spočítána odezva SRES - viz. autentikace) . Tato trojice (RAND - 128 bitů, SRES - 32 bitů a Kc - 64 bitů) je předána do registru VLR, kde je po dobu spojení uchována. Registr VLR dále přepošle náhodné číslo RAND mobilní stanici, která v SIM kartě na základě znalosti Ki a algoritmu A8 vygeneruje šifrovací klíč Kc 64 bitů. Šifrovací posloupnost, kterou k přenášeným datům přičítáme, je generována pomocí algoritmu A5. Vstupními údaji pro tento algoritmus je šifrovací klíč Kc (64 bitů, generovaný zvlášť pro každé spojení) a číslo ***TDMA rámce (22 bitů měnících se každých 4,615 ms).*** Šifrovací algoritmus již není z důvodu dostatečné výpočetní kapacity a rychlosti uložen na SIM kartě, ale je implementován přímo v mobilní stanici. Pokud během hovoru dojde k handoveru, šifrovací klíč Kc se nemění. Ani při šifrování tedy nedochází k přenosu žádného klíče a rádiovým rozhraním jsou přenášena pouze náhodná čísla RAND a šifrovaná data.

Algoritmy A3 a A8 nejsou specifikovány v doporučení, ale GSM MoU (Memorandum of Understnding) a je zde ponechána určitá volnost, ponechávající možnost domluvy mezi provozovatelem sítě a výrobcem SIM karet.