Digitální TV

Vývojem standardů pro digitální vysíláni se v Evropě zabývá konsorcium **DVB** (*Digital Video Broadcasting Project*), které sdružuje jak výrobce, tak poskytovatele služeb v oblasti digitálního vysílání. **DVB** definuje především technické standardy, např. formát vysílaných dat nebo způsob jejich zašifrování před nežádoucím příjemcem, tzv. **Conditional Access** (CA)**.**

Conditional Access

CA je označení pro proces šifrování audiovizuálních dat pro digitální televize. Probíhá v několika rovinách.

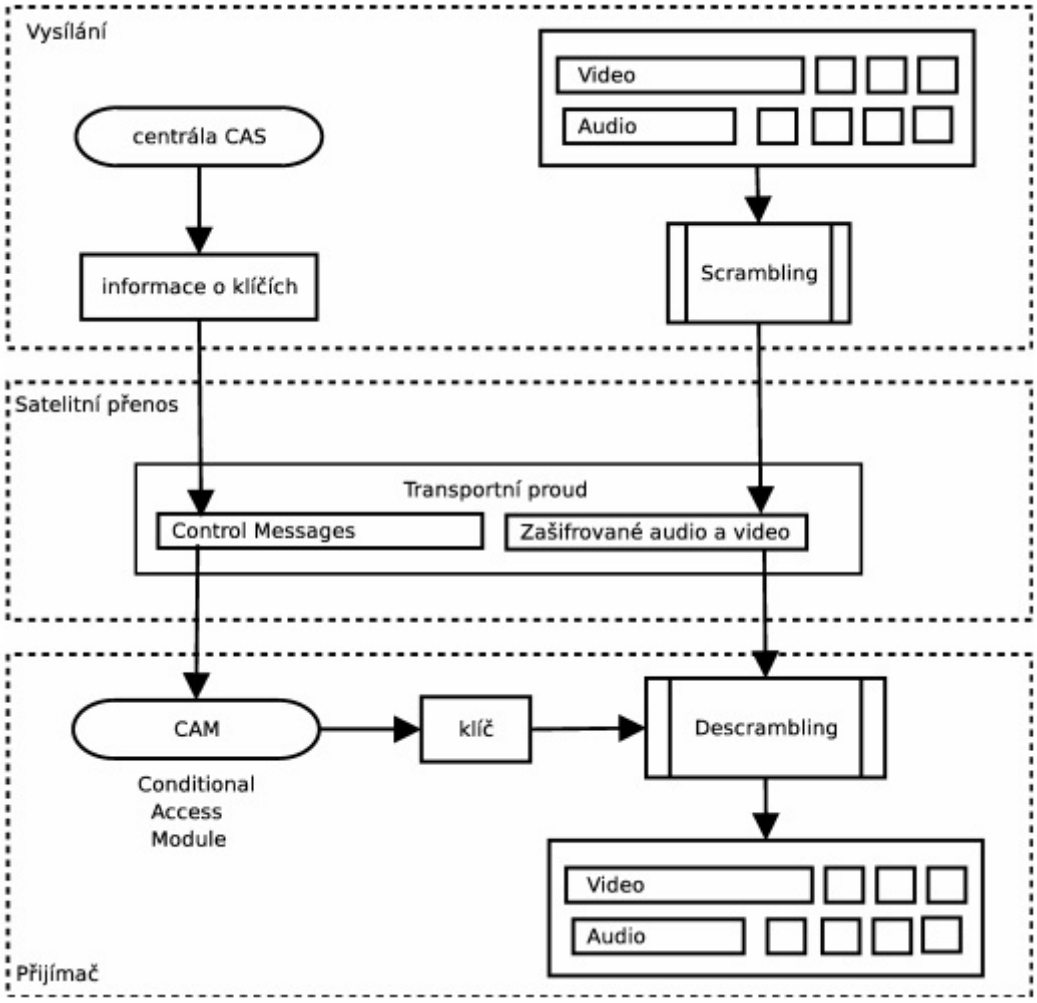
Scrambling, Descrambling

Vlastní zašifrování audiodigitálních dat na straně odesilatele se nazýva **Scrambling**, dešifrování na straně příjemce je **Descrambling**. Oba dva procesy probíhají v reálnem čase a pracují s velkým množstvím dat, proto je nutné používat velmi rychlé algoritmy (symetrická šifra se stejným klíčem pro šifrování i dešifrování). Aby nedocházelo často k prolomení šifry, klíče pro scrambling i descrambling, tzv. **Control Word**, se mění. V praxi to funguje tak, že v přístroji příjemce (přijímač nebo karta) je zároveň uloženo více klíčů a ty se řádově po desítkach sekund mění. Výběr klíče provádí vysílací centrála, která posílá s audiovizuálními daty zárověň i tzv. řídící zprávy - **Control Messages** (CM).

Control Messages

Entitlement Management Message (EMM) je zpráva, která obsahuje údaje o právě používaném klíči, tato zpráva je šifrována algoritmem s nízkým rizikem prolomení (asymetrická šifra) i za cenu delšího času potřebného na šifrování.

Entitlement Control Message (ECM) je zpráva, která obsahuje příkaz ke změně klíče a zárověn samotný klíč



Standart pro Scrambling se nazýva **Common Scrambling Algorithm** (CSA).

Konkrétní implementace *Conditional Access* se nazývá **Conditional Access System (CAS).** Existuje mnoho CAS od různých výrobců. Aby poskytovatelé mohly používat různé CAS, vznikl standard (rozhraní), tzv. **DVB CA Common Interface**.

DVB CA Common Interface

Je to rozhraní, které umožňuje využívat různé implementace **CA.** Pokud je zařízení pro příjem signálu vybaveno slotem, který je kompatibilní s **DVB CA Common Interface,** může uživatel pouhou výměnou kryptografického modulu využívat služby chráněné jinými CAS. Kryptografický modul, který je kompatibilní s DVB CA Common Interface se nazývá **Conditional Access Modul** (CAM).

Samotný descrambling probíhá tak, že přijímač vezme ze vstupního proudu dat kontrolní zprávy (Control Messages), předá je kryptografickému modulu (CAM). Ten je zpracuje a posílá přijímači zpátky klíče, kterými bude audiodata descramblovat. DVB CA Common Interface tedy definuje způsob, jakým přijímač předá Control Messages a jak dostane klíče.

Obsah CM a správa klíču je však v režii dodavatele CA systému. Má to ale poměrně velké riziko, protože občas dojde k prolomení některých CA systémů a může být nutné vyměnit kryptografické moduly, které je používají. Pokud by například došlo k prolomení samotného CSA (Common Scrambling Algorithm), bylo by nutné vyměnit všechny přístroje, protože broadcasteři v Evropě používají právě tuto šifru.

Cryptoworks DVB CA

Systém Cryptoworks byl vyvinut firmou Royal Philips Electronics. Je kompatibilní s výše uvedeným rozhraním a využívá se i v dalších oblastech, např. při autorizaci v počítačových sítích.

Kryptografický modul je vybaven terminálem pro smartkartu (SmartCard). Je to karta velikosti bankovní karty, která obsahuje samostatný čip s procesorem. Karta Cryptoworks může současně držet sady klíčů pro různé služby mnoha poskytovatelů a různé kryptografické techniky a algoritmy. V případě digitálního vysílání uchovává klíče pro *descrambling* a implementaci pro CAM s rozhraním DVB CA Common Interface.

Některé levnější přístroje bez DVB CA Common Interface mají pouze vestavěný dekodovací systém Cryptoworks, který má vstup pouze na smartkartu (u nás se dodává se službou UPC Direct).

Na smartkartě sou uloženy klíče pro descrambling digitálního a zvukového signálu. Centrála je vyměňuje zasláním **ECM (***Entitlement Control Message***)** zhruba jednou za měsíc.

V pravidelných intervalech během vysílání se mění klíč, kterým je obraz a zvuk zašifrován a centrála posílá informace o změně prostřednictvím **EMM** (Entitlement Management Message). Pokud uživatel během sledování televize vytáhne kartu z přístroje, obraz se během několika desítek vteřin přeruší, neboť přístroj nemá k dispozici klíče na descrambling.

Systém Cryptoworks je velmi propracovaný, umožňuje zasílat Control Messages buď všem kartám, jedné kartě a nebo různým sdíleným prostorům karet například podle geografického umístění. Je nezávislý na šifrovací technologii, kterou přenáší.

Při přenosu citlivých informací mezi kryptografickým modulem a centrálou jsou data šifrována pomocí RSA (především klíče pro descrambling). Na kartě je uložena sada RSA klíčů, které nikdy neopustí kartu. Karta přijímá a dostává zprávy pro centrálu v podobě instrukcí zašifrovaných RSA, avšak tento protokol není veřejně zcela znám.

Při descramblingu si přijímač přes DVB CA Common Interface vyžádá **Control Word** od **CAM. CAM** si jej vyžádá od karty, která odpoví instrukcí s klíčem, pokud má karta příslušné oprávnění. Veškeré RSA šifrování/dešifrování probíha na kartě, kartu tedy opouští Control Word nechráněný RSA.

Zdroje včetně obrázku:

[1]
https://is.muni.cz/auth/el/1431/jaro2010/M0170/um/satelit.pdf?fakulta=1431;obdobi=4664;studiu

m=448330;kod=M0170

[2] http://en.wikipedia.org/wiki/Conditional_access

Rádiové signály GPS

Prehľad družicových navigačných systémov

Hneď na začiatku treba zdôrazniť, že americký GPS nieje jediným fungujúcim navigačným systémom, akurát je najznámejším a jedným z najstarších. GPS vzniklo v 70tych rokoch minulého storočia pôvodne pre vojenské účely ministerstva obrany USA. Cieľom bola možnosť zistiť polohu na ľubovoľnom mieste na zemi pomocou jednoduchého prijímača.

V 90tych rokoch došlo k uvoľneniu systému pre širokú verejnosť s tým, že signál bol umelo skreslovaný tak, že odchýlka bola okolo 20 – 30m a taktiež bol dostupný iba na niektorých miestach. Toto opatrenie bolo prijaté proti hrozbe teroristických útokov. 1. Mája bola umelá odchýlka vypnutá a civilný sektor dostával rovnako presné údaje ako armáda.

Okrem neho ďalšie družicové systémy prevádzkuje Rusko s názvom GLONASS, vývoj Galilea prebieha pod vedím európskej vesmírnej agentúry (ESA), v číne vyvíjaju Compass.

názov	**Priníp merania**	**štát**	**Vypustenie družíc**	**Počet družíc v službe**	**Plánovaný počet družíc**	**Výška orbitu**
Navstar GPS	kódové	USA	1978	31	24+3	20 200km
Glonass	kódové	Rusko	1982	20	24	19 100km
Galileo	kódové	EU	2006	2	27+3	23 200km
Compass	kódové	Čína	2007	1	24	21 500km

Princíp fungovania GPS

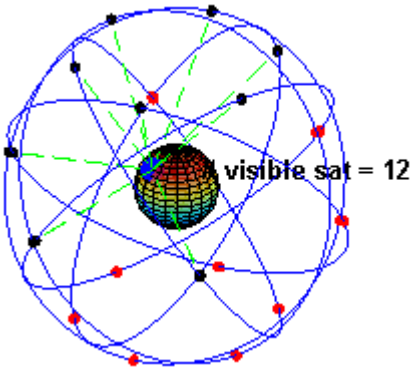
Celý systém je možné rozdeliť na tri časti: kozmickú, riadiacu (kontrolnú) a užívateľskú.

Kozmickú časť tvorí 24 nestacionárnych satelitov Navstar od firmy Rockwell International a tri záložné satelity.Tieto satelity obiehajú zem 11hod a 56minút na 6tich obežných dráhach sklonených o 60°. Z každého miesta na zemi tak v ideálnom prípade je možné zachytávať signály z 12tich družíc. Každá z družíc obsahuje vysielač a prijímač a césiové atómové hodiny. Prijímač slúži na komunikáciu z riadiacim strediskom na Zemi.(napríklad korekcia letovej dráhy). Vysielač je určený k zasielaniu dát späť do riadiaceho centra, ale hlavne vysiela dáta užívateľom.

Riadiaci systém ma za úlohu monitorovať beh družíc a v prípade problémov ich riešiť. Riadiace systémi sú v 9tich pozemných staniciach, umiestnených v okolí rovníka. Hlavná monitorovacia stanica je v Colorado Springs.

Užívateľská časť je tou, ktorú si môže každý kúpiť a používať. Ide napríklad o klasické prijímače s displayom alebo prijímače zabudované do ďalších zariadení ako sú PDA, mobilné telefóny. Väčšina prijímačov je pasívna. Tzn. Že neumožňuje vysielať ale iba prijímať signál. Je to tak z jednoduchého dôvodu bezpečnosť: v armáde – keď vojak nemá vysielač ale iba prijímač, nie je ho možné vystopovať.

Ako to celé funguje? Každá družica vysiela informácie o svojej polohe, presný čas z atómových hodín a približné polohy ostatných družíc. Prijímač, ktorý musí mať priamu viditeľnosť na oblohu využíva časový rozdiel medzi časom vyslania a časom prijatia dát. Ak takto spracuje dáta z 3ch družíc je schopný určiť 2D polohu, tj. Zemepisnú šírku a dĺžku. Pre výpočet 3D polohy tj. Aj s nadmorskou výškou je potrebných 4 satelitov.



Základná charakteristika GPS

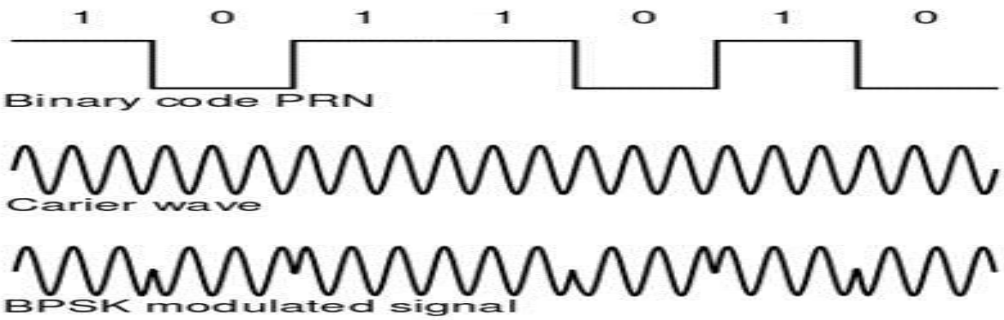
Družice systému GPS vysielajú rádiové signály, ktoré umožňujú užívateľom určovať svoju polohu a čas. Pôvodný návrh počítal s dvoma rôznymi kódmi:

1. C/A kód (Coarse/Acquisition code) – verejne dostupný
2. P kód (Precision code) – prístupný iba autorizovaným užívateľom, tj. Armáde

V plánovanej modernizácii sa v GPSIII pripravujú nové skupiny:

1. C kód (civilian code) – verejne dostupný
2. M kód (military code) - prístupný iba autorizovaným užívateľom, tj. Armáde

Modulácia a demodulácia signálu



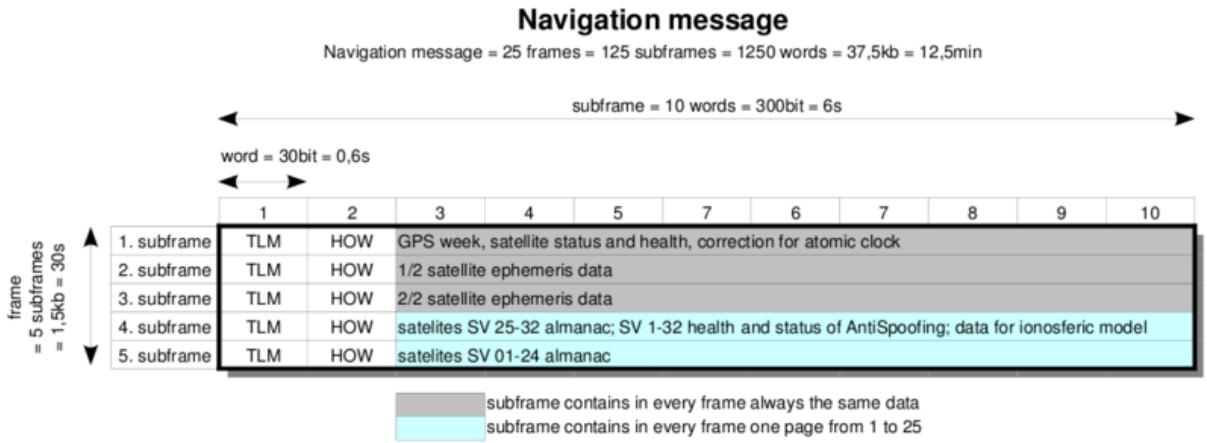
Pre prenos bitového toku sa používa fázová modulácia (PM – phase modulation) s binárnym kľúčovaním (BPSK – binary phase shift keing). To znamená že jedna nosná frekvencia nesie jeden bit, ktorý je zaznačený zmenou fáze nosnej vlny o 180°. Ak sú na jednej frekvencii modulované 2 signály, je druhá modulácia BPSK posunutá o 80-100°. Signál každej družice je pred vysielaním modulovaný pseudonáhodnou postupnosťou kódov s hodnotami +1 alebo -1, ktoré nazývame PRN kód (pseudo random noise code). Pretože všetky družice vysielajú na rovnakej frekvencii, k oddeleniu ich signálov sa využíva metóda CDMA (Code division multiple access), taktiež nazývaná ako kódový multiplex, kde ma každá družica svoj jedinečný PRN kód.

Tvary kódov

C/A kód je 1023 bitov dlhá postupnosť čísel PRN, ktorá je vysielaná rýchlosťou 1,023 Mbit/s, opakuje sa tak každú milisekundu. Každá družica používa iný kód, celkom 32 pre družice a 5 pre špeciálne použitie.

P kód je taktiež PRN kód, približnej dĺžky 2,35 x 10^{14} bitov, ktorý je rozdelený do 38 sekvencií, kde 32 je vyhradených pre družice a 6 pre iné použitie. Dĺžka jednej sekvencie pre jednu družicu je 6,1871x 10^{12}bitov pri dátovej rýchlosti 10,23Mbit/s a opakuje sa jeden krát za týždeň. Veľká časť P kódu zaisťuje eliminovanie nejednoznačnosti.

Štruktúra navigačnej správy



Navigačná správa je modulovaná z 25 rámcov, ktorých odvisielanie trvá 12,5 minúty. Každý rámec obsahuje 5 podrámcov, ktoré obsahujú dáta:

1. Podrámec – číslo týždňa v časovej referencii GPS, korekciu pre atómové hodiny a zdravotný stav družice
2. Podrámec – polohu danej družice 1.časť
3. Podrámec – polohu danej družice 2.časť
4. Podrámec – stav režimu AntiSpoofing a zdravotný stav družíc 25-32
5. Podrámec - zdravotný stav družíc 1-24

Podrámec 1., 2. a 3. Je obsahovo rovnaký v každom rámci, aktualizuje sa po niekoľkých hodinách. 4. A 5. Podrámec nesie v každom rámci iba 1/25 dát, aktualizuje sa po niekoľkých dňoch.

Každý podrámec je rozdelený na 10slov, každé po 30b. Prvé slovo je vždy telemetrické a nesie informácie o začiatku podrámcu. Druhé slovo je predávacie a nesie informáciu o poradí podrámca v aktuálnom týždni GPS (7×24×60×2×5=100 800 možných hodnot) a poradové číslo podrámca v aktuálnom rámci. Ostatné slová majú z 30b informačných iba 24, zvyšných 6 je paritných bitov, ktoré slúžia k zabezpečeniu prenosu pomocou Hammingovho kódu (32,26) zo vzdialenosťou 4. Tento mechanizmus umožňuje detekovať v slove 3 chybné bity alebo 1 opraviť. Pretože jeden bit trvá 20ms, je slovo dlhé 0,6s, podrámec 6s a každý rámec 30s.

Kódovacie systémy PAY TV

Ako už samotný názov napovedá, PAY TV je forma poskytovania predplatených televíznych služieb, inými slovami, „platená televízia“. Šírenie signálu je v takomto prípade najčastejšie realizované prostredníctvom digitálneho satelitného vysielania. Divák príjma signál pomocou satelitného príjmača a prístupovej karty, ktorá umožňuje prístup k vysielaniu v závislosti od toho, aké programy a na akú dobu má divák (pred)platené. Tento koncept má svoj počiatok zhruba v roku 1993, kedy do Európy nastúpila platená televízia. Aby sa zamedzilo neoprávnenému využívaniu televíznych služieb, museli televízne spoločnosti riešiť otázku kódovania signálu.

Conditional Access System (CAS)

Systém podmieneného prístupu (CAS) je v digitálnej oblasti označenie pre kódovací systém. Na trhu ich je niekoľko. Nexistuje žiadna dohoda, štandard, podľa ktorého by televízne stanice využívali nejaký konkrétny kódovací systém. Dôvodom je predovšetkým konkurenčný boj televíznych spoločností a ich snaha o maximálne zabezpečenie digitálneho obsahu. Hlavnou metrikou úspešnosti toho-ktorého kódovacieho systému je počet (rozšírenie, množstvo) neoprávnených (tzv. Pirátskych) prístupov k obsahu.

Kľúče

Kódovanie prebieha pomocou 2 hlavných kľúčov

- **Control Word**
  - Slúži na samotné kódovanie digitálneho obsahu. Pri jeho odhalení je možné priamo dekódovať prijmaný signál. Poskytovateľ však obnovuje tento kľúč niekoľkokrát za minútu. Odhalenie kľúča v určitom momente tedá nemá veľký význam. Kľúč je generovaný automaticky takým spôsobom, aby nebolo možné predikovať nasledujúcu hodnotu kľúča. Má dĺžku typicky 60 bitov.
  - Je unikátny pre každý program v pakete.
  - Mení sa každých 2 – 60 sekúnd.
- **Service key**
  - Je to kľúč vyššej úrovne, je preto možné pomocou neho vypočítať *control word*.
  - Je rovnaký pre celý programový paket.
  - Mení sa len zriedkavo.

Sekvencie

2 druhy dátových vstupov:

- **ECM sekvencia**
  - Slúži na prenos control wordu v zašifrovanom stave od poskytovateľa k príjmaču. Vzniká kombináciou control wordu a service key. Je odosielaný v pravidelných časových intervaloch, spravidla každých 2 – 60 sekúnd. Takto sa dostáva na prístupovú

kartu príjmača control word.

- **EMM sekvencia**
  - Prostredníctvom tejto sekvencie sa na prístupovú kartu príjmača dostáva service key. Je odosielana v oveľa väčších intervaloch než ECM.

Obe sekvencie sa prenášajú v zašifrovanom stave.

Spôsob kódovania

Kódovacie systémy pay tv môžeme rozdeliť do nasledujúcich 2 skupín podľa sôsobu kódovania:

- **Systémy na báze RSA prístupového kľúča**
  - Najrozšírenejší spôsob šifrovania.
- **Systémy na báze DES prístupového kľúča**

Spôsob komunikácie

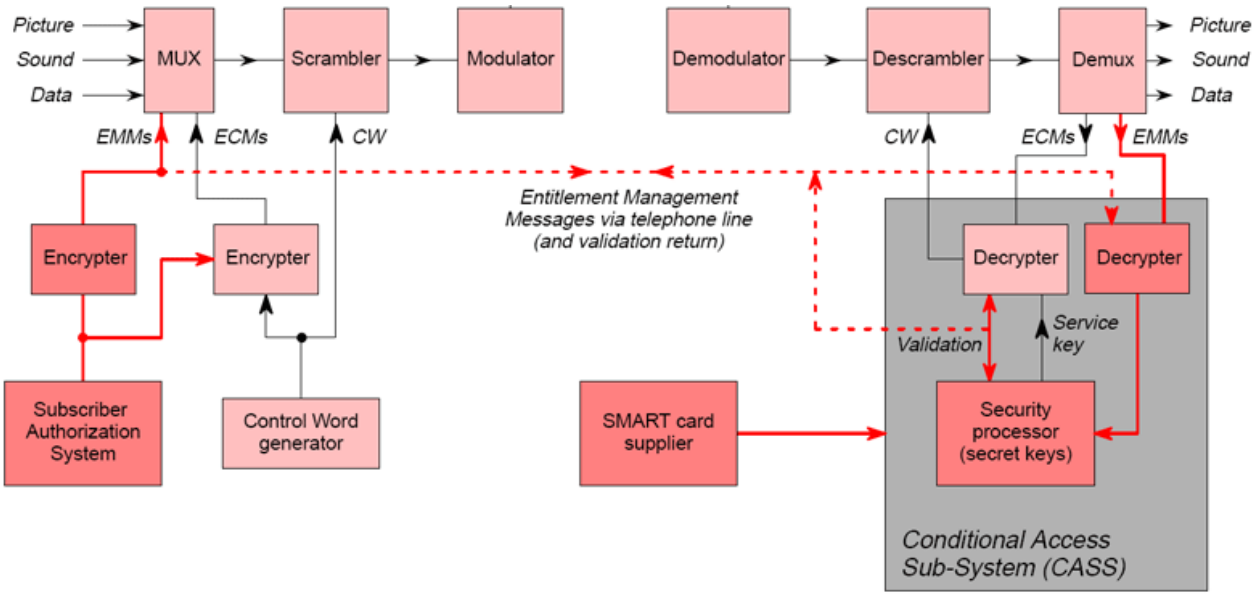
Kódovacie systémy ďalej rozdeľujeme podľa spôsobu komunukácie s abonentom:

- **Pay per View - impulzné**
  - Sú založené na báze neustáleho spojenia so satelitným operátorom, prostredníctvom ktorého dochádza k výmene kľúčov. To je zároveň slabá stránka tohto prístupu, nakoľko je náchylnejšia na výpadky prenosu.
- **Pay per View – dataplexové**
  - Známe tiež ako kartové systémy sú založené na existencii prístupovej karty, v ktorej sú uložené prístupové kľúče a kódy, čím odpadá nutnosť neustáleho spojenia so satelitným operátorom. Prístupová karta je priamo prepojená so satelitným príjmačom.

Priebeh de/kódovania

Televízne spoločnosti digitalizujú a kódujú signál vo svojom vysielacom pracovisku. Následne sa signál dostáva na satelit, odkiaľ sa dostáva divákovi na digitálny príjmač, ktorý ho pomocou dekóderu a prístupovej karty dekóduje.

Spolu s vlastným (obrazovým, zvukovým) signálom sa na prístupovú kartu príjmača dostávajú aj ECM a EMM sekvencie (inštrukcie). ECM je obnovovaná niekoľkokrát za minútu a obsahuje zašifrovaný control word, ktorý je potrebný k dekódovaniu digitálneho obsahu. EMM sa obnovuje oveľa zriedkavejšie. Obsahuje service key, ktorý slúži na dekódovanie control wordu, ale zároveň môže obsahovať aj inštrukcie súvisiace s menežmentom prístupovej karty. Vypočítaný control word sa predáva ďalej modulu, ktorý dekóduje vlastné obrazové a zvukové dáta a predá ich na výstup.



Schéma

Najpoužívanejšie kódovacie systémy

- Conax
- CryptoWorks
- Irdeto
- SECA/MediaGuard
- Viaccess
- Nagravision

[1] http://www.satcentrum.com/clanky/136/kodovacie-systemy-1-cast/

[2] http://en.wikipedia.org/wiki/Conditional_access_system

[3] http://en.wikipedia.org/wiki/Pay_television

[4] http://www.ebu.ch/en/technical/trev/trev_266-ca.pdf

Satelitná telefónia

85% planéty ešte stále nie je pokrytých mobilným telefónnym signálom. Satelity nám v tomto prípade poskytujú ultimatívne prostriedky na pokrytie celej Zeme. Existuje viac druhov služieb poskytovaných satelitnými telefónmi(email, SMS, hlasové služby). Najpodstatnejším rozdielom medzi poskytovateľmi je to, aký druh satelitov používajú.

Geosynchrónne(GEO) satelity sú vo fixnej výške 35,786 km, čo im z pohľadu Zeme umožňuje stáť na mieste. Táto vzdialenosť je ich výhodou, a súčasne nevýhodou. Sú vďaka nej schopné pokryť teoreticky až 1/3 zemského povrchu, no keďže rádiový signál sa šíri rýchlosťou svetla, potrebuje na cestu k satelitu a späť na Zem cca 1/4s, čo predstavuje nepríjemné oneskorenie[1].

Druhou skupinou sú **Low Earth Orbit (LEO)** satelity. Ako už z názvu vyplýva, ide o satelity lietajúce podstatne nižšie, približne 780 až 1420 km nad zemským povrchom. Vďaka krátkej vzdialenosti ktorú musí signál prekonať vzniká oneskorenie len zanedbateľných 0.005 sekundy, no opäť aj táto alternatíva má svoje nevýhody. Čím nižšie satelit lieta, tým menšiu oblasť je schopný pokryť. To vedie k väčšiemu počtu satelitov potrebných na pokrytie celého povrchu[1].

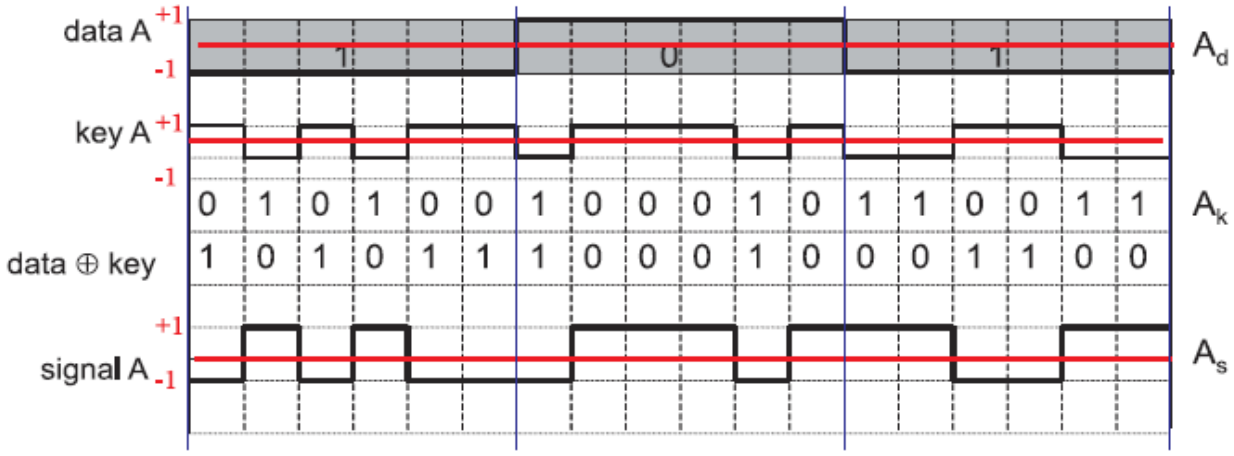
Hlavnými poskytovateľmi satelitných telekomunikačných služieb sú **GlobalStar, Thuaya, Inmarsat** a **Iridium**. Na prenos dát sú použité štandardy CDMA(Code-Division Multiple Access), FDMA (Frequency-Division Multiple Access)a TDMA.

GlobalStar používa CDMA a ostatní spomenutí poskytovatelia kombináciu TDMA a FDMA .

CDMA

Forma multiplexingu, ktorá umožňuje zdieľanie celej šírky pásma jedného prenosového kanálu viacerými signálmi. Je založená na teórii kódovania. Každá stanica má unikátny kód, reprezentovaný postupnosťou prenosových bitov. CDMA patrí do kategórie metód Spred Spectrum(rozprestieranie spektra), čo umožňuje vysielať vyššou rýchlosťou.

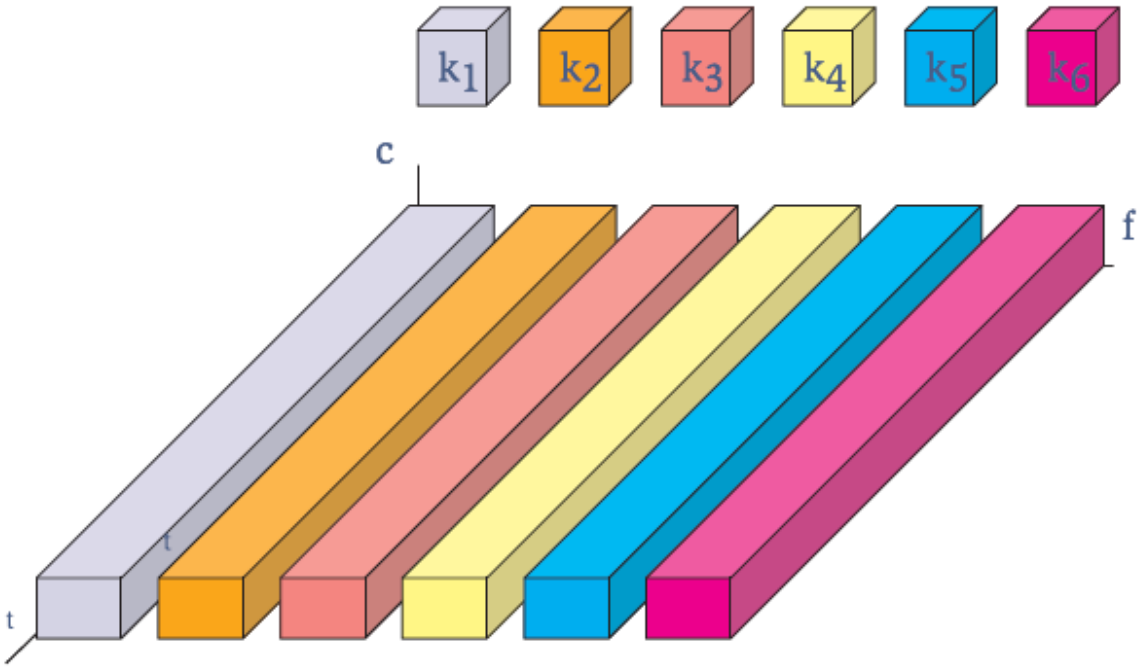
Kódovanie a rozprestrenie signálu vyzerá nasledovne:



Všetky terminály môžu vysielať na rovnakej frekvencii a súčasne môžu používať celú šírku pásma prenosového kanálu. Každý vysielač má svoje unikátne náhodné číslo – bitovú postupnosť, ktorou XORuje pôvodný signál. Takto zakódované dáta sú poslané. Keďže prijímač pozná odosielateľa a teda jeho unikátne náhodné číslo, vie z prijatého signálu XORovaním opäť dostať pôvodné dáta[2][3].

FDMA

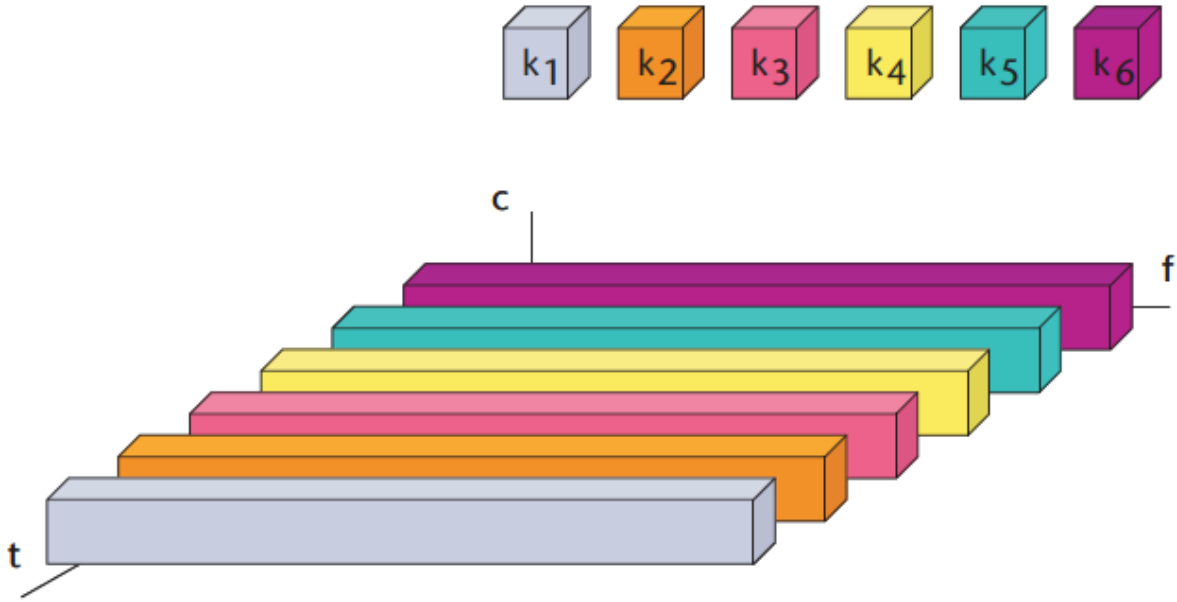
Frekvenčný multiplex vo fyzickej vrstve. Svoje uplatnenie nachádza najmä v satelitných sieťach. Celé dostupné spektrum sa separuje do menších frekvenčných pásem. Komunikačný kanál získava určitú časť spektra k výhradnému použitiu na celú dobu komunikácie. Výhodou tohto prístupu je, že nie je nutná žiadna dynamická koordinácia prenášaných dát. Vytvorí sa spojenie a dáta sa prenášajú po rezervovanej frekvencii. Taktiež odpadá synchronizácia. Nevýhodou je plytvanie pásmom v prípade nesúvislého vysielania(mám rezervovanú frekvenciu, ale nevyužívam ju) , nutnosť ochranných odstupov jednotlivých používaných frekvenčných pásem a nepružnosť (frekvencie sú



nedostatkový zdroj)[2].

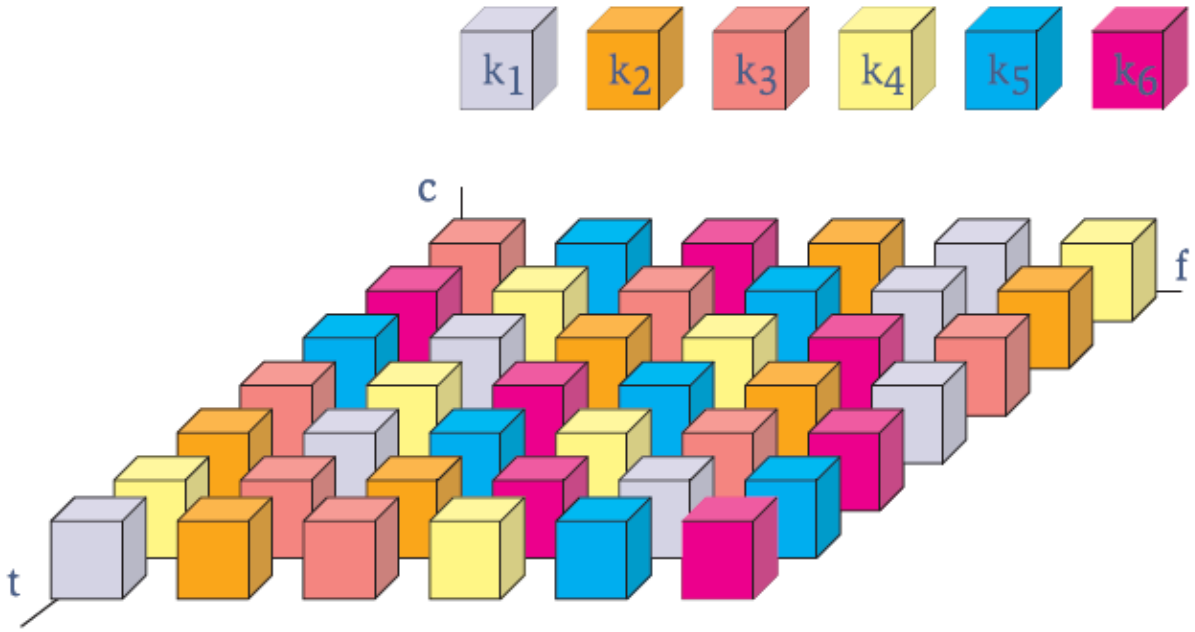
TDMA

Časový multiplex, ktorý nachádza najčastejšie využitie v bunkových mobilných sieťach (GSM). Kanál získa k výhradnému využitiu na nejakú dobu celé dostupné spektrum. Výhodou je, že v prenosovom médiu sa nachádza v každom okamihu iba jeden signál a vysoká priepustnosť aj pri mnohých užívateľoch. Nevýhodou je nutnosť presnej synchronizácie. Rýchlosť média musí byť vyššia než požadovaná rýchlosť prenosu dát daného signálu[2].



Kombinácia TDMA a FDMA

Komunikačný kanál dostane na určitú dobu niektoré frekvenčné pásmo. Prednosťou tohto prístupu je lepšia ochrana proti odpočúvaniu, ochrana proti interferencii frekvencií a vyššia rýchlosť prenosu dát než pri použití kódového multiprexu(CDMA). Nedostatkom je nutná precízna synchronizácia[2].



Ďalšie možnosti zabezpečenia

Aj keď nám tieto druhy prístupov k médiu poskytujú istý druh ochrany súkromia, nie sú považované za bezpečné, čo sa týka ochrany naozaj citlivých informácií, ako je napríklad komunikácia vojenských alebo vládnych subjektov. Za týmto účelom boli vyvinuté napríklad bezpečnostné moduly, pripojiteľné k satelitným telefónom. Tieto používajú kryptovacie algoritmy ako **Citadel**, **Triple**

DES(3DES), alebo **AES**. 3DES a AES sú komerčné a verejne známe riešenia, zatiaľ čo Citadel je neverejný algoritmus[4].

Citadel je používaný práve spomínanou armádou a vládnymi organizáciami po celom svete. Oproti DES, 3DES a AES obsahuje niekoľko výhod. V armádnych aplikáciách sa kryptografické algoritmy pravidelne menia a obnovujú, na čo je tento algoritmus pripravený. Je možné aktualizovať a modifikovať ho, bez zmeny hardwaru. Oproti DES má výhodu, že neobsahuje žiadne slabé kľúče(kľúče, ktoré pri použití s príslušným kryptovacím algoritmom predstavujú bezpečnostné riziko). DES a 3DES sú zraniteľné voči lineárnym a diferenčným kryptoanalýzam. Keďže 3DES získa svoju kľúčovú dĺžku po 3 prechodoch algoritmom DES, je zraniteľný proti útoku „meet in the middle“[5]. Citadel dosahuje kľúčovú dĺžku už po jednom prechode a po jednej iterácii. DES a 3DES sú algoritmy, navrhnuté aby uchránili používateľa proti komerčným hrozbám, zatiaľ čo Citadel je navrhnutý odolať útokom spravodajských služieb. Komerčné algoritmy sú úplne nevhodné pre prípady, kedy je útočníkom iná vládna organizácia, ktorá má prostriedky a motiváciu využiť akékoľvek zraniteľné miesta použitých šifrovacích algoritmov[4].

[1] http://en.wikipedia.org/wiki/Satellite_phone

[2] http://www.fi.muni.cz/usr/staudek/vyuka/PA151/_mac.ps.pdf

[3] http://searchtelecom.techtarget.com/sDefinition/0,,sid103_gci213842,00.html

[4] http://www.outfittersatellite.com/adobe/crypto_CitadelAdvantange.pdf

[5] http://en.wikipedia.org/wiki/Meet-in-the-middle_attack