## 8.5 Zoznam použitej literatúry

[1] Ibrahim K.F.: Newnes Guide to Television and Video Technology, ELSEVIER, 2007

[2] Collins, G.W.Fundamentals of digital television transmission, John Wiley & Sons,Inc.,JOHN WILEY & SONS, INC. New York, 2001

[3] Joanne Tracy, J.-Ward, A.: A practical guide to video and audio compression, Elsevier, 2005

# 9 Šifrovanie TV vysielania a podmienený prístup

Rozsah voľne dostupných programov poskytovaných analógovým TV vysielaním cez kábel alebo satelit je trvalo klesajúci, zároveň ako tento počet klesá, je takmer isté, že rozsiahle množstvo digitálnych TV programov bude platenými (pay-TV) službami, za účelom zisku. Vysoké investície vyžadujú spustenie týchto služieb tak rýchlo ako je to možné. Formy fakturácie budú oveľa viac diverzifikované (bežný poplatok, pay per view – plať za čo pozeráš, near video on demand – blízke video na požiadanie) ako ich poznáme dnes, stane sa ľahšie dostupná vysoká bitová rýchlosť systému a „spätný kanál“ (k vysielateľovi alebo banke) poskytovaný modemom.

DVB štandard predstavuje prenos prístupových riadiacich dát (access control data) prenášaných podmienenou prístupovou tabuľkou (**CAT** - conditional access table) a ďalšími privátnymi dátovými paketami indikovanými programovou mapovou tabuľkou (**PMT** - program map table). Štandard taktiež definuje spoločný kódovací algoritmus (**CSA** - common scrambling algorithm) pri ktorom dohoda medzi cenou a komplexnosťou bola vybratá tak, aby pirátstvo mohlo byť potlačené na primerane dlhú dobu (rovnakú ako je predpokladaná životnosť systému).

Podmienený prístup (CA - conditional access) sám o sebe nie je definovaným štandardom, lebo väčšina operátorov nechce spoločný systém, každý si starostlivo chráni svoj vlastný systém pre obidva komerčné (manažment predplatiteľskej databázy) a bezpečnostné dôvody (viac otvorený systém, skôr pravdepodobnejšie je jeho rýchlejšie cracknutie). Avšak, za účelom vyvarovania sa problému predplatiteľa, ktorý si želá prístup do sieti využitím odlišných systémov podmieneného prístupu (conditional access systems) majúceho množstvo boxov (jeden set-top box pre sieť), DVB štandard predstavuje nasledujúce dve možnosti:

1) **Simulcrypt.** Táto technika, vyžaduje dohodu medzi sieťami využívajúcimi odlišné systémy podmieneného prístupu, ale rovnaký kódovací algoritmus (napríklad, CSA z DVB), umožňujúci prístup k danej službe, alebo programu, niektorým zo systémov podmieneného prístupu, ktoré sú súčasťou dohody. V tomto prípade, transportný multiplex bude musieť prenášať pakety podmieneného prístupu pre každý zo systémov, ktorý môže byť použitý pre prístup k tomuto programu.
2) **Multicrypt.** V tomto prípade, všetky funkcie vyžadované pre podmienený prístup a dekódovanie sú obsiahnuté vo výmennom module v **PCMCIA** forme, ktorý je

vložený do cesty dát transportného toku. Toto je urobené prostredníctvom štandardizovaného rozhrania (common interface - spoločné rozhranie, **DVB-CI**), ktoré zároveň zahrňuje procesorovú zbernicu pre výmenu informácií medzi modulom a set-top boxom. Set-top box môže mať viac než jeden DVB-CI slot, k umožneniu spojenia s mnohými podmienenými prístupovými modulmi. Pre každý odlišný podmienený prístup a/alebo požadovaný kódovací systém, používateľ môže pripojiť modul všeobecne obsahujúci rozhranie pre inteligentnú kartu (smart card interface) a vhodný dekóder.

Multicrypt prístup má výhodu v tom, že nevyžaduje zmluvy medzi sieťami, avšak je viac nákladnejší na implementáciu (cena prípojok, umiestnenie modulov, atď.). DVB-CI prípojka môže byť taktiež použitá na iné účely (napríklad prenos dát). Iba budúcnosť nám povie, ktorá z týchto možností sa uplatní v praxi a ako bude využitá.

## 9.1 Princípy šifrovacieho systému v DVB štandarde

Daná veľmi delikátna podstata tejto časti štandardu, je zrozumiteľná len preto, že sú dostupné veľmi všeobecné princípy; implementačné detaily sú dostupné len pre sieťových operátorov a výrobcov zariadení pod dôvernými zmluvami.

Šifrovací algoritmus predpokladá odolnosť voči útokom od hackerov na tak dlho ako bude možné poskladať šifru s dvomi vrstvami (úrovňami), každú zmenšovaním slabín z ďalších:

- *bloková vrstva* využívajúca bloky 8 bajtov (reverzný šifrový blok zreťazeného módu),
- *streamová (toková) vrstva* (pseudo-náhodný bajtový generátor).

Šifrovací algoritmus používa dve riadiace slova (párne a nepárne) striedajúce sa s frekvenciou poradia vzniku 2 s za účelom urobenia pirátskej práce viac obtiažnejšej. Jedno z dvoch zakódovaných riadiacich slov je prenášané v subjektívnych riadiacich správach (**ECM** - entitlement control messages) počas periódy zatiaľ čo druhé sa používa, rovnako sa riadiace slová zapíšu dočasne do registrov dekódovacieho zariadenia. Je tu taktiež predvolené (východzie) riadiace slovo (ktoré môže byť použité na voľný prístup ku kódovanému prenosu) ale to je málo dôležité.

DVB štandard predvída možnosť šifrovania na dvoch rôznych úrovniach (transportná úroveň a PES úroveň), ktoré nemôžu byť použité simultánne.

## 9.2 Šifrovanie na transportnej úrovni

Transportná (prenosová) paketová hlavička zahrňuje 2-bitové pole nazývané „transportné_šifrovacie_príznaky.“ Tieto bity sú využité na indikáciu či transportný paket je šifrovaný a s ktorým riadiacim slovom, podľa Tab. 9.1.

**Tab. 9.1 Význam transportných_šifrovacích_príznakových bitov**

| TRANSPORTNÉ_ŠIFROVACIE_PRÍZNAKY | VÝZNAM |
|---|---|
| 00 | Bez šifrovania |
| 01 | Šifrovanie s PREDVOLENÝM riadiacim slovom |
| 10 | Šifrovanie s PÁRNYM riadiacim slovom |
| 11 | Šifrovanie s NEPÁRNYM riadiacim slovom |

Šifrovanie na transportnej úrovni je vykonané po multiplexingu celej užitočnej informácie transportného paketu, PES na vstupe multiplexera sa nachádza „mimo nebezpečia.“ Pretože transportný paket môže obsahovať iba dáta prichádzajúce z jedného PES, je z toho dôvodu možné šifrovať na transportnej úrovni všetko alebo iba časť z PES tvoriacej časť z programu multiplexu.

## 9.3 Šifrovanie na PES úrovni

V tomto prípade, šifrovanie obvykle zaberá miesto pri zdroji pred multiplexingom a jeho prítomnosť a riadiace slovo sú indikované 2-bitovým PES_šifrovacím_riadením (PES_scrambling_control) v PES paketovej hlavičke. Tab. 9.2 zobrazuje možné voľby. Nasledujúce obmedzenia sa týkajú šifrovania na PES úrovni:

- hlavička sama o sebe, samozrejme, nie je šifrovaná; dešifrovacie zariadenie pozná kde sa má začať dešifrovanie vďaka informácií obsiahnutej v dielci poľa PES_hlavičky (PES_header) a kde sa má zastaviť vďaka paketovej_dĺžke (packet_length) poľa;

- šifrovanie by malo byť aplikované na 184-bajtové časti a iba posledný transportný paket môže obsahovať adaptačné pole;
- PES paketová hlavička by nemala presiahnuť 184 bajtov, aby sa zmestila do jedného transportného paketu;
- Východzie šifrovacie slovo nie je prípustné v šifrovaní na PES úrovni.

**Tab. 9.2 Význam PES_šifrovacích_riadiacich bitov**

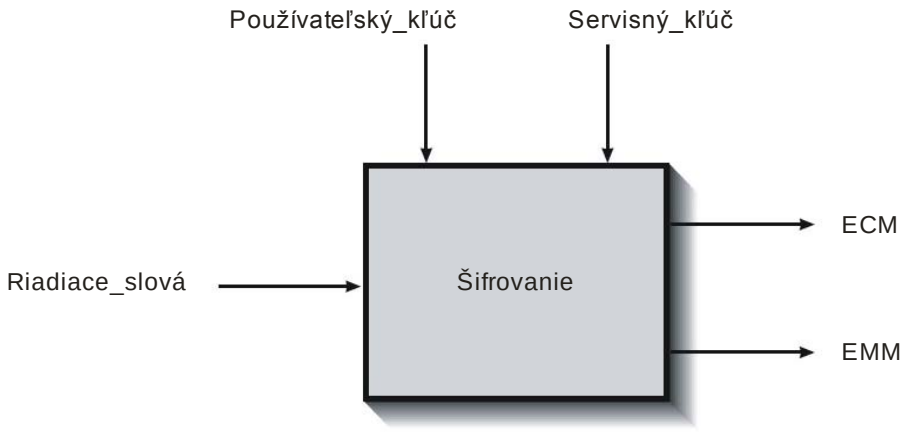
| PES_RIADENIE_ŠIFROVANIA | VÝZNAM |
|---|---|
| 00 | Bez šifrovania |
| 01 | Bez šifrovania |
| 10 | Šifrovanie s PÁRNYM riadiacim slovom |
| 11 | Šifrovanie s NEPÁRNYM riadiacim slovom |

## 9.4 Mechanizmy podmieneného prístupu (CA - Conditional Access)

Informácia potrebná pre dešifrovanie je prenášaná v špecifických podmienených prístupových správach (**CAM** - conditional access messages), ktoré sú dvoch typov: subjektívne riadiace správy (**ECM** - entitlement control messages) a subjektívne manažovacie správy (**EMM** - entitlement management messages). Tieto správy sú generované z troch rôznych typov vstupných dát:

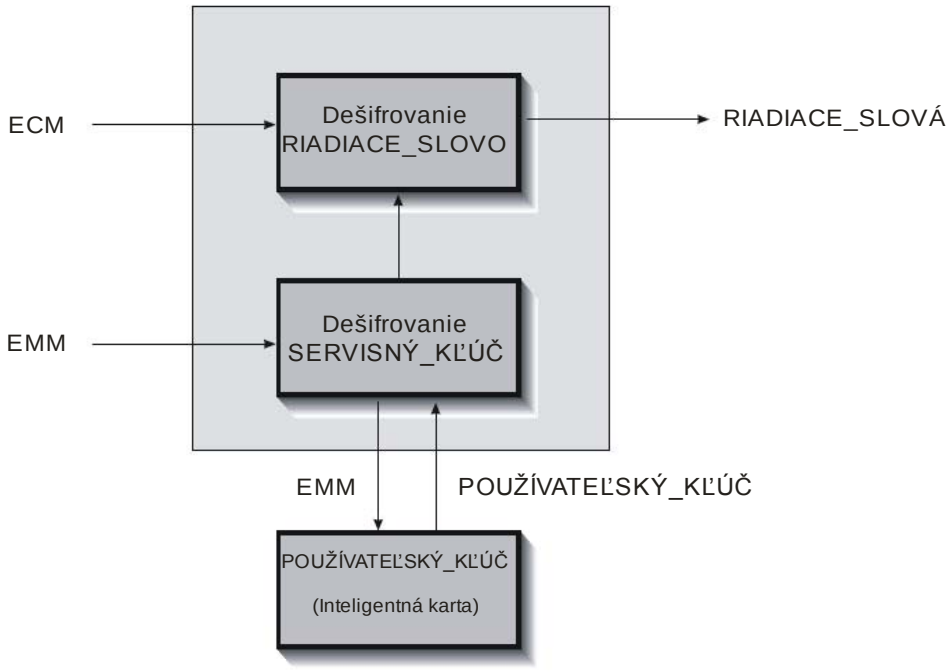
- *riadiace_slovo (control_word)*, ktoré je použité k inicializácií dešifrovacej sekvencie;
- *servisný_kľúč (service_key)*, použitý k zašifrovaniu riadiaceho slova pre skupinu jedného alebo viacerých používateľov;
- *používateľský_kľúč (user_key)*, použitý k zašifrovaniu servisného kľúča.

ECM sú funkciou riadiaceho_slova (control_word) a servisného_kľúča (service_key) a sú prenášané približne každé 2 s. EMM sú funkciou servisného_kľúča (service_key) a používateľského_kľúča (user_key) a sú prenášané približne každých 10 s. Proces generovania ECM a EMM je objasnený na **Obr. 9.1**1.




**Obr. 9.1 Schematická ilustrácia ECM a EMM generačných procesov**

V set-top boxe, princíp dešifrovania pozostáva zo získania servisného_kľúča (service_key) z EMM a používateľského_kľúča (user_key), obsiahnutého napríklad v inteligentnej karte (smart card). Servisný_kľúč (service_key) je následne použitý k dešifrovaniu ECM za účelom získania riadiaceho_slova (control_word) umožňujúceho inicializáciu dešifrovacieho zariadenia. Obr. 9.2 vykresľuje schematicky proces pre získavanie riadiacích_slov (control_words) z ECM a EMM.




**Obr. 9.2 Princíp dešifrovania riadiacich slov z ECM a EMM**

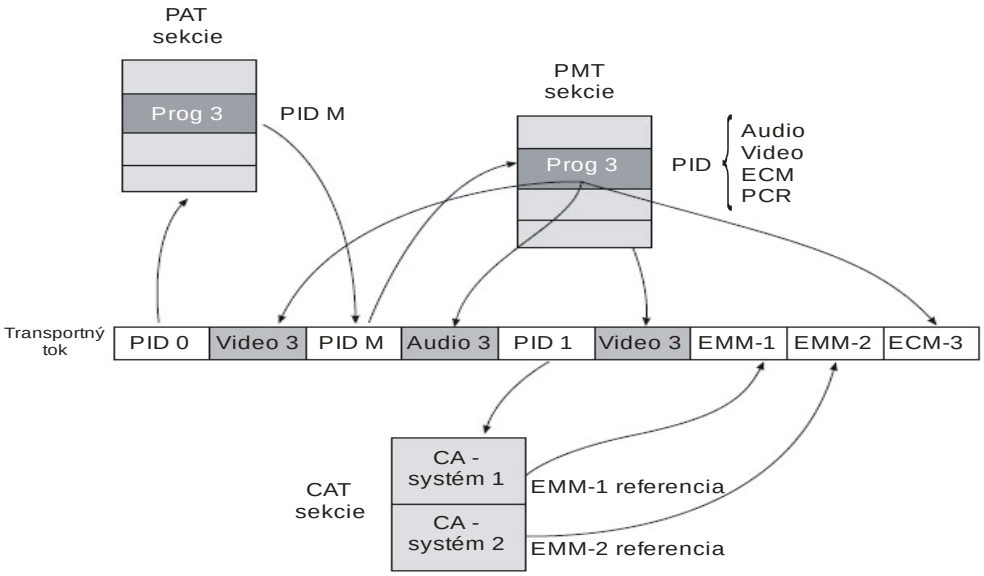
**Dešifrovanie:**

riadiace_slovo = f (ECM, servisný_kľúč)

servisný_kľúč = f (EMM, používateľský_kľúč)

Obr. 9.3 objasňuje proces smerujúci k nájdeniu ECM a EMM potrebných k dešifrovaniu daného programu (tu je to program č. 3):

1) programová alokačná tabuľka (**PAT** - program allocation table), vybudovaná zo sekcii v paketoch s PID = 0×0000, indikuje PID (M) z paketov prenášajúcich programové mapové tabuľkové (**PMT** - program map table) sekcie;
2) PMT indikuje, okrem PID paketov, prenášanie video a audio PES-ov a PCR, PID paketov prenášajúcich ECM;
3) tabuľka podmieneného prístupu (**CAT** - conditional access table), vybudovaná zo sekcii v paketoch s PID = 0×0001, indikuje ktoré pakety preniesli EMM pre jeden (alebo viacero) prístupový(ch) riadiaci(ch) systém(ov) (access control system)(s);
4) z tejto informácie a používateľského_kľúča (user_key) obsiahnutého na inteligentnej karte (smart card), dešifrovací systém môže vypočítať riadiace_slovo (control_word) potrebné k dešifrovaniu ďalšej série paketov (PES alebo transportných v závislosti na šifrovacom móde).




**Obr. 9.3 Proces pri ktorom sú nájdené ECM a EMM v transportnom toku**

Vyššie opísaný proces je vskutku veľmi schematický; podpora obsahujúca používateľský_kľúč (user_key) a reálnu implementáciu systému sa môže meniť od

jedného operátora k druhému. Detaily týchto systémov sú samozrejme, nie verejnou doménou, avšak ich princípy sú podobné.

## 9.5 Základné systémy podmieneného prístupu

Tab. 9.3 ukazuje hlavné systémy podmieneného prístupu (conditional access systems) používané Európskymi digitálnymi platenými TV poskytovateľmi služieb.

Množstvo týchto systémov využíva DVB-CSA šifrovací štandard špecifikovaný v DVB. Prijímač má interný dekodér riadený zabudovaným softvérom podmieneného prístupu, ktorý vypočítava dešifrovacie riadiace slová ECM správ a kľúčov obsiahnutých na predplatiteľskej inteligentnej karte (smart card) s platnými prístupovými právami obnovovanými EMM.

Systémy umožňujúce službu „plať-za-čo-pozeráš“ (pay-per-view) majú často druhý slot pre čítačku karty pre bankovú kartu ako aj modem k objednávke programov ako aj k platbám z bankového účtu.

**Tab. 9.3 Hlavné podmienené prístupové systémy**

| SYSTÉM | PÔVOD | POSKYTOVATELIA SLUŽIEB (PRÍKLADY) |
|---|---|---|
| Betacrypt | Betasearch (zastaralý) | Premiere World, German cable |
| Conax | Conax AS (Nórsko) | Scandinavian operators |
| CryptoWorks | Philips | Viacom, MTV Networks |
| IrDETO | Nethold | Multichoice |
| Mediaguard 1 & 2 | SECA (momentálne Kudelski S.A.) | Canal+, Canal Satellite, Top Up TV |
| Nagravision 1 & 2 | Kudelski S.S. | Dish Network, Premiere, German cable |
| Viaccess 1 & 2 | France Telecom | TPS, AB-Sat, SSR/SRG, Noos |
| Videoguard/ICAM | News Datacom (NDS) | BskyB, Sky Italia |

## 9.6 Zoznam použitej literatúry


[1] Andre Kudelski. Method for scrambling and unscrambling a video signal. United States Patent 5375168, 20 December 1994.

[2] Access control system for the MAC/packet family: EUROCRYPT. European Standard EN 50094, CENELEC, December 1992.

[3] Vincent Lenoir. EUROCRYPT, a successful conditional access system. IEEE Transactions on Consumer Electronics, 37(3):432-436, August 1991.

[4] Michael Cohen and Jonathan Hashkes. A system for controlling access to broadcast transmissions. European Patent Application 0 428 252 A2, 22 May 1991.

[5] Ross J. Anderson and Markus G. Kuhn. Tamper resistance - a cautionary note. In The Second USENIX Workshop on Electronic Commerce Proceedings, pages 1-11, Oakland, California, 18-21 November 1996.

[6] V. Mangulis. Security of a popular scrambling scheme for TV pictures. RCA Review, 41(3):423-432, September 1980.

[7] D. Raychaudhuri and L. Schi_. Unauthorized descrambling of a random line inversion scrambled TV signal. IEEE Transactions on Communications, 31(6):816-821, June 1983.