Čečenské dráhy

Analýza kódu na jízdenkách

šachy

sachy@s0c4.net

Současná podoba jízdenek

České dráhy OT75 0198

1154 *0831-761 OT0198 UPOK001178

15.05.16 [illegible] 00000

Obyčejná Osob: 1 Třída: 2

zpáteční Km: 26

Z: Veselí n. Lužnicí

Do: Jindřichův Hradec

Přes: Doňov

Platí od: 15.05.16

do: 16.05.16

Jízdu nutno nastoupit 1.den platn.

Sazba DPH 15%

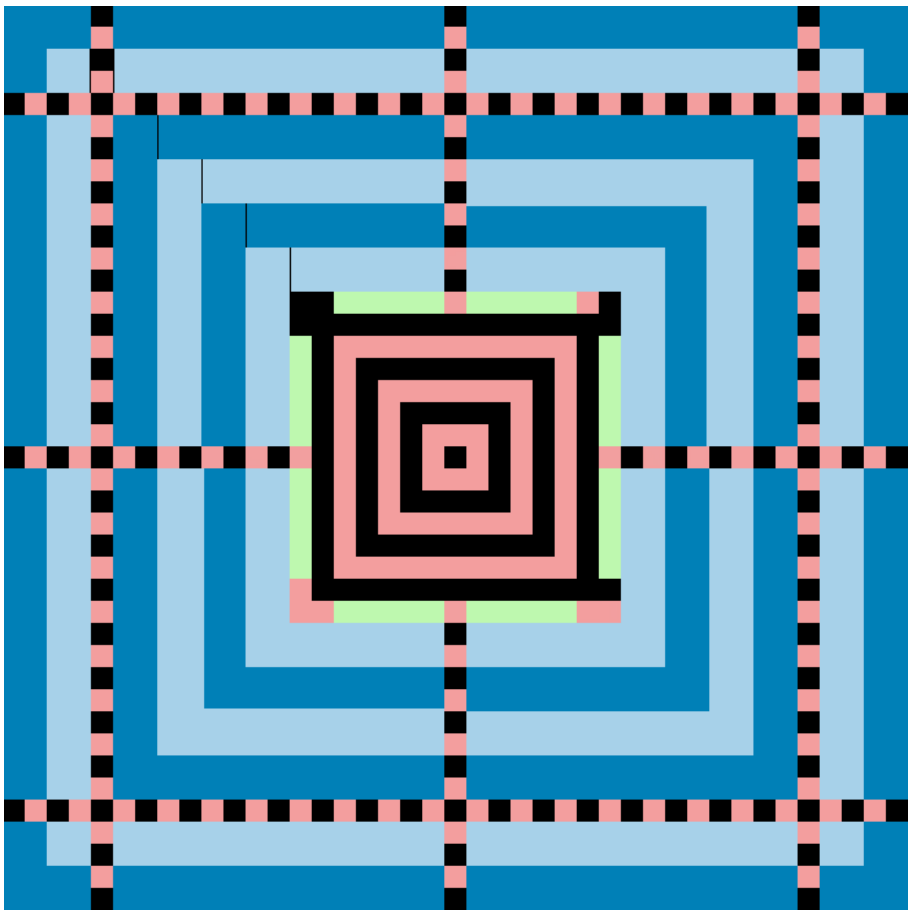
ZDD: 62581/10089

Cena: Kč 84,-

Hotově

ČD 0735 2 4113

ISO/IEC 24778:2008 (Aztécký kód)[1]



Pevně definované bity
Struktury
Nastavení (velikost, mod)
Data + Reed-Solomon
Začátek dvojřádku

Jízdenka 0033_0010

České dráhy používají od roku 2012

Data na jízdence

Binární blob proměnlivé délky (okolo 96B)
Nešifrované údaje

```
23434430 31C2830E 29C39BC2 9A040000
11C2B10C 00C29129 C3A4C2B8 2EC381C3
A440C2B4 44530006 150A2500 00000000
20C381C3 A4400000 000040C3 81C3A440
10C28553 003AC288 53000100 000000C3
90200000 0A
```

Data na jízdence

Zvýrazněné prvky (viz další slajd)
Fixní pořadí, proměnlivé offsety

```
23434430 31C2830E 29C39BC2 9A040000
11C2B10C 00C29129 C3A4C2B8 2EC381C3
A440C2B4 44530006 150A2500 00000000
20C381C3 A4400000 000040C3 81C3A440
10C28553 003AC288 53000100 000000C3
90200000 0A
```

Význam některých struktur

2343443031 - "#CD01"- identifikátor dopravce
9A040000 - datum + 2B 0x00
C381 - kontrolní součet, vždy před oddělovačem
C3A440 - globálně konstantní oddělovač (3x)
C2B44453 - ID Prodejní stanice (=Praha hl.n.)
10C28553 - ID Odkud (=Veselí nad Lužnicí)
3AC28853 - ID Kam (=Jindřichův Hradec)
XXXXXXXX - neznámý význam a padding

Nedekódované údaje

- Datum a čas (částečně)
- ID jízdenky, pokladny/pokladní, jízdenkové řady
- Počet osob
- Slevy (IN25/50/100, studentská, zpáteční,...)
- Extra (kolo, pes, místenka,...)

Nejisté údaje

Možná to v kódu uložené je, možná ne

- Kilometráž
- Cena
- Trať (Praha – Č. Budějovice přes Tábor/Písek)

Jízdenka z webu ČD

Při online nákupu si lze vytisknout jízdenku doma

Kod je mnohem obsáhlejší a NEdodržuje výše popsanou strukturu
Obsahuje navíc údaje o přepravovaném:

- Jméno Příjmení
- ID dokladu (OP, pas, řidičák, zbroják)
- Číslo vlaku, trať
- Kontroluje se online (sync DB každých pár minut)

Pravděpodobně šifrováno (ÚOOÚ)?

Zdroje

Databáze (SQLite) jízdenek a scripty okolo:
`http://brmcd.s0c4.net/`

[1] `https://upload.wikimedia.org/wikipedia/commons/1/1a/Aztec_Code_Scheme.png`