

ZABEZPEČENIE DÁT POMOCOU 16/32-BITOVÉHO KÓDU CRC

Juraj Ondrej Dúbrava
FIT VUT 2017/2018

- 3 spôsoby zabezpečenia dát
 - ▣ HW CRC modulom
 - ▣ Pomocou CRC tabuľky
 - ▣ Základným algoritmom výpočtu CRC hodnoty
- Zabezpečované dáta – náhodne vygenerovaný reťazec dĺžky 512 bajtov

Implementácia

- 16 a 32-bitová varianta CRC
 - ▣ 16-bit – použitý polynóm 0x8005
 - ▣ 32-bit – použitý polynóm 0x04C11DB7.
- HW CRC modul
 - ▣ Počiatočná hodnota 0 pri 16 aj 32-bit
 - ▣ Nezrkadlenie vstupu ani výstupu
 - ▣ Vhodný pri častom počítaní CRC hodnoty
- Výpočet s CRC tabuľkou
 - ▣ SW riešenie
 - ▣ Dynamické vygenerovanie CRC tabuľky pre 16 aj 32-bit s 256 hodnotami
 - ▣ Výpočet CRC použitím tabuľky

□ Základný algoritmus CRC

▣ SW riešenie

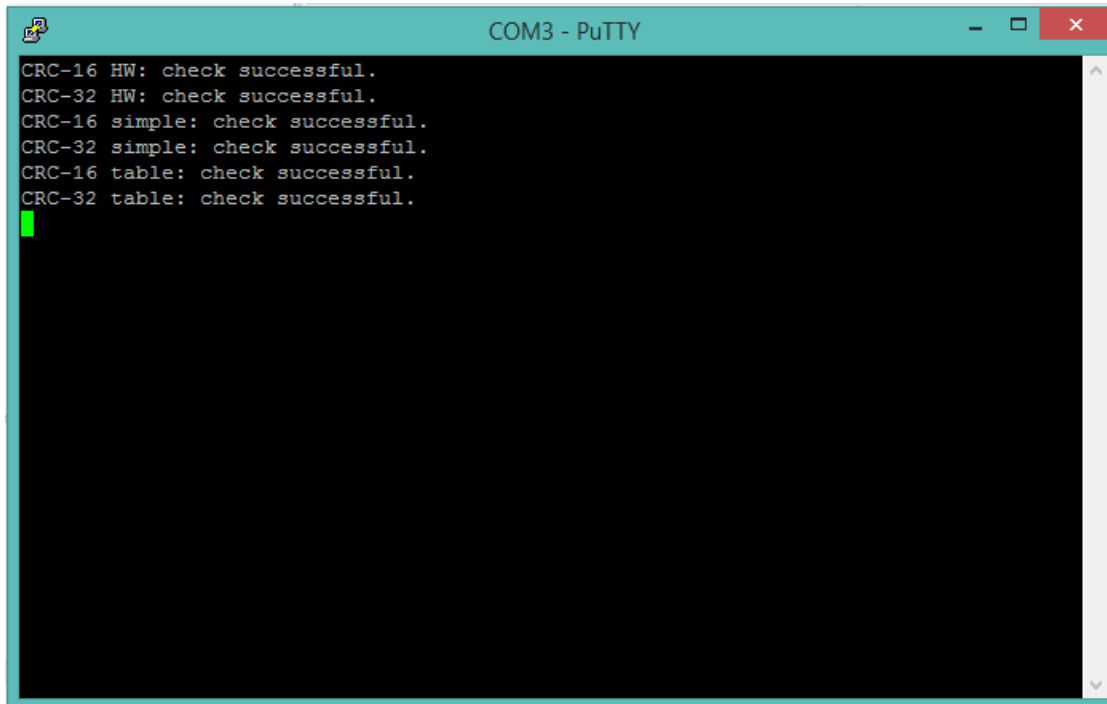
▣ Výpočet CRC hodnoty, spracovanie po bajtoch

□ Overenie správnosti

▣ Porovnanie vypočítaných CRC hodnôt pre vstupné dáta s predpočítanou hodnotou CRC pre dané vstupné dáta

▣ Hlásenie úspechu alebo neúspechu kontroly

- Výstup informácií o správnosti zabezpečených dát
 - ▣ využitie modulu UART (polling)
 - ▣ Výstup na terminál pomocou aplikácie PuTTY



A screenshot of a PuTTY terminal window titled "COM3 - PuTTY". The window has a teal header bar with standard window controls (minimize, maximize, close) on the right. The main area is black with white text. The text shows a series of successful CRC checks: "CRC-16 HW: check successful.", "CRC-32 HW: check successful.", "CRC-16 simple: check successful.", "CRC-32 simple: check successful.", "CRC-16 table: check successful.", and "CRC-32 table: check successful.". A green cursor is visible on the line following the last message. A vertical scrollbar is on the right side of the terminal area.

```
COM3 - PuTTY
CRC-16 HW: check successful.
CRC-32 HW: check successful.
CRC-16 simple: check successful.
CRC-32 simple: check successful.
CRC-16 table: check successful.
CRC-32 table: check successful.
█
```

- Najrýchlejšia varianta zabezpečenia – HW CRC modul
- Pomalší spôsob – CRC tabuľka, zrýchlenie základného algoritmu, rôzne veľké tabuľky
- Čím dlhšia hodnota CRC, tým lepšie
- Pravdepodobnosť neidentifikovania chyby s počtom použitých bitov klesá
 - ▣ CRC16 - $1/2^{16}$
 - ▣ CRC32 - $1/2^{32}$