VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Semestrální práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Jakub Jedlička ***ID:*** 198597
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Šifrátor pro hardwarově omezené zařízení

POKYNY PRO VYPRACOVÁNÍ:

V rámci práce se student seznámí s hardwarovou akcelerací založené na platformě FPGA. Seznamte se s programovacím jazykem VHDL, FPGA obvody řady Zynq-7000 a platformou Xilinx Vivado. Nastudujte šifrovací algoritmy určené pro lehkou kryptografii. Následně šifru popište jazykem VHDL, odsimulujte a implementujte na hardwarovém zařízení FPGA s omezenými hardwarovými zdroji.
Výstupem semestrální práce je návrh šifrování v prostředí Vivado a funkční simulace ověřující správnou funkčnost návrhu.
V navazující bakalářské práci věnujte pozornost konkrétnímu FPGA obvodu s čipem Artix s omezenými hardwarovými zdroji a zprovozněte šifrátor na reálním zařízení. Úkolem bude také zprovoznění jednotlivých periferií komunikující s FPGA obvodem Artix (komunikace pomocí rozhraní USB 2.0, Micro SD, Ethernet, a jiné).

DOPORUČENÁ LITERATURA:

[1] BURDA, Karel. Aplikovaná kryptografie. Brno: VUTIUM, 2013. ISBN 978-80-214-4612-0.

[2] PINKER, Jiří, Martin POUPA. Číslicové systémy a jazyk VHDL. 1. vyd. Praha: BEN - technická literatura, 2006, 349 s. ISBN 80-7300-198-5.

Termín zadání: 2.10.2020 ***Termín odevzdání:*** 11.12.2020

Vedoucí práce: Ing. David Smékal

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu