

## I. IDENTIFIKAČNÍ ÚDAJE

<b>Název práce:</b>	<b>Modernizace systému pro generování individuálních šifrových textů</b>
<b>Jméno autora:</b>	<b>Miroslav Smutný</b>
<b>Typ práce:</b>	bakalářská
<b>Fakulta/ústav:</b>	Fakulta elektrotechnická (FEL)
<b>Katedra/ústav:</b>	Katedra radioelektroniky
<b>Oponent práce:</b>	Ing. Pavel Bezpalec, Ph.D.
<b>Pracoviště opONENTA práce:</b>	Katedra telekomunikační techniky

## II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

<b>Zadání</b>	<b>náročnější</b>
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
Rozsah zadání směřuje k náročnější realizaci.	

<b>Splnění zadání</b>	<b>splněno</b>
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.</i>	
Práce ve všech bodech splňuje zadání.	

<b>Zvolený postup řešení</b>	<b>správný</b>
<i>Posuďte, zda student zvolil správný postup nebo metody řešení.</i>	
Studentem zvolený postup řešení je správný.	

<b>Odborná úroveň</b>	<b>A - výborně</b>
<i>Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.</i>	
Student skloubil teoretické znalost kryptografie a programování v praktické realizaci programového produktu.	

<b>Formální a jazyková úroveň, rozsah práce</b>	<b>A - výborně</b>
<i>Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.</i>	
Typograficky i formálně je práce na výborné úrovni.	

<b>Výběr zdrojů, korektnost citací</b>	<b>A - výborně</b>
<i>Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.</i>	
Výběr studijních pramenů je dobrý, použití v práci je řádně zaznamenáno v souladu se zvyklostmi.	

<b>Další komentáře a hodnocení</b>
<i>Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.</i>
Vložte komentář (nepovinné hodnocení).

### III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

*Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.*

Student ve své práci aktualizoval stávající programový systém pro generování jednoduchých šifrových úloh a obohatil jej o vlastní implementace algoritmu pro moderní asymetrické šifrování. Programový celek velmi podrobně zdokumentoval. Prokázal výbornou znalost kryptografických systémů stejně jako vysokou znalost moderních programovacích technik.

Předloženou závěrečnou práci **doporučuji** k obhajobě a hodnotím ji klasifikačním stupněm **A - výborně**.

#### Otázky k obhajobě:

1. Popište stručně principiální rozdíly mezi šiframi Rijndael a Baby Rijndael.
2. Odhadněte, jaké úpravy vašeho kódu by byly potřeba pro implementaci šifry Rijndael.

Datum: 13.6.2016

Podpis: