Název práce: Konstrukce a kryptoanalýza AES
(Advanced Encyption Standard)
Autor: Jan Říha
Katedra: Katedra Algebry
Vedoucí bakalářské práce: Doc. RNDr. Jiří Tůma, DrSc.
E-mail vedoucího bakalářské práce: Jiri.Tuma@mff.cuni.cz

Abstrakt: V předložené práci studujeme nejnovější symetrickou blokovou šifru AES. Nejprve se zabýváme vývojem a vznikem šifry od vypsání soutěže až po vyhlášení vítězného kandidáta. Poté se věnujeme její konstrukci, ve které se využívá některých netriviálních poznatků algebry při práci s polynomy nad konečným tělesem. V této kapitole je též popsána přímá inverzní šifra a ekvivalentní inverzní šifra sloužící k dešifrování zašifrovaných dat. Ve třetí kapitole zkoumáme navrhované implementace šifry AES na jednotlivé platformy a nakonec rozebíráme možné útoky a odolnost šifry AES vůči nim.

Klíčová slova: AES, šifra, implementace, kryptoanalýza

Title: The design and cryptanalysis of the AES
(Advanced Encyption Standard)
Autor: Jan Říha
Department: Department of Algebra
Supervisor: Doc. RNDr. Jiří Tůma, DrSc.
Supervisor's e-mail address: Jiri.Tuma@mff.cuni.cz

Abstract: In the present work we study the newest symetric block cipher AES. At first we consider development and creation of the cipher from the start of selection proces till announcement of winning candidate. Then we turn to its design, in which we use some non-trivial algebraic knowledge at work with polynomials with coefficients in finite field. In this chapter there is also described straightforward inverse cipher and equivalent inverse cipher make for decryption of encrypted dates. In chapter three we investigate proposed implementations of the cipher AES on individual platforms and in the end we analyse posible attacks and how the cipher AES is resistant against them.

Key words: AES, cipher, implementation, cryptoanalysis