

# **Description - Rypto**

## **March 29, 2017**

**Table of Contents**

Preface..... 2

Algorithms and data structures..... 2

Problem to be solved..... 2

Input..... 2

Performance..... 2

# Preface

"Tietorakenteet ja algoritmit" – exercise.

Rypto is a software, which can encrypt and decrypt.

## Algorithms and data structures

Software implements AES-algorithm[FIPS197] with 128 bit keys in ECB mode, using the C programming language.

Implementation covers encryption and decryption.

The data structures implemented are those that are described in the standard:

- Round Keys (1-dimensional array derived from Cipher Key) and
- State (2-dimensional array).

In addition, files are used as input and output. Cipher Key is given from the command line among other parameters.

## Problem to be solved

The problem is to encrypt Plaintext to Ciphertext and vice versa. AES is widely used encryption algorithm which is believed to be secure[WIKI000].

## Input

The following input is given to the software:

- Mode of operation, e.g. encrypt or decrypt
- 128 bit Cipher Key as a hex number (32 hex digits)
- Source file to be read
- Destination file to be written

## Performance

Space efficiency: Used space is constant.

Time efficiency:  $O(N)$

## References

FIPS197: U.S. Department of Commerce/National Institute of Standards and Technology, Federal Information Processing Standard, FIPS PUB 197 Advanced Encryption Standard (AES), 2001

WIKI000: Wikipedia, Advanced Encryption Standard, 2017,  
[https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)