# Implementation - Rypto
# March 29, 2017

# Table of Contents

# Preface

"Tietorakenteet ja algoritmit" – excercise.

Rypto is a software, which can encrypt and decrypt.

# General structure

Software is comprised of the following main components:

- Library aes – all of the AES-related functionality
- Executable rypto – user interface
- Test cases – CUnit format

## Library aes

In the library, the helper functions are also visible to facilitate unit testing. All exported symbols begin with AES_ .

The source code of the library is in two files: aes.c and aes.h.

If the library is used in a source file, then file aes.h must be included.

The constants (like AES_S_Box array) were extracted from[FIPS197], unless otherwise mentioned.

The Galois multiplication table AES_g_m was extracted from[WIKI001].

### Types

Two types are defined:

- AES_byte (8-bit unsigned integer)
- AES_word (32-bit unsigned integer)

### Functions

void AES_KeyExpansion(AES_byte *key, AES_word *w) – expands a given key (128 bits, 16 bytes) to an AES Key Schedule (11 x 4 words). Must be done before encryption or decryption.

# Performance

Space efficiency: Used space is constant.

Time efficiency: O(N)

# Missing features, possible new features

Other key sizes than 128. Other operation modes besides ECB.

# 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

WIKI001: Wikipedia, Rijndael mix columns, 2017, https://en.wikipedia.org/wiki/Rijndael_mix_columns