# Testing - Rypto
# March 28, 2017

# Table of Contents

# Preface

"Tietorakenteet ja algoritmit" – excercise.

Rypto is a software, which can encrypt and decrypt.

# Testing arrangements

Unit testing is done with CUnit framework and gradle.

High-level tests are implemented with a shell script.

# Test cases

## AES_makeword

The  makeword test case is: 0x01, 0x02, 0x03, 0x04 → 0x01020304.

## AES_RotWord, AES_SubWord

The RotWord and SubWord test cases were extracted from the standard, pp. 27, first line of the table.

## AES_KeyExpansion

The three Key Schedule test cases were obtained from Sam Trenholme's web site http://www.samiam.org/key-schedule.html .

Selected test cases were the following:

- A key with all bits zero.
- A key with all bits one.
- A key with all bytes different.

# AES_AddRoundKey, AES_SubBytes, AES_ShiftRows

Test cases were taken from the standard, pp. 33, first possible cases.

# How to repeat tests

Say

```
cradle build
```

from the command line

# Test results