Testing - Rypto
April 11, 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.

Higher-level tests are implemented as a shell script.

Test cases

Unit tests

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[FIPS197], pp. 27, first line of the table.

AES_KeyExpansion

The three Key Schedule test cases were obtained from[SAMIAM].

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, AES_MixColumns

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

AES_Inv*

Test cases were generated from standard version test cases by inverting input and output.

AES_encrypt, AES_decrypt

Test cases were taken from the standard, pp. 35-

Integration tests

Performance tests

How to repeat tests

Unit tests

The static libcunit.a must be linked to directory libs/ in the project root for tests to run.

Say

```
cradle build
```

from the command line.

Integration tests

Integration tests are located on directory tests/.

Performance tests

Performance tests are located on directory tests/.

Test results

Unit tests

Unit tests – passed on both development machine (Mac OS X) and melkki (Ubuntu Linux).

Integration tests

Performance tests

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
SAMIAM: Trenholme, Sam, Rijndael's key schedule, 2016, http://www.samiam.org/key-schedule.html