Manual - Rypto
April 27, 2017

Table of Contents

Preface

"Tietorakenteet ja algoritmit" – excercise.

Rypto is a software, which can encrypt and decrypt.

Operation

Rypto encrypts or decrypts files with 128-bit AES in ECB mode. The encrypted data is padded according PKCS#7. Padding is removed upon decryption. Thus, encrypting and decrypting a file with the same key will produce the identical file.

How to execute

Encryption

To encrypt, execute the command

```
rypto e <key> <source> <destination>
```

Where

- <key> is encryption key, 32 hex digits (128 bits)
- <source> is the (plaintext) file to be encrypted
- <destination> is the encrypted file

Decryption

To decrypt, execute the command

```
rypto d <key> <source> <destination>
```

Where

- <key> is encryption key, 32 hex digits (128 bits)
- <source> is the (ciphertext) file to be decrypted
- <destination> is the decrypted file

Input to the software

Software takes as input the following:

- Operation mode: Encrypt or decrypt
- Key
- Source file to be read
- Destination file to be written

Source and destination files must be actual files, pipes or the like (stdin or stdout) cannot be used.

Location of the executable and test data

Executable is in file build/exe/rypto/passing/rypto.

Tests are documented on separate "Testing" document.