

Weekly report 2

Total working hours - 8.

Tasks completed:

- Started rest of the documents – Implementation.pdf, Manual.pdf, Testing.pdf.
- Environment and the tool chain (CUnit, gradle) working. First live test case passed.
- Helper functions AES_makeword, AES_SubWord, AES_RotWord; test cases, unit tests.
- AES_KeyExpansion – function, test cases, unit test.

Progress on the software:

- Key Schedule (AES_KeyExpansion) implemented and unit tested.

Learned:

- C programming is coming back to me. Bitwise stuff is hairy but strangely rewarding.

Unclear / problems:

- None, for now.

Next:

- Encryption helper functions and unit testing of those.