Weekly report 3

Total working hours - 8.

Tasks completed:

- Helper functions AES_AddRoundKey, AES_SubBytes, AES_ShiftRows, AES_MixColumns; test cases, unit tests.

- Galois tables imported to the code.

- Inverse S-box imported to the code.

Progress on the software:

- Cipher helper functions AddRoundKey, SubBytes, ShiftRows, MixColumns implemented and unit tested.

Learned:

- Debugging.

- Standard contains ample material for unit test cases. Very easy to debug and implement.

Unclear / problems:

- None, for now.

Next:

- Encryption main function and unit testing.

- Decryption helper functions and unit testing.

- Decryption main function and unit testing.