



Computer Security – CMPS 485 L01

Project Preproposal

Instructor : Dr. Ryan Riley

Students	: Mohammed Amaan Johar Sheikh	- 201205380
	: Babikr Elnimah	- 201204005
	: Ahmed Ibrahim	- 201204361

Date of Submission : 31 March 2016

1. Detailed evaluation of the DES encryption algorithm, looking into its history and the technique used to build it. Analysis of the cracks that were generated for this encryption algorithm and how they were avoided in later encryption systems. **(Depth)**
Implementation of the DES encryption algorithm on ARMSim in assembly language of the ARM7 Microprocessor. **(Implementation)**
2. Detailed evaluation of encryption algorithms and hash functions for embedded systems. **(Breath)** Implementation of the TEA, XTEA, and RC4 algorithms on ARMSim in assembly language of the ARM7 Microprocessor. **(Implementation)**