A Lightweight Encrypted Access Control System

Stuart Miller
Department of Electrical and
Computer Engineering
Missouri University of Science & Technology
Rolla, Missouri 65401
Email: sm67c@mst.edu
Web: http://web.mst.edu/~sm67c

***Abstract*—The Data Encryption Standard (DES) block cypher algorithm is a vital piece of computing history. Although DES is no longer considered to be secure, an analysis of the need for and means of implementing DES proves to be an insightful lesson in the need for it's successors. In particular, this paper will focus on the implementation of DES on an 8051 microcontroller, an 8-bit platform that was common when the algorithm was designed. DES proves highly applicable to 8-bit programming methodologies and is easily computed on such a low-power platform. Throughout the following design of an access-control system, protected with DES encryption, such benefits will be enumerated.**

I. Introduction

Intro stuff.

II. About DES

Brief backgroud on DES and why is is applicable to 8-bit platforms like the 8051.

III. Program Structure

Overview of code structure. Note on encryption vs. decryption.

IV. Test Results

Examples of encryption and decryption. Verification of algorithm

V. Product Design

Connecting to 8051 to external I/O. Probably will use and LCD and some buttons. Maybe 3D print a housing for a keypad-type thing or perhaps buy one off Digikey. Need to get on that soon.

VI. Physical Security

Followup to the external I/O and brief discussion of how encryption is rendered useless if individual buttons can be intercepted or modified. Discussion of the applicability of this as system an intermediary between an access control panel and a host system.

VII. Conclusion

VIII. test

My intro... blah blah [**?**].