Table of contents

Project Management Plan

Proposal and reference implementation of a new symmetric cipher algorithm

http://amberj.devio.us/projects/crypto/

Master of Computer Applications
Semester VIII
Session Jan – May, 2011

Under the guidance of
Mrs. Yasmin Sheikh

Submitted By
Amber Jain
Roll number: IC-2K7-05

International Institute of Professional Studies
Devi Ahilya Vishwavidyalaya, Indore, M.P.
2011

Revisions

Project Management Plan

S. No.	Description	Revision Number	Changes
1	Project Management Plan	1	Initial document.

1. INTRODUCTION

1.1. Project Overview

This project titled "*Proposal and reference implementation of a new symmetric cipher algorithm*" (http://amberj.devio.us/projects/crypto/) includes the study of design guidelines and desired properties of symmetric cryptographic algorithms. I'll then propose a new symmetric cipher algorithm based on my study. I'll also provide a reference implementation of the proposed algorithm in Python 3 programming language and test vectors for the proposed algorithm. I'll place the proposed algorithm in public domain and it will be unpatented in all countries. Anyone would freely be able to use the algorithm. The specification, source code and test data for the proposed algorithm would be available to anyone wishing to implement the algorithm, in accordance with country specific export laws.

1.2. Budget Summary

Since this is a research and academic project, there are no budget requirements.

1.3. Project Deliverables

- Project Management Plan.
- A report outlining the desirable design guidelines and specification of proposed algorithm.
- Reference implementation of proposed algorithm.
- Test vectors

2. PROJECT ORGANIZATION

2.1. Research Process Models

I'll follow the following *model for this research project:*

- Identify research topic (or algorithm).
- Study the existing publications about the various algorithms.
- Propose the new algorithm
- Implement the proposed algorithm.

- Release the algorithm specification and source code in public domain for public cryptanalysis

2.2. Roles and Responsibilities

Amber Jain will be responsible for all the activities related to this project.

2.3. Tools and Techniques

The reference implementation will be in Python 3 programming language (and will execute on any system python interpreter has been ported to). The portability of other software implementations will depend on portability of choice of programming language.

The algorithm will be efficiently implementable in custom (special purpose) VLSI hardware as well as on general purpose large, medium and small sized processors (for e.g. microprocessors, microcontrollers and smart cards respectively).

3. PROJECT MANAGEMENT PLAN

3.1. Tasks

3.1.1. Description

Task Title	Task Description	Task Sequence Number
Identify research topic	Identify the possible research topic and do the initial brainstorming.	1
Existing possibilities	Lookup existing possibilities on Internet and other sources of information so as not to reinvent the wheel.	2
Study of existing symmetric cipher algorithms	Study various existing symmetric cipher algorithms and note down	3

	the design guidelines used in these algorithms.	
Propose a new algorithm	Proposal of a new symmetric cipher algorithm and test vectors for it.	4
Implementation of proposed algorithm	Implementation of the proposed algorithm in Python 3 programming language.	5
Cryptanalysis	Careful cryptanalysis (as well as modifications and improvements) of the proposed algorithm by public.	6

3.1.2. **Deliverables and Milestones**

Milestone Title	**Milestone Description**	**Milestone Date**
Study of existing algorithms	Study various existing symmetric cipher algorithms and note down the design guidelines used in these algorithms.	20 February – 20 March, 2011
Proposal of new symmetric cipher algorithms	Proposal of a new symmetric cipher algorithm and test vectors for it.	20-28 March 2011
Implementation of proposed algorithm	Implementation of the proposed algorithm in Python 3 programming language.	25 March – 4 April 2011
Report submission and final presentation	Submission of project report and presentation.	5 April – 15 April 2011
Public cryptanalysis	Careful cryptanalysis (as	After 4 April, 2011

	well as modifications and improvements) of the proposed algorithm by public.	

3.1.3. **Resources Needed**

This project will use resources in the form of time and effort that I shall spend developing the project deliverables.

- Budget Allocation: None.

3.1.4. Dependencies and Constraints

- Project Constraints: None.
- Critical Project Barriers: None.

3.1.5. Risks and Contingencies

The specification, source code and test data for the proposed algorithm would be available to use only in accordance with country specific export laws. The same applies to study of the existing algorithms.

3.2. Time Table

Figure 1: Gantt chart

Today's Date: 2/23/2011 (Wed)

Start Date: 2/19/2011 (Sat)
End Date: 4/15/2011 (Fri)

WBS	Tasks	Start	End	Duration (Days)	% Complete	Days Complete	Days Remaining
1	Study of existing algorithms	2/19/11	3/20/11	30		13	17
2	Proposal of new algorithm	3/20/11	3/28/11	10	0%	0	10
3	Reference implementation of proposed algorithm	3/25/11	4/4/11	6	0%	0	6
5	Report preparation and submission	4/05/11	4/12/11	8	0%	0	8
6	Final Presentation	4/12/11	4/15/11	4	0%	0	4
7	Modifications, improvements and cryptananlysis.	04/16/11	-	-	-	-	-