## A PROJECT REPORT

## ON

**ENHANCING CRYPTOGRAPHIC ALGORITHMS BY GENERATING STRENGTHENED KEYS**

## submitted in partial fulfillment for the requirement of award of

## BACHELOR OF TECHNOLOGY

## In

## INFORMATION AND COMMUNICATION TECHNOLOGY

**Submitted By**

**P SRAVAN KUMAR**

**113014125**

**M SUDHAKAR RAJ**

**113014131**



**Under the Guidance of**

**Mr. G. MANIKANDAN**

**ASSISTANT PROFESSOR**

**DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY**

**SCHOOL OF COMPUTING**

**SHANMUGHA**

**ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY**

## (SASTRA UNIVERSITY)

**(A University Established under section 3 of the UGC Act, 1956)**

**TIRUMALAISAMUDRAM**

**THANJAVUR – 613401**

**APRIL-2013**

## SHANMUGHA

## ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY

## (SASTRA UNIVERSITY)

(**A University Established under section 3 of the UGC Act, 1956**)

## TIRUMALAISAMUDRAM THANJAVUR– 613401



SCHOOL OF COMPUTING

# BONAFIDE CERTIFICATE

**This is to certify that the project entitled**

**ENHANCING CRYPTOGRAPHIC ALGORITHMS BY GENERATING STRENGTHENED KEYS**

is a work done by

**P SRAVAN KUMAR**

**113014125**

**M SUDHAKAR RAJ**

**113014131**

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION AND COMMUNICATION TECHNOLOGY**

**OF SASTRA UNIVERSITY, Thanjavur during the year 2012-2013**

**Internal Guide Associate Dean (ICT)**

**G. Manikandan Dr. K.S.Ravichandran**

**Submitted for the university examination held on:**

**Internal Examiner External Examiner**

**ACKNOWLEDGEMENT**

First and Foremost, I take pride in thanking the **Almighty** who gave us strength for the successful completion of this project.

I would forever remain grateful to **Prof. R. Sethuraman, Vice Chancellor** and

**Dr.G. Bhalachandran, Registrar,** SASTRA UNIVERSITY, for giving me an opportunity to do this project.

I am extremely thankful to my dignified **Dr. P.Swaminathan, Dean School of computing and Dr. K.S. Ravichandran, Associate Dean, Department of ICT,** for inspiring and motivating me to bring out a perfect and successful project work.

I am highly grateful and express my earnest and humble thanks to my project internal guide **Mr**. **G.Manikandan**, **Assistant Professor, Department of ICT** for his timely help, valuable suggestion, guidance and moral support throughout my project work.

I also thank all the **Teaching staff, Non-teaching staff,** and those who have directly or indirectly helped me by extending their moral support and encouragement for completion of this project.

Last but not the least, I take immense pleasure in thanking my **Parents and Friends** who were a constant source of encouragement and inspiration and provided their cooperation to enable me to complete this project to the fullest satisfaction.

**SYNOPSIS**

Cryptography is the process of writing a secret code that is only known to the targetted users leaving the third parties with no clue what the code is about. The need for cryptographic algorithm is to protect the sensitive data from unauthorized usage. Considering communication between applications, there are some specific security speculations such as authentication, privacy/confidentiality, integrity, non-repudiation. In order to meet the above speculations, various cryptographic algorithms are being used.

The existing system comprises of a black box technique for generating a new complex key from the key provided initially by the user. The new complex key thus obtained is hard to crack because of the complex black box design. In general black box may be of anything which has a set of confused and diffused mathematical formulas.

In this project we introduce a new black box technique for generating a complex key from the user given key. The new key is very hard to crack by the intruders because of the complexity in our proposed black box design. Here we use the Magic Square concept for designing the black box. The objective of our project is to improve the effectiveness of any cryptographic algorithm by generating a strong key. Since the new key is generated dynamically and randomly after the input of the user’s key, it is difficult for the intruders and the eve-droppers to crack the system.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **S.NO** | **Content** | **Page No** |
| 1 | Introduction | 1 |
| 2 | Software Project Plan | 4 |
| 3 | Software Requirement Specification | 8 |
| 4 | System Analysis | 11 |
| 5 | System Design | 14 |
| 6 | Coding | 25 |
| 7 | Implementation | 49 |
| 8 | Future Scope | 51 |
| 9 | References | 53 |