

ENCRYPTED CHEQUE VERIFICATION (SAFE CHEQUE)

Project report is presented in partial fulfillment for the award of the
Bachelor of Electrical Engineering (Honours)
UNIVERSITI TEKNOLOGI MARA



**SHAIFUL NIZAM RAZALI
B. ENG (Hons.) ELECTRICAL
Faculty of Electrical Engineering
UNIVERSITI TEKNOLOGI MARA (UiTM)
40450 SHAH ALAM, SELANGOR DARUL EHSAN
MALAYSIA**

OCTOBER 2004

ACKNOWLEDGEMENTS

All praises be to Allah, Lord of the Universe, the Most Merciful who gives strength and ability to complete this thesis and Beneficent to Prophet Mohammad S.A.W on the members of his family and his companions.

First, I would like to special appreciation to my supervisor, Pn. Rosidah Sam and Prof Ir. Dr. Shah Rizam Mohd. Shah Baki, lecturers who devoted their time in giving me the guidance, suggestions, advices, support and positive ideas in helping me throughout the course of this project.

Secondly, I would like to express my thanks to my Visual Basic lecturer, Mr. Rosli Jusoh, for his understanding and consideration to share his knowledge to help me overcome a great obstacle to complete this project.

I am also indebted to Nasri, Rosfakarudin, Azlee and all my friends, together with whom I have shared the opinions, suggestions and constructive comments. To those that have contributed information, knowledge, ideas, time and effort.

And most important of all, to my mother and my family, for the supports and encouragement to produce the best work that I could.

Thank you.

ABSTRACT

The Safe Cheque system is designed as an anti fraud protection system. Providing security against 'external' fraud attacks such as attempts to amend sensitive financial details on printed cheque and against 'internal' fraud attacks where un-authorized personnel may attempt to make in-appropriate payments which could damage the credibility and finances of the organization they work within. This project also described an encrypted barcode system for the Safe Cheque, which includes the hardware and software development. The hardware includes the barcode scanner and a computer. The software developed using Visual Basic design and tests the Safe Cheque system.

TABLE OF CONTENTS

| | |
|---|------------|
| DECLARATION | i |
| ACKNOWLEDGEMENT | ii |
| ABSTRACT | iii |
| TABLE OF CONTENTS | iv |
| LIST OF FIGURES | vii |
| LIST OF TABLES | ix |
| ABBREVIATIONS | x |
| | |
| CHAPTER 1: INTRODUCTION | |
| 1.1 Safe Cheque | 1 |
| 1.2 Cryptosystems | 1 |
| 1.3 Barcode Technology | 2 |
| 1.4 Scope of Work | 4 |
| 1.5 Organization of Report | 5 |
| | |
| CHAPTER 2: CRYPTOGRAPHY: ENCRYPTIONS AND DECRYPTIONS | |
| 2.1 Cryptography | 6 |
| 2.1.1 Basic Terminology | 6 |
| 2.1.2 Basic Cryptography Algorithms | 8 |
| 2.1.3 Cryptographic Hash Functions | 9 |
| 2.1.4 Cryptographic Random Number Generators | 10 |
| 2.1.5 Strength of Cryptographic Algorithms | 11 |
| 2.2 Cryptography's Benefits, Limitations and Drawbacks | 13 |
| 2.3 Encryption and Decryption | 15 |

CHAPTER 1

INTRODUCTION

1.1 Safe Cheque

In today's world of technology and the unfortunate misuse of it, companies are left with the difficult task of making corporate procedures more secure and safer in the present climate of doing business.

Fraudulent cheque writing has become a profitable way of life for many criminals. Poor cheque cashing policies and carelessness increase the risk of loss. Information such as who the cheque is made out to, the amount and the date of the cheque are particularly vulnerable to fraudulent alteration and institutions that mass print cheque are at greatest risk.

The Safe Cheque range of products is an innovative breakthrough in radically reducing the risk of cheque fraud. The solutions are built around a set of fraud prevention core technologies. All the solutions are based on the encrypted two dimensional symbols which, once printed, cannot be copied or reproduced. The solutions include a cheque maintenance system, an accountability system based on biometrics, a cheque enquiry system as well as the establishing and logging of accountability at each stage of the life cycle of a cheque.

1.2 Cryptosystems

As we move into an information society, the technological means for global surveillance of millions of individual people are becoming available to major governments. Cryptography has become one of the main tools for privacy, trust, access control, electronic payments, corporate security, and countless other fields [1][14]. The use of cryptography is no longer a privilege reserved for