

# **NCP** Network Crypto Protocol(Design)

*Secure Way to Communicate*

By:

Imran Anawar

244002-05

MCS (Network and Communication) Fall 2000



Supervised by:

Mr. Jahanzeb Ahmad

*A report is submitted to Department of Computer Science,  
Bahria Institute of Management and Computer Science, Islamabad*

---

**Department of Computer Science**  
Bahria University Islamabad

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

## Abstract

There has always been a lot of mystique and media hype surrounding cryptography.

In distributed systems, objects are scattered to different places. This makes the security issues more difficult. Another problematic field in distributed systems security is authentication. The decision that should be made is whether the security should be enforced centrally or locally. In centralized security enforcement, there could be some kind of Key Distribution Center (KDC), where the keys of all the devices are stored. The Key Distribution Center acts as a Trusted Third Party (TTP) that users can use to authenticate themselves and other users, and to get secure connections everywhere in the network.

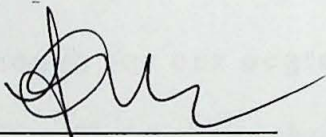
There could be a trusted Certification Authority (CA), which issues key certificates and a Certification Distribution Center (CDC), which stores all the certificates issued by the Certification Authority.

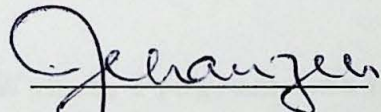
Our aim is to design and develop Symmetric Cryptographic system with KDC and CA Server.

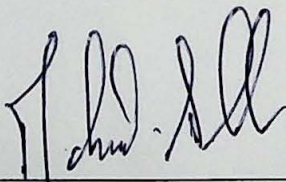
Acknowledgement

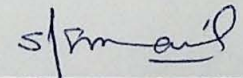
**Certificate**

We accept the work contained in this report as a confirming to the required standards for the partial fulfillments of the degree of MCS

  
\_\_\_\_\_  
Head of department

  
\_\_\_\_\_  
Supervisor

  
\_\_\_\_\_  
Internal Examiner

  
\_\_\_\_\_  
External Examiner

## Acknowledgement

All praise goes to Allah through whom all blessings flow. We are nothing without his blessings.

I would like to thank **Mr Jahanzeb Ahmed**, our project supervisor and Dr. MA Kahn for his helpful guidance and feedback during the development of this project. Many thanks to the professors who served on our project committee for examining it to be perfect enough for our degree requirement.

Special thanks go to Mr. Fazal-e-Wahab, Program Leader and all CS Teachers always encouraging throughout our academic career at Bahria Institute.

# Table of Contents

Abstract	i
Certificate	ii
Acknowledgement	iii
List of Figures	vii
List of Tables	viii

## **ChapterNo.1 INTRODUCTION 1**

### INTRODUCTION

1.1 Purpose of this project	1
1.2 Purpose of this document	1
1.3 Overview of this document	3
1.4 Existing Systems	4
1.4.1 Communication Patterns	4
1.5 TERMINOLGY	5
1.5.1 Messages and Encryption	5
1.5.2 Algorithms and keys	5
1.6 General Security Concerns	6

## **CHAPTER NO 2 CRYPTOGRAPY 9**

### INTRODUCTION 9

2.2 Types of cryptography	11
2.3 Trust models	14
2.3.1 Public-key certificates and CAs	14
2.3.2 PKI	16
2.3.3 Kerberos	17
2.3.4 PGP Web of Trust	20
2.4 Do you need cryptography	21

## **CHAPTER NO.3 DISTRIBUTED SYSTEM SECURITY 24**

### INTRODUCTION 24

3.2 Current Implementation	26
3.2.1 Single Sing-On	28
3.2.2 For end users	28
3.2.3 For operations	28
3.2.4 Security advantages	28
3.2.5 The problem	29
3.3 Basic Authentication	30
3.4 SSO within Windows 2000 Domains	32
3.4.1 Seamless Integration	34
3.5 Security Architecture for the Internet Protocol	35
3.5.1 What is IPsec	36

3.5.2 What IPsec Does	37
3.5.3 How IPsec Works	38
3.6 Security Research on Payment System on E-commerce network	40
3.6.1 What E-commerce	41
3.6.2 Safety problem of payment balance system of EC	42
3.7 MD5 arithmetic	44
3.8 Certificate Authority	45
3.9 Electronic Tag	46

## **CHAPTER NO.4 SYSTEM ANALYSIS** 48

### INTRODUCTION

4.1 System Requirements	48
4.2 Functional Requirements or System Functions	51
4.2.1 Basic Functions	52
4.3 Non Functional Requirements or System Attributes	55

## **CHAPTER NO.5 DESIGN CONSIDERATIONS** 57

### INTRODUCTION

5.1 Algorithms to be used	57
5.2 DES(Data Encryption Standard)	57
5.2.1 The Initial Permutation	60
5.2.2 The Key Transformation	60
5.2.3 The Expansion Permutation	61
5.2.4 The S-Box Substitution	62
5.2.5 The P-Box Permutation	64
5.2.6 The Final Permutation	65
5.3 MD5	66
5.4 SYSTEM DESIGN	69
5.4.2 Major Modules	69
5.4.2 Sub Modules	70
5.5 Real Use Cases	77
5.5.1 Register Member	78
5.5.2 Login	79
5.5.3 Send Message	80

# CHAPTER NO 6 STEP BY STEP WORKING

83

## INTRODUCTION

6.1 STEP BY STEP WORKING	83
6.2 Protocols	83
6.3 User Define Protocol	85
6.3.1 Registration	85
6.3.2 Get Session Key	85
6.3.3 Request for the other User Key	85
6.4 Registration Process	89
6.5 Session Key Process	89
6.6 Get Other's Key Process	91

## References

96



## List of Figures

<b>Fig No</b>	<b>Description</b>	<b>Page No</b>
1.1	Illustrates the cryptography	5
2.1	Illustrates the types of cryptography	13
2.2	Illustrates how Kerbero	18
3.1	Illustrates Single Sign Ons works	27
3.2	Single sign-on uses certificate-based authentication	30
3.3	Using a password to authenticate a client to a server	31
3.4	Illustrates how SSO works in Windows 2000 domain	33
3.5	Illustrates the Relationship between element of EC	44
4.1	Illustrate Communication between client A & B	50
4.2	Illustrates administrative client	50
5.1	Illustrates One round of DES.	59
5.2	Illustrates MD5 main loop.	67
5.3	Illustrates the System architecture	69
6.1	User Datagram Header Format	84
6.2	Illustrates the Registering procedure of Client	88
6.3	Illustrates providing session key to user	90
6.4	User Password Get Method	92
6.5	Client Request Process	93
6.6	Server Process	94
6.7	Server Work Diagram	95

## List of Tables

Table No	Description	Page No
4.1	Shows Function category and their meaning	51
4.2	Show Basic function including name description and category	52
4.3	Shows Details and boundary constraints of attribute	56
5.1	Shows Crypto System-Secure Communications Networking Module.	71
5.2	Shows Certification Authority (CA) Management Module ( <i>CAMM</i> )	74
5.3	Shows Key Distribution Center Module ( <i>KDCM</i> )	75
5.4	Shows ClientModule( <i>CM</i> )	77
5.5	Shows Typical Course of Events of Registering member	79
5.6	Shows Typical Course of Events of Login	80
5.7	Shows Typical course of Events sending message	82
6.1	Shows all the response acknowledgements	86