UNIVERSITI TEKNOLOGI MARA
CAWANGAN PULAU PINANG

SECURE ENCRYPTION IN NETWORK USING DATA ENCRYPTION STANDARD (DES) FOR HIGH SECURITY TRANSMISSION

NUR AMILA BINTI ABDULLAH

Faculty of Electrical Engineering

July 2017

ABSTRACT

Network security have become as significant issue in the recent years. In the field of network security, the role of cryptography is most important. A secrecy key and shared key algorithm is known as a symmetric key algorithm. This is because, in symmetric key algorithm a shared key does both the encryption and decryption. However, there are some weakness of that technique such as if the key is known to others the entire conversation is compromised. In data security system, encryption has become a solution and act as significant role providing the security. The Data Encryption Standard (DES) algorithm is a symmetric key algorithm for the encryption of electronic and allowed for information. The objective of this paper is to improve the security data by using DES algorithm. The substitution technique is applied with addition a XOR operator to enhance the DES algorithm as proposed. Substitution cipher is a technique of encoding where units of plain text are replaced with cipher text and XOR operator is one of the encryption process used to make the cipher text harder to decryption. The result has been compared and analysed by using method, encryption strength, message length and encryption time. The strength level is higher because of used the Extended ASCII-code with 256 character length bit and addition with the 8-bit binary key to break the cipher text. Hence, the analysis are obtained when the message length is long around 40 to 188, the encryption time has been achieved the limitation time. The graph that can be show is static .To summarize it, all this technique are useful for real time encryption. The security provided by this algorithm can be enhanced further, if more than one algorithm is applied to data.

ACKNOWLEDGEMENT

Alhamdulillah. First and foremost, I would like to thank Allah S.W.T. for giving me the time, strength and blessing to finish this study. Without His blessings, none of this is possible. Special appreciation goes to my parent for their love, understanding and unconditional support throughout this long and tough journey.

I would like to express my special gratitude and thanks to my supervisor, Haji Mohd Daud Alang Hassan for his valuable advice, support, ideas and guidance throughout this study.

I wish to extend my special gratitude to my father and mother Abdullah Bin Hasan and Nasiah Bt Che Omar for their prayer, support and encouragement that I need through all these year.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 OVERVIEW OF CHAPTER

This chapter consist of five session which is overview, problem statement, research objective, scope of study and relevancy. For the overview part, the hold of project has been explained with the example of algorithm. Then, at the part 1.3 is about the problem in the encryption's world and solution of the project. Hence, at session 1.4 is the objective of the project and 1.5 is the scope of project. Thus, for the session 1.6 is about the relevancy of the project. The project is relevant because of improving technology now days.

1.2 RESEARCH BACKGROUND

The striking increase of the internet has open the potential that no one ever imagined. The internet can be used for browsing purposes, internet banking, to buy stuff and more. But, some personal transactions, credit card information and personal data can be accessed through the internet. But still left with a difficult job of protecting networks from a variety of attacks. With the lots of efforts, network support staff came up with a solution to the problem named "Cryptography".

Nowadays, cryptography is one of the technique used for sending and receiving messages in secured way over protected medium. Cryptography is the area of study which creates protected messages using encryption and decryption methods and techniques. Due to high demand in message security, encryption and decryption data have recently been widely investigated to avoid invader from invading the data. Encryption is a process by which convert the data into no readable from while decryption is vice versa from it. Plaintext is the original message[1]. While cipher text is the coded message[2]. The reason of encryption algorithm is to secure the message