

Universiti Teknologi MARA

**Image Encryption Through Web
Application Using AES**

Aina Nadhrah Binti Mohd Zaid

**Thesis submitted in fulfilment of the requirements
for Bachelor of Computer Science (Hons.) Data
Communication and Networking
Faculty of Computer and Mathematical Sciences**

August 2020

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, my special thank goes to my supervisor, Dr Zolidah Kasiran for always guiding me throughout completing this project despite having other mentees, she still give her best to make sure I do understand my project and answer all my questions about things that I do not understand.

Special appreciation also goes to my beloved parents that never stop give me moral support by providing me the most convenience environment especially when I have to complete this project at home due to the pandemic and never stop pray the best for me every day.

Last but not least, I want to give my gratitude to my dearest friends that always open their arm and ears to listen to me ranting and always give me the best advice whenever I need it. Unable to meet them physically, they will always send me motivation text through social media to keep me going with this project.

ABSTRACT

A few decades ago, the advent of informational technology (the Internet) led to many changes in the way information is disseminated and shared among people, between countries and throughout the world. Years afterwards, the problem of the "theft" of information has emerged globally. Specialists in the area of information security are curious to see if it can be remedied. It is now clear that security of knowledge is the panacea, despite the prevalence of certain newly discovered methods of cryptanalysis. Thus, this project is proposed in order to create a secure web application for people to encrypt their image. The application is user friendly for everyone to use it daily without much hustle. This project will use Laravel and XAMPP to create the web application and the encryption process. User will upload their image for encryption and decryption through the web application and download their image whenever they need it.

TABLE OF CONTENTS

Contents

SUPERVISOR APPROVAL	I
STUDENT DECLARATION	II
ACKNOWLEDGEMENT	III
ABSTRACT	IV
TABLE OF CONTENTS	V
LIST OF FIGURES	VIII
LIST OF TABLES	X
INTRODUCTION	1
1.1 Project Background	1
1.2 Problem Statement	1
1.3 Research Objective	2
1.4 Project Scope	2
1.5 Project Significance	3
1.6 Conclusion	3
LITERATURE REVIEW	4
1.7 File Encryption	4
1.8 History of Cryptography	4
1.8.1 Standard Cryptography	5
1.8.2 Present Cryptography	6
1.8.3 Symmetric- key cryptography	7
1.8.4 Asymmetric-key cryptography	8

INTRODUCTION

1.1 Project Background

In this modern era, the security issue is becoming extremely important in the context of Internet providing important communication between millions of people and is increasingly being used as an e-commerce tool. The Web is commonly used to upload web pages and other documents to public web hosting sites from a private development system. Files transferring such as e-shopping, tenders, etc. requires a special authenticated process. With communications and transmission of files over the Internet exponentially increased in recent years, such a transfer of files requires protection. One of the approaches to efficient communication is cryptography. This is the way plain text is converted into encrypted text and then cipher text in plain text is decrypted. (Rajan.S.Jamgekar & Joshi, 2013)

Technique of cryptography translates original ordinary plain text into unintelligible form. The technique of cryptography is divided into symmetric key encryption and public key encryption. This technique uses keys to do the translation process. Therefore, all the data and information can only be accessed by an authorized user. To everyone, cipher text data is visible. AES, DES, 3DES, Concept, BRA, and blowfish are the algorithms used for symmetrical key cryptography. The major challenge is to turn a multi-user program into the receiver key. Such algorithms require low security data encoding delay. RSA and ECC algorithms are the public key cryptography algorithm. Public and private keys use public key encryption algorithms. These algorithms have high standards of protection, but they increase encoding and decoding delays. In the other hand, steganography hides in the envelope the hidden data existence. Data are not available to anyone in this technique. The data exist is only accessible to the legitimate receiver. The technique of text steganography is used to establish high data protection. In text cover file, user secret data is covered. It appears like the normal text file after adding text to the text cover file. If an unauthorized individual discovers text file, confidential data cannot be retrieved. It is necessary to recover original data if the unauthorized user wants to do so as long. For text encoding and decoding DES algorithm is used. The benefit of the technique of text steganography is to ensure text protection. For steganography of text, minimum space is necessary compared to image steganography. (Abu Marjan, 2014)

1.2 Problem Statement

In any online transaction, such as online shopping, file transfer or online banking, security has always been the major concern. Knowing the possibilities of our data and information is exposed to a hacker or any unauthorized person, we tend to be scared to do the transactions even when the two-way steps verification and many other security measures has been implemented.