DIGITAL ROAD TAX USING DIGITAL SIGNATURE ALGORITHM

SAW JUNKAI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: DIGITAL ROAD TAX USING DIGITAL SIGNATURE ALGORITHM

SESI PENGAJIAN: [2020 / 2023]

Saya: SAW JUNKAI

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
✓	TIDAK TERHAD	

PM Dr. Nur Azman Abu
Faculty of ICT,
Universiti Teknikal Malaysia Melaka

(TANDATANGAN PELAJAR)

Alamat tetap: 1-12-1, BL AVENUE, Solok Thean Teik, 11500 Ayer Itam, Pulau Pinang.

Tarikh: 18/09/2023

(TANDATANGAN PENYELIA)

(NUR AZMAN ABU)

Tarikh: 21/09/2023

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak

DIGITAL ROAD TAX USING DIGITAL SIGNATURE ALGORITHM

SAW JUNKAI

This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Software Development)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

DIGITAL ROAD TAX USING DIGITAL SIGNATURE ALGORITHM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 18/09/2023

(SAW JUNKAI)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of [Computer Science (Computer Security)] with Honours.

PM Dr. Nur Azman Abu
Faculty of ICT,
Universiti Teknikal Malaysia Melaka

SUPERVISOR : _____ Date : 21/09/2023

(NUR AZMAN ABU)

DEDICATION

I dedicate this letter to my cherished parents, who have continually inspired and motivated me in everything. Thank you, supervisor, for constantly providing me with such excellent suggestions and invaluable time to help me complete this year's final assignment. My friends, who have always supported me and offered wise counsel. I appreciate it. There are no words to describe how much I love each of you.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Pm Dr. Nor Azman Bin Abu, your wisdom, patience, and commitment to nurturing my intellectual growth have been invaluable. This report is a testament to the knowledge and skills you have imparted, shaping my professional aspirations. I also want to express my gratitude to my assessor, Dr. Shekh Faisal Bin Abdul Latip, for his evaluation of me and his precious suggestion provided on my research.

Next, I would like to thank my family, especially my parents Saw Lai Hin and Lau Yen Ling, whose unwavering support and boundless love have been my anchor throughout this academic voyage, I offer my deepest gratitude. Your belief in me, constant encouragement, and sacrifices have shaped the person I am today. This report is a tribute to your unwavering faith in my abilities.

In closing, I would also like to thank my friends, especially Tan Wei Ming and Low Pei Zuo, who have been my companions on this intellectual odyssey, I extend my heartfelt appreciation. Your camaraderie, stimulating discussions, and shared experiences have enriched my educational journey beyond measure. This report is a reflection of the collaborative spirit that has propelled us forward.

ABSTRACT

The implementation of a digital road tax system aims to address the issue of cloned vehicles and enhance the security and authenticity of road tax documentation in Malaysia. Cloned vehicles, which are illegally registered cars without the knowledge of their original owners, pose a significant challenge to law enforcement agencies. This project proposes the adoption of a digital road tax solution utilizing cryptography techniques, specifically digital signatures, to create a secure and tamper-proof system.

The digital road tax system will generate a unique 2D barcode for each road tax, containing crucial information such as car model, car number, expiry date, and amount. This barcode will be encrypted using the private key of the authorized person. The authenticity of the barcode can only be verified by scanning it using a system equipped with the public key of the authorized person, thereby ensuring its validity.

Digital signatures, based on mathematical techniques, will be employed to validate the authenticity and integrity of the road tax documentation. By retrieving the hash of the message and encrypting it with the sender's private key, the digital signature guarantees the source and integrity of the road tax information. This approach significantly reduces the risk of fake road tax issuance and provides a more secure and reliable system for both vehicle owners and authorities.

The adoption of a digital road tax system not only strengthens the enforcement against cloned vehicles but also offers a more efficient and convenient process for road tax management. Vehicle owners can easily present their digital road tax documents using mobile devices or printed barcodes, while enforcement agencies can quickly verify the authenticity and validity of the road tax information through the decryption process.

ABSTRAK

Pelaksanaan sistem cukai jalan digital bertujuan untuk mengatasi isu kenderaan palsu dan meningkatkan keselamatan serta keaslian dokumen cukai jalan di Malaysia. Kenderaan palsu, yang merupakan kenderaan yang didaftarkan secara haram tanpa pengetahuan pemilik asal, merupakan cabaran besar bagi agensi penguatkuasaan undang-undang. Projek ini mencadangkan penggunaan penyelesaian cukai jalan digital dengan menggunakan teknik kriptografi, khususnya tandatangan digital, untuk mencipta sistem yang selamat dan tidak boleh diubah suai.

Sistem cukai jalan digital akan menghasilkan kod bar 2D yang unik untuk setiap cukai jalan, mengandungi maklumat penting seperti model kereta, nombor kereta, tarikh luput, dan jumlah. Kod bar ini akan dienkripsi menggunakan kunci peribadi individu yang berkebenaran. Keaslian kod bar hanya boleh disahkan melalui pemindaian menggunakan sistem yang dilengkapi dengan kunci awam individu yang berkebenaran, memastikan keabsahan dokumen cukai jalan.

Tandatangan digital, berdasarkan teknik matematik, akan digunakan untuk mengesahkan keaslian dan keselamatan dokumen cukai jalan. Dengan mengambil hash mesej dan mengenkripsi dengan menggunakan kunci peribadi penghantar, tandatangan digital menjamin asal usul dan keintegritian maklumat cukai jalan. Pendekatan ini secara signifikan mengurangkan risiko pengeluaran cukai jalan palsu dan menyediakan sistem yang lebih selamat dan boleh dipercayai untuk pemilik kenderaan dan pihak berkuasa.

Pelaksanaan sistem cukai jalan digital tidak hanya mengukuhkan penguatkuasaan terhadap kenderaan palsu tetapi juga menawarkan proses pengurusan cukai jalan yang lebih efisien dan mudah. Pemilik kenderaan dapat dengan mudah menyediakan dokumen cukai jalan digital menggunakan peranti mudah alih atau kod bar yang dicetak, sementara agensi penguatkuasaan dapat dengan cepat mengesahkan keaslian dan keabsahan maklumat cukai jalan melalui proses dekripsi.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATIONS

FYP	**-**	**Final Year Project**
ECDSA	**-**	**Elliptic Curve Digital Signature Algorithm**
ECC	**-**	**Elliptical Curve Point**
RSA	**-**	**Rivest, Shamir, Adleman algorithm**

LIST OF ATTACHMENTS

CHAPTER 1: INTRODUCTION

The purpose of this chapter is to provide project background, problem statement, project questions, project goals, project scope, project contribution and project development for the entire project.

1.1 Project Background

Road tax refers to a tax that vehicle owners must pay annually to the government to drive their vehicles on public roads. The amount of road tax that a vehicle owner has to pay depends on various factors such as the type of the vehicle, engine capacity, and purpose of use. Road tax is a legal requirement and failure to pay it can result in fines and other penalties. The revenue generated from road tax is used to maintain and improve the country's road infrastructure.

In Malaysia, the payment of road tax is a mandatory requirement for all vehicle owners who wish to use their vehicles on public roads. According to the Road Transport Department (JPJ), the act of falsifying the registration of cars smuggled into Malaysia, commonly referred to as cloned cars, is not only done secretly without the knowledge of the original owners, but also by those who conspired with syndicates that offered them compensation to be involved in the illegal act. A total of 314 cloned vehicles have been seized from the year 2016 until March of 2021 and most of the cloned cars are luxury vehicles (Ramli, 2021).

The rise of technology makes possible of creating a digital road tax which will be much harder to duplicate as a fake road tax. A digital road tax can avoid the situation by producing a 2D barcode for each road tax which contain the elements of road tax such as car model, car number, expiry date, amount and the most

important one is encrypted using the private key of the authorized person. The barcode produced can only be scan by the system store with the public key of the authorized person to decrypt and verify the validity of the barcode. The cryptography technique applied will be digital signature which is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. Generally, digital signature is formed by retrieving the hash of the message and encrypting the message with the sender's private key. This signature guarantees the source and integrity of the message (Aufa et al., 2018).

1.2 Problem Statements

The increase in creating fake road tax for cloned car used by paying an illogical price which are very low compare to the market price led to avoid of yearly road tax payment and reduced the revenue generated yearly to maintain and improve the country's road infrastructure. Moreover, the congested and long lines at the JPJ counter to wait for a collection of physical copy road tax have bring inconvenient to the nations and the JPJ officer. It is challenge to check on a validity of an electronic road tax off-line.

Table 1.1: Summary of Problem Statements

NO	PROBLEM STATEMENT
1.	An increase of fake road tax have highly reduced the revenue generated yearly.
2.	Physical copy of Road Tax easily tampered or destroyed by third-party.

1.3 Project Questions

Digital Signature Algorithm associated with the 2D barcode have widely been used in current industry practice to ensure the security and integrity of the data provided and generated. This research highlighted two questions which holds strong fundamentals in helping to solve the problems.

Table 1.2: Summary of Project Questions

NO	PROJECT QUESTION
1.	Which Digital Signature schemes is suitable to be applied in this system?
2.	Which type of 2-Dimensional barcode is appropriate to be applied in this system?

1.4 Project Objectives

This study's goal is to study the digital signature algorithm. The second objective is to propose a digitally signed road tax. Finally, the objective is to verify the validity of a road tax produced using barcode scanner.

Table 1.3: Summary of Project Objectives

NO	PROJECT OBJECTIVES
1.	To study the digital signature algorithm.
2.	To propose a digitally signed road tax.
3.	To verify the validity of a road tax.

1.5 Project Scope

This project will produce two system, one will be website and the other one will be mobile application. Scope of the project is going to be conduct as below:

1. Developing a website to provide the service of generating digital road tax in a string form encrypted with the digital signature of the authorized person. The language that will use to develop this website will be C++ programming language through the Visual Studio 2022 platform and using Microsoft Access as database. The target user of the application will be JPJ officer which will used to generate digital road tax and verify the digital signature for vehicle owner.
2. The primary functions of the codes are to generate an ECDSA-based digital signature using the SECP256K1 curve, encode the original message in

base64, and return as a string for verification that uses the public key of the operator to verify the integrity of the digital road tax. The goal is to use cryptographic techniques to build a reliable and effective digital road tax.

1.6 Project Contribution

The development of this project is intended to solve the problem of fake road tax issued by third party to avoid payment of road tax by providing a digital type of road tax with a higher security level which implemented to generate the road tax in the form of a encoded string that will be digitally signed by authorised person. Moreover, the congestion and long lines at the JPJ office will be reduced as the vehicle owners do not necessary go to the office to acquire the physical copy of road tax.

1.7 Project Organization

This report consists of seven chapters that will be covered in the project research. This report is divided into chapters and organised according to the project's progress.

Table 1.4: Table for Project Organization

Chapter	Detail
Chapter 1 Introduction	This chapter discuss about the introduction, project background, problem statement, project question, project objective, project scope, project contribution and project organization.
Chapter 2 Literature Review	This part will be reviewing past research, journal and conference papers as well as related works for the project matter. The definition of the terms used in the project, the introduction to the literature review, and the related or earlier works utilized to describe the research method. Additionally, this chapter will compare different digital signature algorithm exist. Finally, this chapter will offer a solution that needed to complete the project and wrap up the literature review chapter.

Chapter 3 Methodology & Design	This chapter will explain the method used to determine the digital signature algorithm and project methodology. Project schedule and milestone will discuss in this chapter to finish the project in time. This chapter also discusses the requirement that will be used to run this project and a flowchart. The flowchart is discussed in detail about how the process works.
Chapter 4 Implementation	This chapter implements the chosen digital signature algorithm using the selected language and technique. The research and results of the suggested method were covered in this chapter. This chapter also determines whether the suggested approach works out.
Chapter 5 Testing	This chapter is about testing. Specifics on how to evaluate the outcomes of each segmentation strategy and decide which is best for segmenting land use are provided via testing and analysis.
Chapter 6 Conclusion	This chapter will summarize all chapters as a conclusion. Project summarization, limitation and future work will discuss.

1.8 Conclusion

As a conclusion, the first chapter is to summarise the entire project development research in order to understand the project. The problem statement, project question, project objectives and project scope are discussed in this chapter to identify and solve the problem. Besides that, the project organization also provide a clear flow to make sure this project runs in sequence. Next, the chapter of literature review will be covered in this project.

CHAPTER 2: LITERATURE REVIEW

This chapter will review the significant and information in details for the work being proposed. It introduces the Digital Signature algorithm and its component that available to be used for it. Moreover, this chapter highlight some critical reviews of existing works and its proposed solution.

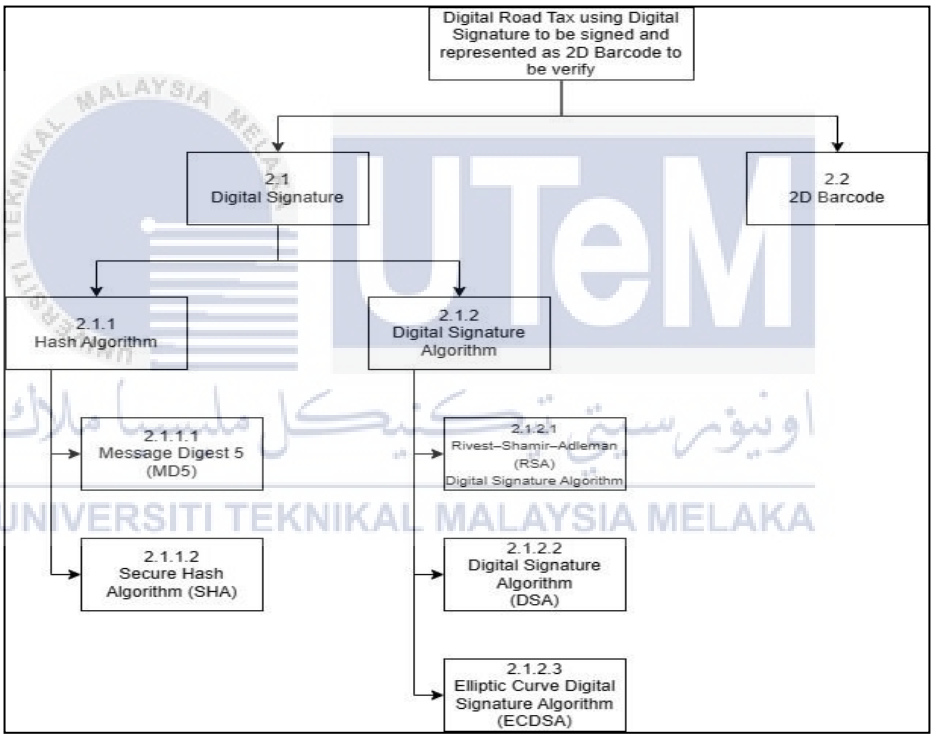

Figure 2.1: Taxonomy of Research Background

2.1 Digital Signature

According to Malaysian Communications and Multimedia Commission (2023), Digital Signature is an electronic signature used to verify the identity of the sender or signer of a message and also to ensure the correctness and validity of information in electronic transactions. The application of a recognized digital signature can satisfy the needs of information integrity, non-repudiation, identity authentication, and confidentiality.

A digital signature is an algorithm that allows one to verify that a certain message (in our case, a digital road tax) has been created by a particular person. The basic idea is that the author generates a pair of keys: a secret key k_{sec}, which must be kept out of reach for all others, and a public key k_{publ}, which can be known to anyone. There is a fixed-length output function sgn(x,k) taking an arbitrary message x and a secret key k, such that the triplet

$$\{m, \text{sgn}(m,k_{sec}), k_{publ}\} \quad (1)$$

verifies the fact the author, identified with the public key k_{publ}, indeed possesses the corresponding secret key k_{sec} and signed the message m. On the other hand, the above triplet does not allow one to determine k_{sec} using a reasonable amount of classical computational resources (Kiktenko et al., 2018).

According to the research implemented by Kaur et al., (2012), Digital Signature can be classified into two processes:

1. Signature and Encryption
2. Decryption and Signature Verification

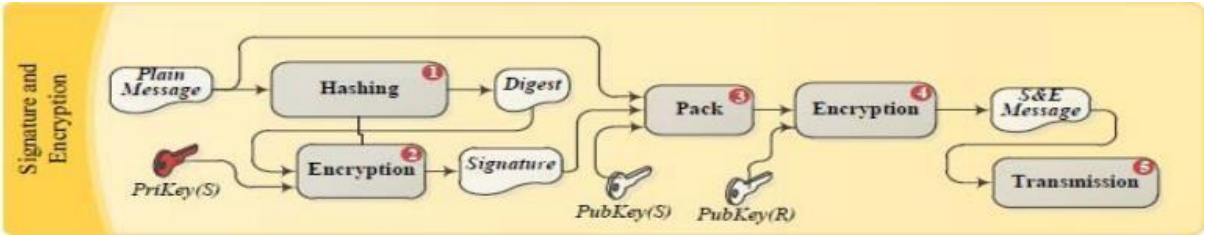

Figure 2.2: Signature and Encryption (Kaur et al., 2012)

The Signing and Encryption process will be describe based on Figure 2.2:

1. **Hashing:** A hashing algorithm is applied in this step. The small message digest is computed as a unique representation of the message. The message integrity

is ensured by this examination. The digital signature is applied to this smaller message digest. A unique code is created by this evaluation.

2. **Encryption:** The encryption involves particular Digital Signature Algorithm. The message digest is encrypted using private key of the sender. The message digest will be sign and generated as signature. Decrypting of the message signature using corresponding public key of sender will obtain the original message. The signing is performed in this step to obtain non-repudiation.
3. **Pack:** A single packed unit contains the plain message, the message signature, and the sender's public key.
4. **Encryption:** The plain message, message signature, and the public key of the sender as a single packed unit is encrypted using the receiver's public key by a particular Digital Signature Algorithm to form signed and encrypted message that will be ready for transmission.
5. **Transmission:** The signed and encrypted message will then be transmitted.

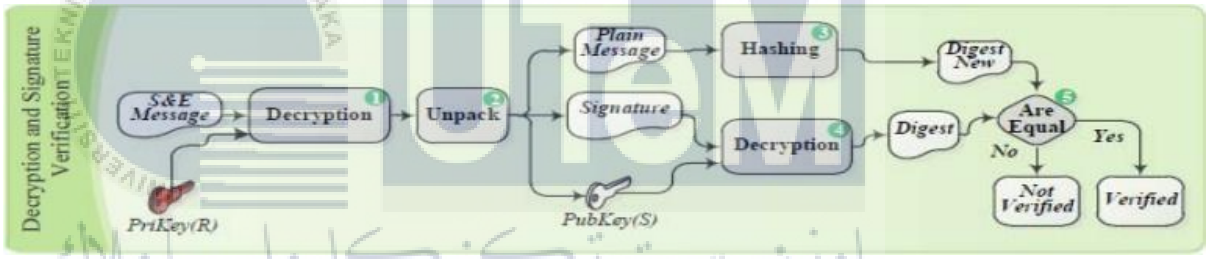

Figure 2.3: Decryption and Signature Verification (Kaur et al., 2012)

The Decryption and Signature Verification process will be describe based on Figure 2.3:

1. **Decryption:** The target receiver that received the message will use the receiver's private key to decrypt the message and form a single packed unit which contains plain message, message signature, and the public key of the sender.
2. **Unpack:** The sender's public key, plain message and message signature will be obtained after decryption step by unpacking the packed single unit.
3. **Hashing:** The plain message that obtained will compute to message digest using the same hash function used by the sender.
4. **Decryption:** The message signature will be decrypt using the sender's public key to obtain the message digest that is computed by the sender.