A Project Report

On

Credit Card Encryption and Decryption

**Network Infrastructure and Security**

A project report submitted in partial fulfillment of the requirements for the degree of Bachelor of Technology in Computer Science and Engineering

by

**I Kaustubh Sastry (2010030064)**

**M Abhiram (2010030457)**

**Manohar Karthik (2010030197)**

Under the guidance of

**Dr. S. Balaji**

Professor

****

**K L University, Hyderabad**

**DEPARTMENT OF COMPUTER SCIENCE**

(R.V.S Nagar, Moinabad-Chilkur Rd, near AP Police Academy, Aziznagar, Telangana 500075)

****

**K L University, Hyderabad**

(R.V.S Nagar, Moinabad-Chilkur Rd, near AP Police Academy, Aziznagar, Telangana 500075)

**DEPARTMENT OF COMPUTER SCIENCE**

**CERTIFICATE**

This is to certify that the Project work entitled “**Credit card Encryption and Decryption**” is carried out by **I. Kaustubh Sastry (2010030064),M. Abhiram (2010030457), K V Manohar Karthik(2010030197)** in partial fulfillment for the award of degree of **Bachelor of Technology** in **Computer Science and Engineering**, K L University, Hyderabad during the academic year 2022-2023.

Dr. S. Balaji

(Professor)

Internal Guide

Signature of the HOD External Examiner

(Certificate from Industry)

**DECLARATION**

I hereby declare that the project titled “**Credit card Encryption and Decryption**” submitted to Computer Science and Engineering, K L University, Hyderabad for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a result of original work carried-out in this project report. I understand that my report may be made electronically available to the public. It is further declared that the project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

Name of Student(s) : I. Kaustubh Sastry ,M. Abhiram, K V Manohar Karthik

Roll Number(s) : 2010030064, 2010030457, 2010030197

Degree : Bachelor of Technology in K L University, Hyderabad

Department : Computer Science and Engineering

Title of the project : Credit card Encryption and Decryption

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**I Kaustubh Sastry (2010030064)**

**M Abhiram (2010030457)**

**K V Manohar Karthik (2010030197)**

Date: November 2022

## ACKNOWLEDGEMENT

First and foremost, we thank the lord almighty for all his grace & mercy showered upon us, for completing this project successfully.

We take grateful opportunity to thank our beloved Founder and Chairman who has given constant encouragement during our course and motivated us to do this project. We are grateful to our Principal **Dr. L. Koteswara Rao** who has been constantly bearing the torch for all the curricular activities undertaken by us.

We pay our grateful acknowledgement & sincere thanks to our Head of the Department **Dr. Chiranjeevi Manike** for his exemplary guidance, monitoring and constant encouragement throughout the course of the project.

We thank **Dr. S. Balaji** of our department who has supported throughout this project holding a position of supervisor.

We whole heartedly thank all the teaching and non-teaching staff of our department without whom we won’t have made this project a reality. We would like to extend our sincere thanks especially to our parents, our family members and friends who have supported us to make this project a grand success.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I Kaustubh Sastry (2010030064)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

M Abhiram (2010030457)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

K V Manohar Karthik (2010030197)

## ABSTRACT

**Abstract:** Credit cards are usually encrypted in order to reduce the chances of sensitive information like CVV, Passwords etc. The encryption of a credit/debit card consists of the security measures taken within the card and the encryption algorithms used in the back end of the system. Stronger the algorithm, more secure the encryption algorithm, more secure is our credit/debit card. When the credit card owner swipes the card to the machine, our sensitive information such as account number, CVV etc. are scrambled using some encryption algorithms like RSA. RSA has stood nearly 40 years of attacks, making it the choice for internet transactions and card transactions. This information is gathered by the machine using the magnetic strip at the back of the card. The magnetic strip fetches the information to the scanner only when the encryption keys match. This ensures stronger security to the credit cards. There are other types of cards which have an embedded electronic chip in them which may make it even harder to steal information. This type of card is known as a smart card.

The process of decryption is exactly the reverse process of encryption. You can use any of the number of existing open-source implementations of AES or TDES mode, which contains a default initial vector of all zero bytes. Suppose we are having the exact 16-byte decryption key, the process of decryption is easy. Then comes the actual tricky part which is the key derivation. The basic things we need to remember is the key used in the encryption process and the algorithm used. Thus, the decryption is done using the key. These days, each and every credit-card data is encrypted using a key, that is obtained using a special key-management scheme called Derived Unique Key Per Transaction (DUKPT). There is one thing to understand that in the DUKPT world, every transaction has its own key. Replay-attacks are impossible since the key used cannot be used again for other transactions.

**Keywords:**

* AES
* SDES
* TDES
* DUKPT
* CVV
* Smart Card

## TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
|  | | **Page** |
|  | |  |
| **List of Figures** | | viii |
| **List of Abbreviations** | | ix |
| **CHAPTER 1: INTRODUCTION** | |  |
| 1.1 | Introduction | x |
| 1.2 | Problem statement | xi |
| 1.3 | Objectives | xii |
| **CHAPTER 2: LITERATURE REVIEW** | |  |
| 2.1 | Summary of literature review and research gap | xiii |
| **CHAPTER 3: METHODOLOGY** | |  |
| 3.1  3.2 | Methodology  Working | xiv  xv |
| **CHAPTER 4: RESULTS AND DISCUSSION** | |  |
| 4.1 | Summary of results and discussion | xix |
| **CHAPTER 5: CONCLUSION AND RECOMMENDATIONS** | |  |
| 5.1 | Conclusion | xx |
| **REFERENCES** | | xxi |
|  | |  |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Figure 4.1.1 | Hierarchy of Credit Card Security |  |
| Figure 4.1.2  Figure 4.1.3 | Encrypted Credit Card Value  Decrypted Credit Card Value |  |

## LIST OF ABBREVIATIONS

* AES – Advanced Encryption Standard
* DES – Data Encryption Standard
* SDES – Simplified DES
* TDES – Triple DES
* DUKPT - Derived Unique Key Per Transaction
* CVV – Card Verification Value

**1.1 Introduction**

Credit cards are an integral part of the payment process. Consumers expect that most businesses will accept cards as a method of payment, rather than relying on cash to conduct transactions. Businesses provide electronic terminals that a consumer can scan his or her credit card through, with the terminals sending the card’s identifying information to computer servers in order to verify that the consumer has sufficient funds.

Credit card encryption is the conversion of the sensitive information required for credit card transactions into an encoded form that is only decipherable by the payment processor using the corresponding decryption key. The encryption tool is designed to validate and restrict access to card tokenization services. A few examples of encryption algorithms are DES, AES, RSA

**1.2 Problem Statement**

Applying Pluggable Encryption and Decryption to your Credit Card:

* Improves the system's ability to protect credit card data during transfer and storage.
* Upgrades existing credit card data.
* Protects data during information display.

Once upgraded, the system displays credit card numbers so as to mask them. Before upgrade, the system displayed all digits of a credit card number, whether display-only or editable. The feature modifies the display to show only the last four digits, replacing each preceding digit with an X.

**1.3 Objectives**

Pluggable Cryptography protects critical PeopleSoft data and enables more secure data communication with other businesses. It enables you to extend and improve cryptographic support for your data in PeopleTools. By incrementally acquiring stronger and more diverse algorithms for encrypting data, Pluggable Cryptography offers strong cryptography with the flexibility to change and grow.

Enhanced cryptography capability is provided by PeopleSoft pluggable encryption technology (PET), which employs 3DES algorithms and 168-bit encryption keys to secure data.

**2.1 Literature Review**

Implementation of Encryption and Decryption Methodologies” is the project designed to explain about encryption and decryption. Below are the findings of various research papers.

As we said the significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. Many studies propose methods to combine cryptography with steganography systems in one system. This Project has been implemented on the basis of the requirements of security i.e. authentication, confidentiality, and robustness. There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together. In proposed an encrypting technique by combining cryptography and steganography techniques to hide the data. In cryptography process, we proposed an effective technique for data encryption using one’s complement method. It used an Asymmetric key method where both sender and receiver share the Secret key for encryption and decryption. In steganography part, we used the LSB method that is used and mostly preferred. We present a method based on combining both the strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. An encryption technique is employed for encrypting a secret message into a Cipher text using the Senders Private Key and receiver public key. The Cipher Text is finally embedded in a suitable cover 11 image and transferred securely to deliver the secret information. They utilized a least significant bit method to accomplish the digital image steganography. At the receiver’s side, the secret data is retrieved through the decoding process. Thus, a three-level security has been rendered for them a secret message to be transferred.

**3.1 Methodology**

When a credit account holder makes a purchase with their card, the information such as the account number is scrambled by an algorithm. The intent is to make it impossible to access that information without the corresponding encryption key that lets the merchant and financial institution conduct their transactions. Until the information is decrypted by the key, the information is not usable, making it safe so long as it remains locked.

Card issuers use a variety of methods to encrypt credit cards. The magnetic strip on the back of a card is typically encrypted and can only be read by a card scanner. Relying solely on the magnetic strip is a less secure method than requiring the use of a PIN-and-chip, because a PIN makes it more difficult for stolen credit cards to be authorized and used. A smart card with an electronic chip may be harder for thieves and hackers to steal information from, compared with other forms of encryption and security put in place to protect credit account information.

**3.2 Working**

Mastercard Encryption and Decryption

* Introduction
* Configuring the Mastercard Encryption
* Performing Mastercard Encryption
* Performing Mastercard Decryption
* Encrypting Entire Payloads
* Decrypting Entire Payloads
* Using HTTP Headers for Encryption Params

**Introduction**

The core methods responsible for payload encryption and decryption are encryptPayload and decryptPayload in the FieldLevelEncryption class.

* **encryptPayload usage:**

String encryptedRequestPayload = FieldLevelEncryption.encryptPayload(requestPayload, config);

* **decryptPayload usage:**

String responsePayload = FieldLevelEncryption.decryptPayload(encryptedResponsePayload, config);

**Configuring the Mastercard Encryption**

Use the FieldLevelEncryptionConfigBuilder to create FieldLevelEncryptionConfig instances.

Example:

Text

Description automatically generated

**Performing Mastercard Encryption**

Call FieldLevelEncryption.encryptPayload with a JSON request payload and a FieldLevelEncryptionConfig instance.

Text

Description automatically generated

**Performing Mastercard Decryption**

Call FieldLevelEncryption.decryptPayload with a JSON response payload and a FieldLevelEncryptionConfig instance.

Example using the configuration above:

Text

Description automatically generated

**Encrypting entire payloads**

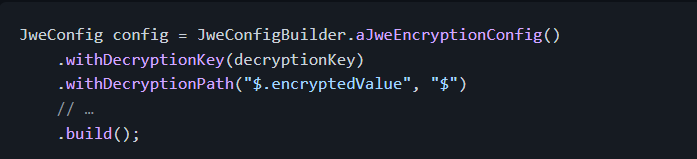
Entire payloads can be encrypted using the "$" operator as encryption path:

Text

Description automatically generated

**Encrypting entire payloads**

Entire payloads can be decrypted using the "$" operator as decryption path:



**Using HTTP Headers for Encryption Params**

In the sections above, encryption parameters (initialization vector, encrypted symmetric key, etc.) are part of the HTTP payloads.

Here is how to configure the library for using HTTP headers instead.

Configuration for Using HTTP Headers

Call with{Param}HeaderName instead of with{Param}FieldName when building a FieldLevelEncryptionConfig instance. Example:

Text

Description automatically generated

**4.1 Results and Discussion**

This is how the hierarchy of the Credit Card security looks like

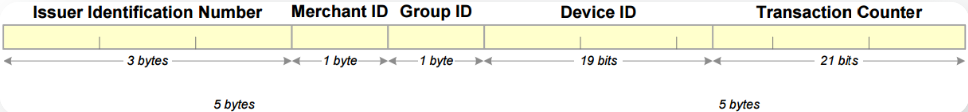
****

Fig 4.1.1

The encrypted ID Card number is as follows

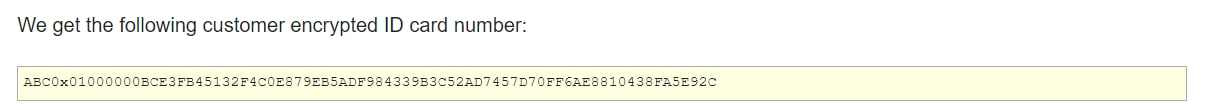


Fig 4.1.2

When Decrypted, We will be able to get the decrypted credit card value.



Fig 4.1.3

**5.1 Conclusion and Future Scope**

Cryptography plays vital role in explosive growth of digital data storage and communication. In this paper, it has been surveyed that the existing works on the tools that cryptographers and cryptanalysts use has shifted from mechanical machines to stronger and stronger computers. With the growth of the internet and the spread of the computers and smart phones, the importance of day-to-day information security is no longer thought of as only a military or government concern.

In future, We are trying to encrypt and decrypt the Credit Card using SQL server and XML.

**References**

* Iwasokun, Gabriel Babatunde, Taiwo Gabriel Omomule, and Raphael Olufemi Akinyede. "Encryption and tokenization-based system for credit card information security." Int J Cyber Sec Digital Forensics 7, no. 3 (2018): 283-93.
* Khatarkar, Sarika, and Rachana Kamble. "A survey and performance analysis of various RSA based encryption techniques." International Journal of Computer Applications 114, no. 7 (2015).
* Nithin, N., and Anupkumar M. Bongale. "XBMRSA: A new XML encryption algorithm." In 2012 World Congress on Information and Communication Technologies, pp. 567-571. IEEE, 2012.
* Ogburn, Monique, Claude Turner, and Pushkar Dahal. "Homomorphic encryption." Procedia Computer Science 20 (2013): 502-509.