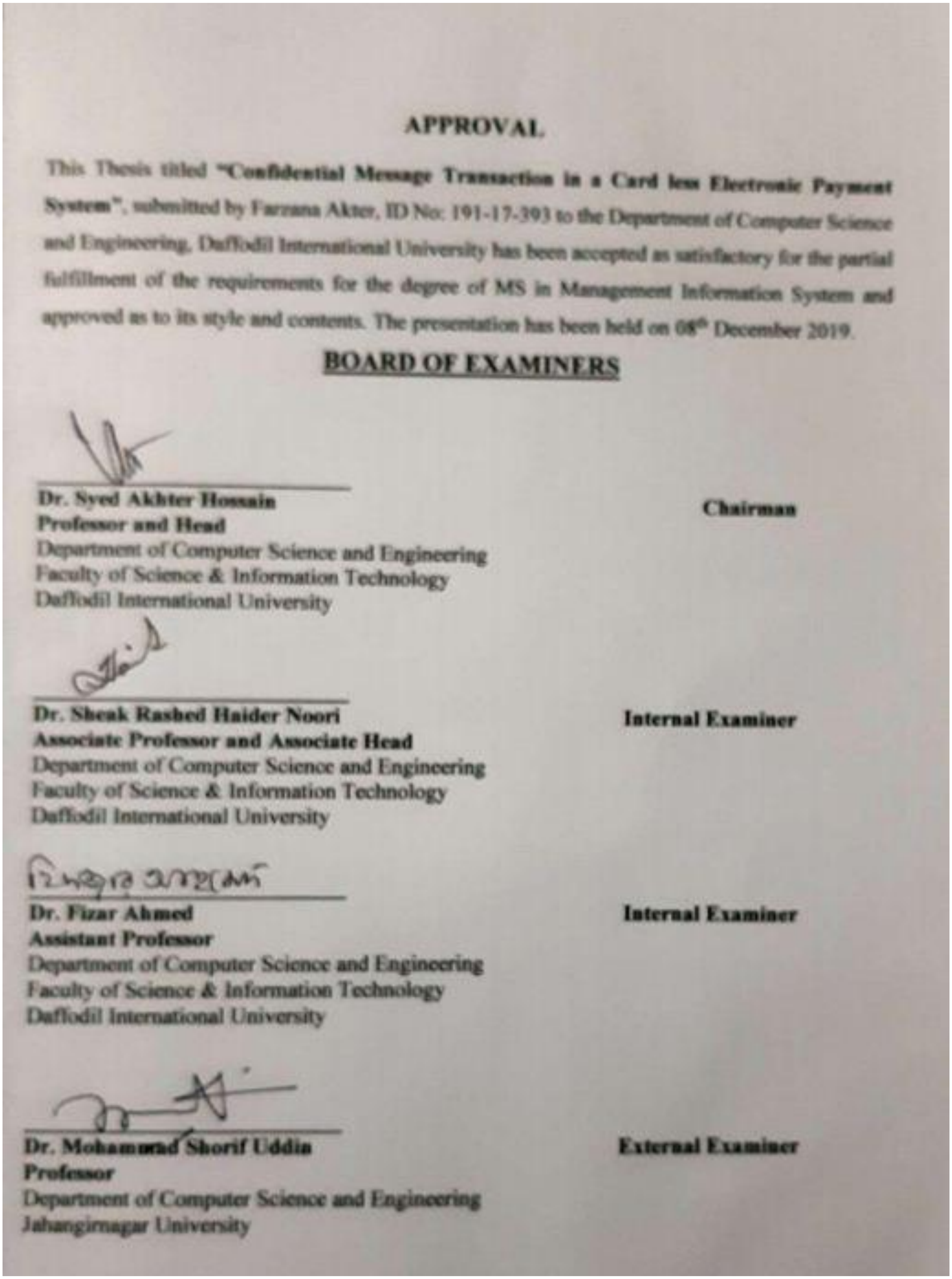
Confidential Message Transaction in a Card less Electronic Payment System

Submitted By
Farzana Akter
ID: 191-17-393
Department of Management Information System (MIS)
Daffodil International University, Dhaka

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science in Management Information System.

Supervised By
Md. Zahid Hasan
Assistant Professor
Department of Computer Science and Engineering (CSE)
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
DECEMBER 2019



APPROVAL

This Thesis titled **"Confidential Message Transaction in a Card less Electronic Payment System"**, submitted by Farzana Akter, ID No: 191-17-393 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of MS in Management Information System and approved as to its style and contents. The presentation has been held on 08th December 2019.

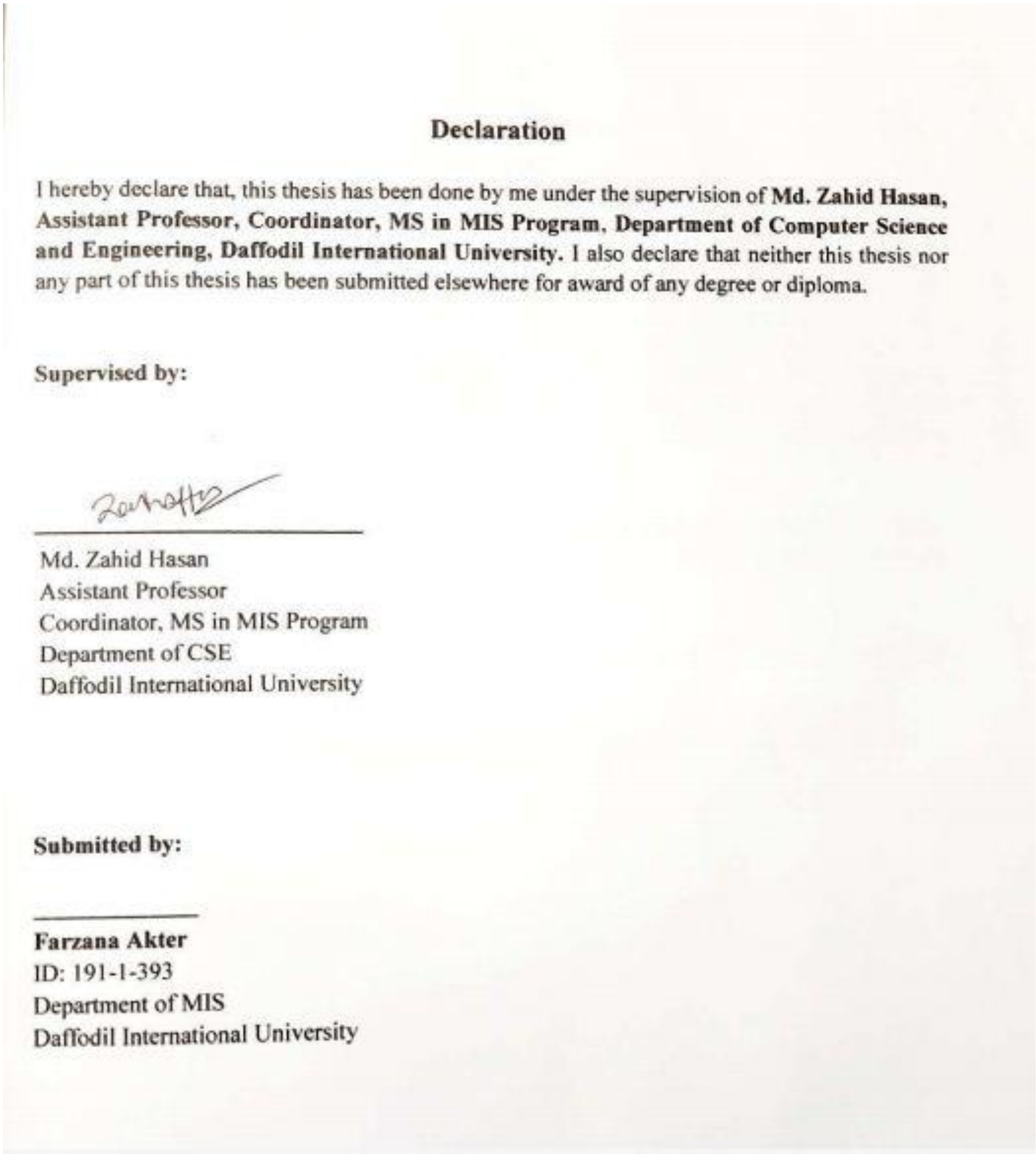
BOARD OF EXAMINERS

Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Sheak Rashed Haider Noori — **Internal Examiner**
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

ফিজার আহমেদ
Dr. Fizar Ahmed — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Mohammad Shorif Uddin — **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University



Declaration

I hereby declare that, this thesis has been done by me under the supervision of **Md. Zahid Hasan, Assistant Professor, Coordinator, MS in MIS Program, Department of Computer Science and Engineering, Daffodil International University.** I also declare that neither this thesis nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Md. Zahid Hasan
Assistant Professor
Coordinator, MS in MIS Program
Department of CSE
Daffodil International University

Submitted by:

Farzana Akter
ID: 191-1-393
Department of MIS
Daffodil International University

ACKNOWLEDGEMENT

FirstIexpressmyheartiestthanksandgratefulnesstoalmightyAllahforhisdivineblessingmakes me possible to complete the final year project/internshipsuccessfully.

Iamreallygratefulandwishmyprofoundindebtednessto**ZahidHasan,AssistantProfessor**and **Professor Dr. Md. Ismail Jabiullah,** Department of CSE, Daffodil International University, Dhaka.Deepknowledge&keeninterestofmysupervisorinthefieldof"WebBasedApplication Development" helps me to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete thisthesis.

Iwouldliketoexpressmyheartiestgratitudeto**Dr.SyedAkhterHossain,ProfessorandHead,** Department of CSE, for his kind help to finish my thesis and also to other faculty members and the staff of MIS department of Daffodil InternationalUniversity.

I would like to thank my entire course mates in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

Abstract

This thesis is on “**Confidential Message Transaction in a Card less Electronic Payment System**”.Now-a-dayspeoplewantmodernsystemaswellasmuchmoreuserfriendlythanbefore. In a card less electronic payment system messages are used instead of credit or debit cards. These messagesarepassedbetweendifferententitiesinordertodoelectronictransactionsoveranetwork. The security of the card less electronic payment system is a critical issue. In this process it define thesecurityandtheconfidentialityofmessagesincardlesspaymentsystem.Themessagespassed between different entities are secured by using hybrid encryption and decryption technique. The Analysis of different pair of encryption/decryption algorithms which are RSA-DES, RSA-AES andRSA-TRPLEDESinthehybridencryptiontechniqueisdoneandconclusionsaredrawnonthe basis of execution time and memory usage. Experimental results show that RSA-DES executes faster and takes less memory so it is most suitable for hybrid encryption/decryption ofmessages.

Table of Contents

Index **Page No**

APPROVAL……….…………………………………………………………….. i

CERTIFICATION………….…………………………………………………… ii

ACKNOWLEDGEMENT……………………………………………………… iii

ABSTRACT…………………………………………………………………... iv

LIST OF FIGURES…………………………………………………………... vii

LIST OF TABLE……………………………………………………………... viii

Chapter 1: Introduction 01 - 02

1.1 Introduction 01
1.2 Motivation 01
1.3 Objective 01
1.4 Expected Outcome 02
1.5 Report Layout 02
1.6 Summary 02

Chapter 2: Literature Reviews 03 - 04

2.1 Introduction 03
2.2 Related Works 03
2.3 Comparative Studies 04
2.4 Challenges 04

Chapter 3: Background Analysis 05 - 11

3.1 Security Requirement for Secure Payment System 05
3.1.1 Authentication 05
3.1.2 Access Control 05
3.1.3 Data Confidentiality 05
3.1.4 Data Integrity 05
3.1.5 Non Repudiation 05
3.2 Types of Attacks on Unsecure System 06
3.2.1 Network Attacks 06
3.2.2 Snooping 06
3.2.3 Tampering 06
3.2.4 Spoofing 06
3.2.5 Hijacking 06

3.2.6 Capture-Replay 06
3.2.7 PIN Guessing Attacks 06
3.3 Cryptographic attacks 06
3.3.1 Cipher Text-Only Attack 06
3.3.2 Known-Plaintext 06
3.3.3 Chosen-Plaintext Attack 07
3.3.4 Chosen-Cipher Text (CCT) Attack 07
3.4 Issues of Security Approach to Secure Payment System 07
3.4.1 Secure Sockets Layer 07
3.4.2 Secure Electronic Transaction 07
3.4.3 D Secure 08
3.5 Cyber Cash 08
3.6 The Secure Electronic Payment System Using Communication Tunnel 08
3.7 Secure Communication Tunnel 08

Chapter 4: Algorithms 12 - 20

4.1 RSA Algorithm 12
4.2 Key Generation Algorithm 12
4.3 A Practical Key Generation 12
4.4 Summary of RSA 14
4.5 Key Length 14
4.6 Minimum Key Lengths 14
4.7 Data Encryption Standard (DES) 15
4.8 Advanced Encryption Standard (AES) 16
4.9 Comparison 18

Chapter 5: Proposed Model 21 - 24

5.1 Flow Diagram 21
5.2 RSA Flowchart Process 21
5.3 Proposed Solution 23

Chapter 6: Experimentation and Result 25 - 26

6.1 Introduction
6.2 Experiment

Chapter 7: Conclusion 27 - 27

7.1 Conclusion
7.2 Future Scope

References 28

List of Figures

Chapter 3: Background Analysis

3.1 Secure Communication Tunnel Consists Of SSL and Nested Crypto Tunnel 09
3.2 Asymmetric Encryption 10

Chapter 4: Algorithms

4.1 Data Encryption Standard (DES) 15
4.2 Advanced Encryption Standard (AES) 17
4.3 Comparison of DES, AES, and RSA Encryption Time Among
4.4 Decryption Time among DES, AES, and RSA Comparison

Chapter 5: Proposed Model

5.1 Hybrid Algorithm Process 21
5.2 RSA Flowchart Process 22
5.3 Card less Electronic System 23
5.4 Electronic Transactions Secure By Enhancing the Confidentiality of Messages 24

Chapter 6: Experimentation and Result

6.1 Hybrid Encrypt/Decrypt the Message of Three Different Sizes 25
6.2 RSA-DES Consumes less Memory

List of Table

Chapter 4: Algorithms

4.1 Comparable Table 15

4.2 Comparison AES, DES, RSA 18

4.3 Comparison AES, DES, RSA 19

Chapter 6: Experimentation and Result

6.1 Comparison 3 Pair 25

CHAPTER 1
INTRODUCTION

1.1 Introduction

Execution of technology give solutions for so many security services which is based on cryptographic approach. Cryptography algorithms are used to providing best security for information. Usually Cryptography algorithms are providing secure communication betweengovernment agencies, individuals, and military forces. So that, now-a-days cryptography is a foundation of the modern security issues used to defendresourcesand informationon both open and closed networks. Cryptography is all about "Secret writing. Methods of transforming an comprehensible message into one that is incomprehensible when art or science surround the principles, and then the changed message again back to its original form. Card less electronic payment system assign to a system in which main actionispurchasing and sellingof various products and services accepted out over the Internet and computer networks without the use of debit or creditcard instead of messages are passed between different individuals. The main reason of using this, it’s a card less e-payment system. People only will trust electronic payment systems when the security is high and it will be beneficial to them because they can buy goods and services from the global market.

1.2 Motivation

To build up something useful obviously need some motivation. The new developments also need a review of cash and the vision of a cashless community. In the sixties some difficulty of cash became probable and the vision of a cashless community built on electronic means ofpayment.Anelectronicpaymentsystemisthatpaymentby credit, electronic transfer with the card details, or another electronic payment system seems to be payment by cheque and cash. Respectively, an electronic payment system is mainlymaking a payment over the internet. Nowso many payment services have come to the market in lastyears, mostofthemarebasedontechnologicalmodernizationontheinternet.

1.3 Objectives

Security is the main problem of this card less electronic payment system. people will trust electronic payment systems when the security is upgraded then beforeand it will be beneficial to people because they can buy goods and services from the global market. Card less e-payment systems security can be extend by rising the confidentiality of the messages which have the information about the payment and payer in the card less e-payment system. The system Inspire people to usingelectroniccashto make a cashlesstransactionindigital age.There are so many security solutions available in the internet tomakeelectronicpaymentsprocess in secure wayand create awareness about different types of security.

1.4 ExpectedOutcome

From card less payment system main expectation is the security and the confidentiality of messages. By using hybrid encryption and decryption technique the messages cross between different individuals in asecured way. The hybrid encryption technique is done on the basis of memory usage and execution time. empirical results show that RSA encryption standardproduce faster and takes less memory so it iscompatible for hybrid encryption/decryption of messages more than RSA-DES, RSA-AES. So, this is the prospective outcome of thisthesis.

1.5 ReportLayout

The layout of this report is described below:

In chapter 1 I have covered the introduction to my project, motivation for building this kind of system, objectives and goals of the card less e-payment system, what I have planned or the expected outcome of the application and the ultimate layout of this report.

In chapter 2 I have added some related paper and some case studies that helped me a lot in developing this research. I also included the process and security issues of the whole system.

In chapter 3 I have specified the whole process of this application using some algorithm.

In chapter 4 I have specified the proposed model of the research.

In chapter 5 I have added the experiment and result details and reports indetails.

Chapter 6 is covered by the discussion and future development scopes andplans.

1.6 Summary

FinallyIdiscussaboutCardlessElectronicPaymentSystem,confidentiality,objective,motivation and report layout of my thesispaper.

CHAPTER 2
Literature Review

2.1 Introduction

Cardlesselectronicpaymentsystemreferstoasysteminwhichbusinessactivitieslikesellingand purchasing of products and services carried out over electronic systems like the Internet and computer networks without the use of credit or debit card instead Messages are passed between different entities. The security of the card less e-payment system can be enhanced by increasing theconfidentialityofthemessageswhichhavetheinformationaboutthepaymentandpayerinthe card less electronic payment system. The messages can be made confidential by using symmetric encryption or asymmetric encryption. But to enhance the confidentiality and to make it stronger this research uses the technique of hybrid encryption/decryption. This technique uses the combination of both symmetric and asymmetric encryption/decryption algorithms. This strong confidentiality of message minimizes the risk of information leakage. The propose solution providesapaymentsystemfordevelopingcountrieswhichwillbemoresecureandallowtheusers to purchase goods and services without the use of credit cards or debit cards [1]. Hybrid encryption/decryption technique is widely used in applications and software. Examples are GNU PRIVACYGUARD(hybridencryptionsoftware),GPGPKI(hybridencryptionsoftware)[2]etc. As a contribution hybrid encryption/decryption technique is studied in detailed and a new system is proposed which apply hybrid encryption/decryption on messages in a card less electronic paymentsystemthusenhancingthesecurityofthesystem.Restoftheorganizationofthepaperis as follows: section [2] describes related work; section [3] will describe the purposed solution. Section [4] will present experimental results and section [5]conclusion.

2.2 RelatedWorks

Balouch et.al. Proposed a card less electronic payment system. The main idea of this study resolves around the designing and implementation of a messaging system for electronicpayments for the developing countries. The system act as a card less system because it obviates the use of cards e.g. credit cards and debit cards for electronic payments. Most of people in developing countries do not possess credit cards, debit cards or any other form of plastic money. Also when theywishtotransferlargeamountoffunds,creditcardsdonothelpthemasthereisalimitbeyond which they cannot employ the plastic money. So they need such a system which minimize theuse of cards and enable them to transfer money without any limitations. On the basis of these requirements and the local infrastructure, she proposed a messaging for electronic payments for localenvironment.

Khan and Singh carried out a research on joint signature and hybrid encryption. They provide securityofadocumentbyusinghybridencryptionandforauthenticitytheyusedigitalsignatures. TheyusethecombinationofIDEARSAalgorithmforhybridencryptionandRSAdigitalsignature algorithm for digital signatures. Their joint signature uses “encrypt then sign”. Their proposed scheme achieved a speed of 2.8Mbps.

MathewandJacobpresentanovelandfasttechniqueforcryptographicapplications.Itisdesigned and developed using the symmetric key algorithm "MAJE4" and asymmetric key algorithm "RSA". They develop a new hybrid system called MARS4 by combining the two encryption methods with an aim to get the advantages of both. Symmetric algorithm MAJE4 is used for encryption/decryptionoffilesbecauseitismuchfasterandoccupieslessmemorythanRSA.The RSA algorithm is used for key exchange andauthentication.

2.3 ComparativeStudies

After reviewing some other similar approaches and their case studies I have sorted common features and unique features of each. Most of them are built for specific purpose for their own demand.

2.4 Challenges

- Online transactions are "card-not-present" transactions. As e-commerce expands, opportunities for fraudulent misuse of payment networks and data theft grow right alongside.
- Chargebacks, in addition to being costly, can damage business reputations; an excessive number of chargebacks can lead to closed merchant accounts, effectively killing the business.
- Consumers are becoming increasingly familiar with biometric identification, such as fingerprint recognition, which is often used to unlock phones. It is now being introduced to increase mobile payment security and preventfraud.
- Cross-border payments can be slow, inefficient, and expensive, but they play an important role in global trade. As-
  - Emerging transnational systems will decrease reliance on correspondentnetworks.
  - Government-led initiatives and mandates will begin to regulate payments andfees.
  - Payment systems will manage credit risk, liquidity, and costs moreeffectively.
  - Multinationals will achieve economies of scale, with a side benefit of consolidating creditrisk.
  - Outsourcing will increase processing efficiency and drive downcosts.
- Payment Card Industry Data Security Standards certification is required for every merchant or business accepting credit or debit cards, online or off. PCI DSS standards require merchants and processors to meet 12 criteria across six security arenas:
  - Build and maintain a secure network andsystems.
  - Protect cardholderdata.
  - Maintain a vulnerability managementprogram.
  - Implement strong access control measures.
  - Regularly monitor and testnetworks.
  - Maintain an information securitypolicy.
- Global ecommerce means accepting a variety of payment methods and currencies.

Chapter 3
Background Analysis

3.1 Security Requirements for Secure PaymentSystem

The primary goal of cryptography is to secure important data as it passes through a medium that may not be secure itself. Usually, that medium is a computer network. There are many different cryptographic algorithms, each of which can provide one or more of the following services to applications.Itisgenerallyacceptedthat,inordertobeconsideredsecure,apaymentsystemmust satisfy the following fundamental securityrequirements.

3.1.1 Authentication

Theassurancethatthecommunicatingparityistheonethatisclaimstobepreventsthemasquerade of one of the parties involved in the transaction. Both parties should be able to feel comfortable that they are communicating with the party with whom they think they are communicating. Applicationsusuallyperformauthenticationchecksthroughsecuritytokensorbyverifyingdigital Certificates issued by Certificate authorities. Cryptography can help establish identity for authenticationpurposes.

3.1.2 AccessControl

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.)

3.1.3 Data Confidentiality(Secrecy)

Data Confidentiality is the protection of data from unauthorized disclosure. Confidentiality is an essentialcomponentinuserprivacy,aswellasintheProtectionofproprietaryinformation,andas a deterrent to theft of information services. The only way to ensure confidentiality on a public networkisthroughstrongencryption.Dataiskeptsecretfromthosewithoutthepropercredentials, even if that data travels through an insecuremedium.

3.1.4 Data Integrity (Anti-tampering)

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no medications, insertion, deletion, or replay) and prevents the unauthorized medication of data. Financialmessagestravelthroughmultipleroutersontheopennetworktoreachtheirdestinations. We must make sure that the information is not modified intransit.

3.1.5 Non-Repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.

- Non-repudiation, Origin- Proof that the message was sent by the specified party.
- Non-repudiation, Destination- Proof that the message was received by the specified party.
- Non-repudiation is usually provided through digital signatures and public key certificates.

3.2 Types of Attacks on InsecureSystem

3.2.1 NetworkAttacks

These simple services can be used to stop a wide variety of network attacks, including.

3.2.2 Snooping

An attacker watches network traffic as it passes and records interesting data, such as credit card information.

3.2.3 Tampering

An attacker monitors network traffic and maliciously changes data in transit.

3.2.4 Spoofing

An attacker forges network data, appearing to come from a different network address than he actually comes from. This sort of attack can be used to thwart systems that authenticate based on host information.

3.2.5 Hijacking

Once a legitimate user authenticates, a spoofing attack can be used to "hijack" the connection.

3.2.6 Capture-replay

In some circumstances, an attacker can record and replay network transactions to ill effect. For example,saythatyousellasingleshareofstockwhilethepriceishigh.Ifthenetworkprotocolis not properly designed and secured, an attacker could record that transaction, and then replay it later when the stock price has dropped, and do so repeatedly until all your stock isgone.

3.2.7 PIN-guessingattack

An attacker can fake the digits and use the user authentication code (UAC) to launch a PIN-guessing attack.

3.3 Cryptographicattacks

Inordertodefinethesecuritylevelofacryptosystemwehavetospecifythetypeofattackweare assuming and the type of breaking which we wish to prevent. Given these specifications, wehave toshowthatbreakingthecryptosystemwiththespecifiedattackisashardasperformingacertain computational task. The types of attacks are-

3.3.1 Cipher Text-OnlyAttack

Cipher text-only attack in which the adversary sees only cipher texts.

3.3.2 Known-Plaintext

Attack Known-plaintext attack in which the adversary knows the plaintexts (messages) and the corresponding cipher texts transmitted.

3.3.3 Chosen-PlaintextAttack

Chosen-plaintext (CP) attack; where the adversary gets to pick (adaptively); plaintexts of his choice and by exploiting the encryption mechanism he sees their encryption value.

3.3.4 Chosen-Cipher Text (CCT)Attack

Chosen-cipher text (CC) attack - where in addition to access to the encryption mechanism the adversary can pick (adaptively) cipher texts of his choice and by using the decryption mechanism (as a black box) he gets the corresponding plaintexts.

3.4 Issues of Security Approach to Secure Payment System

3.4.1 Secure SocketsLayer

ProtocolNetscape Inc.originallycreatedtheSecureSocketsLayer(SSL)protocol.Onaccountof its popularity and acceptance, it is now implemented in all web browsers. SSL has two main objectives**:**

- To ensure confidentiality, by encrypting the data that moves between the communicating parties (client and the server).
- To provide authentication of the session partners using RSA algorithm.

A. the SSL Handshake protocol, in which the communicating parties (client and the server) authenticate themselves and negotiate an encryption key. One point to note here is that the SSL there is significant additional overhead in starting up an SSLsession.

B. the SSL Record protocol, in which the session data is exchanged between the communicating parties(clientandtheserver)inanencryptedfashion.SSLisagreatboontothetraditionalnetwork protocols, because it makes it easy to add transparent confidentiality and integrity services to an otherwise insecure TCP-based protocol. It can also provide authentication services, the most important being that clients can determine if they are talking to the intended server, not some attacker that is spoofing the server. SSL is currently the most widely deployed security protocol. It is the security protocol behind secure HTTP (HTTPS), and thus is responsible for the littlelock in the corner of your web browser. SSL is capable of securing any protocol that works over TCP. AnSSLtransactionstartswiththeclientsendingahandshaketotheserver.Intheserver'sresponse, it sends its certificate. As previously mentioned, a certificate is a piece of data that includes a public key associated with the server and other interesting information, such as the owner of the certificate, its expiration date, and the fully qualified domain name associated with theservers.

3.4.2 Secure ElectronicTransaction

To carry out transactions successfully and without compromising security and rust, business communities, financial institutions and companies offering technological solutions wanted a protocol that works very similar to the way how a credit card transactions work Visa and MasterCard, leading credit card companies in the world formed a consortium with computer vendors such as IBM and developed an open protocol which emerged as a standard in ensuring security, authenticity, privacy and trust in electronic transactions. The main business requirements for SET are:

- Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a branded payment card account.
- Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring Financial Institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network provider.

The goal of SET is to ensure that the payment process is private, convenient and most-important-of-all-secure.

3.4.3 DSecure

The main advantage over SSL/TLS is that 3-D Secure provides credit card authorization andnon-repudiation.3-DSecureisbuiltupontherelationshipsbetweenthreedomains,namedtheacquirer, the issuer, and interoperability domains .The acquirer domain covers the relationship between the merchant and the acquirer. The issuer domain covers the relationship between the cardholder and the issuer. The interoperability domain supports the relationship between the acquirer and issuer domains. To protect the security of communication between the various entities, 3-D Secure requires the following links to be protected using SSL/TLS: cardholder merchant, cardholder-ACS, merchant Visa Directory, and Visa Directory-ACS (access controlsever).

3.5 CyberCash

The Cyber Cash provide several separate payment services on the Internet including credit card and electronic cash. Cyber Cash uses specialized software on the merchant and customer's sides of the connections to provide secure payments across the Internet.

3.6 The Secure Electronic Payment System Using Secure CommunicationTunnel

Secure electronic payment system consists of four system participants (segments). The communication between the participants goes through secure communication tunnels.

3.7 Secure CommunicationTunnel

Means provide a secure way for communication between two or more parties or segments, i.e., Customer to merchant and merchant to payment gateway.

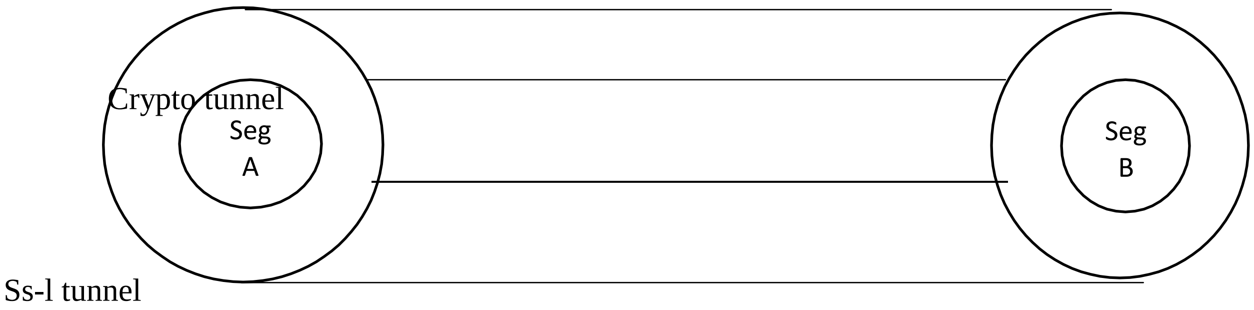


Figure 3.1: Secure Communication Tunnel Consists Of SSL and NestedCrypto Tunnel

Secure communication tunnel consists of SSL and nested crypto tunnel, which is created by employing cryptographic algorithms and techniques on the information that aretransmitted between parties. The SSL is based on session key and Crypto tunnel is based on public key cryptosystem. These Secure communication tunnel are work between customer to merchant and merchant to payment gateway and transfer datasecurely.

Surveillance solution for E-Payment system

Internet security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Internet security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned a user nameandpasswordorotherauthenticatinginformationthatallowsthemaccesstoinformationand programs within theirauthority.

The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensuresthatalldatapassedbetweenthewebserverandbrowsersremainprivateandintegral.SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. The objective of internet security includes protection of informationandpropertyfromtheft,corruptionornaturaldisasterwhileallowinginformationand propertytoremainaccessibleandproductivetoitsindentedusers.Theseareimportantfeaturesof security – confidentiality, authentication, integrity, non-repudiation, non-deny, availability, identification.

Implementation of technology solutions for all the security services is based on cryptographic techniques. Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks.

Cryptographyisthestudyof"Secret(crypto-)writing(-graphy).Theartorscienceencompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form Modern electronic cryptosystems use complex mathematical algorithms and other techniques and mechanisms to provide network and informationsecurity.

Cryptography-based security technologies commonly use one or more of the following basic components to provide security functions:

- Encryption algorithms
- Message digestfunctions
- Hashed Message Authentication Code (HMAC) functions
- Secret key exchange algorithms
- Digital signatures

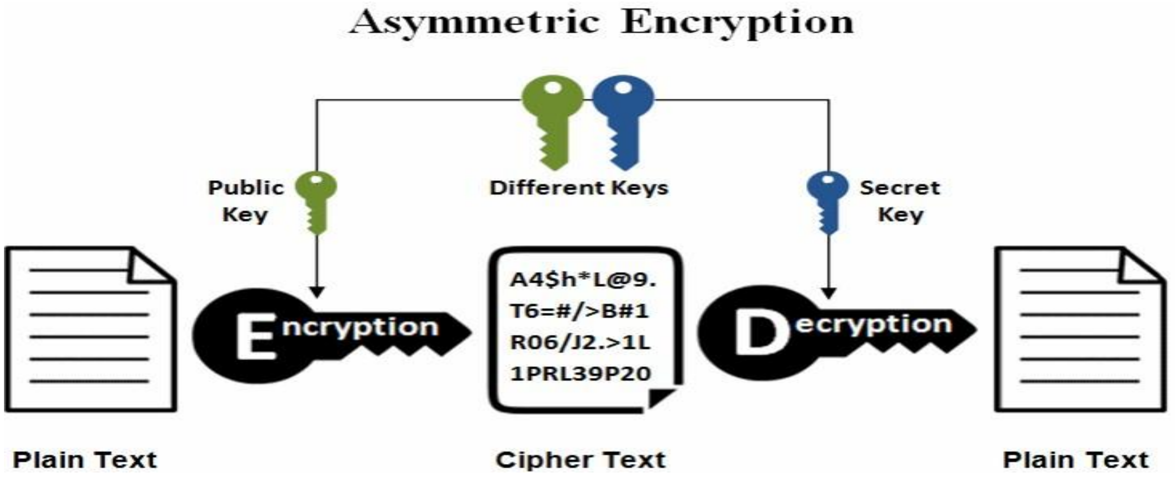


Figure 3.2: Asymmetric Encryption

Plaintext	**The Original Intelligible Message**
Cipher text	The transformed message.
Cipher	An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution.
Key	Some critical information used by the cipher, known only to the sender & receiver.
Encipher (encode)	The process of converting plaintext to cipher text.
Decipher (decode)	The process of converting cipher text back into plaintext.

Symmetricsystemsoperateeitherintheblockcipherorinthestreamciphermode.Thesecretkey is shared between two persons or entities it is very important to be able to ensure the secure exchange of the secretkey.

Asymmetric or Public Key Cryptosystems are built around the possession of a pair of keys – a public key and a private key – by each entity wishing to engage in secure communication. Public key is known to everyone and private key is known to the owner. The algorithm used to generate these keys is such that if either of the keys is used to encrypt a message only the other corresponding key is the key pair will be able to decrypt it. Public key cryptosystems are used to provide both the services of confidentiality and authentication.

One of the most popular and widely used public key cryptosystems is the RSA algorithm developed in 1978 by Ron Rivest, Adi Shamir and Len Adleman of MIT. Digital signatures are not used only to verify the authenticity of the message and the claimed identity of the sender, but also to verify message integrity. Using RSA cryptosystem, a message is encrypted with the sender's private key to generate the 'signature'. The message is then sent to the destination along withsignature.Therecipientdecryptsthesignatureusingsender'spublickey,andifresultmatches with the copy of the message received, the recipient can be sure that the message was sent by the claimed originator and that the message has not been modified duringtransmission.
A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system to protect private network and individuals machines from the dangers of the greater internet, a firewall can be employ to filter incoming or outgoing traffic based on a predefined set of rules called firewalls policies

Chapter 4
Algorithms

4.1 RSA Algorithm

The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. Itcanbeusedtoencryptamessagewithouttheneedtoexchangeasecretkeyseparately.TheRSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring largeintegers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A justusesB'spublickeytoencryptthemessageandBdecryptsitusingtheprivatekey,whichonly he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's publickey.

4.2 Key Generation Algorithm

This is the originalalgorithm

Generate two large random primes, pp and qq, of approximately equal size such that their product $n=pqn=pq$ is of the required bit length, e.g. 1024bits.

Compute $n=pqn=pq$ and $\phi=(p-1)(q-1)\phi=(p-1)(q-1)$.
Choose an integer ee, $1<e<\phi 1<e<\phi$, such that $\gcd(e,\phi)=1\gcd(e,\phi)=1$.
Compute the secret exponent dd, $1<d<\phi 1<d<\phi$, such that $ed\equiv 1 \bmod \phi ed\equiv 1 \bmod \phi$.
The public key is $(n,e)(n,e)$ and the private key $(d,p,q)(d,p,q)$. Keep all the values d, p, q and $\phi\phi$ secret.
n is known as the modulus.
e is known as the public exponent or encryption exponent or just the exponent.
d is known as the secret exponent or decryption exponent.

4.3 A Practical Key Generation

Algorithm: Generate an RSA keypair.

INPUT: Required modulus bit length, kk.
OUTPUT:AnRSAkeypair $((N,e),d)((N,e),d)$whereNisthemodulus,theproductoftwoprimes $(N=pqN=pq)$ not exceeding kk bits in length; ee is the public exponent, a number less than and coprime to $(p-1)(q-1)(p-1)(q-1)$; and dd is the private exponent such that$ed\equiv 1 \bmod (p-1)(q-1)ed\equiv 1 \bmod (p-1)(q-1)$.

```
Select a value of ee from 3,5,17,257,655373,5,17,257,65537
repeat
   p ← genprime(k/2)
until $(p \bmod e)\neq 1(p \bmod e)\neq 1$
repeat
   q ← genprime(k - k/2)
until $(q \bmod e)\neq 1(q \bmod e)\neq 1$
```

```
N ← pq
L ← (p-1)(q-1)
d ← modinv(e, L)
return (N,e,d)
```

The function generic prime (b) returns a prime of exactly bb bits, with the bit set to 1. Note that the operation k/2k/2 is integer division giving the integer quotient with no fraction.

If you've chosen e=65537e=65537 then the chances are that the first prime returned in steps (3) and (6) will pass the tests in steps (4) and (7), so each repeat-until loop will most likely just take one iteration. The final value of NN may have a bit length slightly short of the target kk. This actually does not matter too much (providing the message m is always < N), but some schemes require a modulus of exact length.

Encryption

Sender A does the following:-

Obtains the recipient B's public key (n,e)(n,e).

Represents the plaintext message as a positive integer mm with 1<m<n1<m<n.

Computes the cipher text c=memodnc=memodn.

Sends the cipher text cc to B.

Decryption

Recipient B does the following:-

Uses his private key (n,d)(n,d) to compute m=cdmodnm=cdmodn.

Extracts the plaintext from the message representative mm.

Digital Signing

Sender A does the following:-

Creates a message digest of the information to be sent.

Represents this digest as an integer mm between 1 and n−1n−1

Uses her private key (n,d)(n,d) to compute the signature s=mdmodns=mdmodn.

Sends this signature ss to the recipient, B.

Signature verification

Recipient B does the following (older method):-

Uses sender A's public key (n,e)(n,e) to compute integer v=semodnv=semodn.

Extracts the message digest HH from this integer.

Independently computes the message digest H′H′ of the information that has been signed.

If both message digests are identical, i.e. H=H′H=H′, the signature is valid.

More secure method:-

Uses sender A's public key (n,e)(n,e) to compute integer v=semodnv=semodn.

Independently computes the message digest H′H′ of the information that has been signed.

Computes the expected representative integer v′v′ by encoding the expected message digest H′H′.

If v=v′v=v′, the signature is valid.

4.4 Summary of RSA

n=pqn=pq, where pp and qq are distinct primes.
ϕ=(p−1)(q−1)ϕ=(p−1)(q−1)
e<ne<n such that gcd(e,ϕ)=1gcd(e,ϕ)=1
d=e−1modϕd=e−1modϕ
c=memodn,1<m<nc=memodn,1<m<n
m=cdmodn

4.5 KeyLength

When we talk about the key length of an RSA key, we are referring to the length of the modulus, nn, in bits. The minimum recommended key length for a secure RSA transmission is currently at least 1024 bits. A key length of 512 bits is no longer considered secure, although crackingitisstillnotatrivialtaskforthelikesof youandme.Thelonger yourinformationneeds to be kept secure, the longer the key you should use. Keep up to date with the latest recommendations in the securityjournals.

There is one small area of confusion in defining the key length. One convention is that the key length is the position of the most significant bit in nn that has value '1', where the least significant bit is at position 1. Equivalently, key length = ⌈log2 (n+1)) ⌉⌈log2⁡ (n+1)) ⌉, where ⌈x⌉⌈x⌉ is theceilingfunction,theleastintegergreaterthanorequaltoxx.Theotherconvention,sometimes used, is that the key length is the number of bytes needed to store nn multiplied by eight, i.e. ⌈log256 (n+1) ⌉×8⌈log256⁡ (n+1)⌉×8.

The key used in the RSA is an example. The modulus is represented in hex form as

```
0A 66 79 1D C6 98 81 68 DE 7A B7 74 19 BB 7F B0
C0 01 C6 27 10 27 00 75 14 29 42 E1 9A 8D 8C 51
D0 53 B3 E3 78 2A 1D E5 DC 5A F4 EB E9 94 68 17
01 14 A1 DF E6 7C DC 9A 9A F5 5D 65 56 20 BB AB
```

The most significant byte 0x0A in binary is 00001010'B. The most significant bit is at position 508, so its key length is 508 bits. On the other hand, this value needs 64 bytes to store it, so the key length could also be referred to by some as 64 x 8 = 512 bits. We prefer the former method. YoucangetintodifficultieswiththeX9.31methodforsignaturesif youusethelatterconvention.

4.6 Minimum KeyLengths

The following table is taken from NIST's Recommendation for Key Management. It shows the recommendedcomparablekeysizesforsymmetricalblockciphers(AESandTripleDES)andthe RSA algorithm. That is, the key length you would need to use to have comparablesecurity.

Table 4.1: Comparable Table

Symmetric key algorithm	Comparable RSA key length	Comparable hash function	Bits of security
2TDEA*	1024	SHA-1	80
3TDEA	2048	SHA-224	112
AES-128	3072	SHA-256	128
AES-192	7680	SHA-384	192
AES-256	15360	SHA-512	256

4.7 Data Encryption Standard(DES)

DES(DataEncryptionStandard)algorithmpurposeistoprovideastandardmethodforprotecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process.

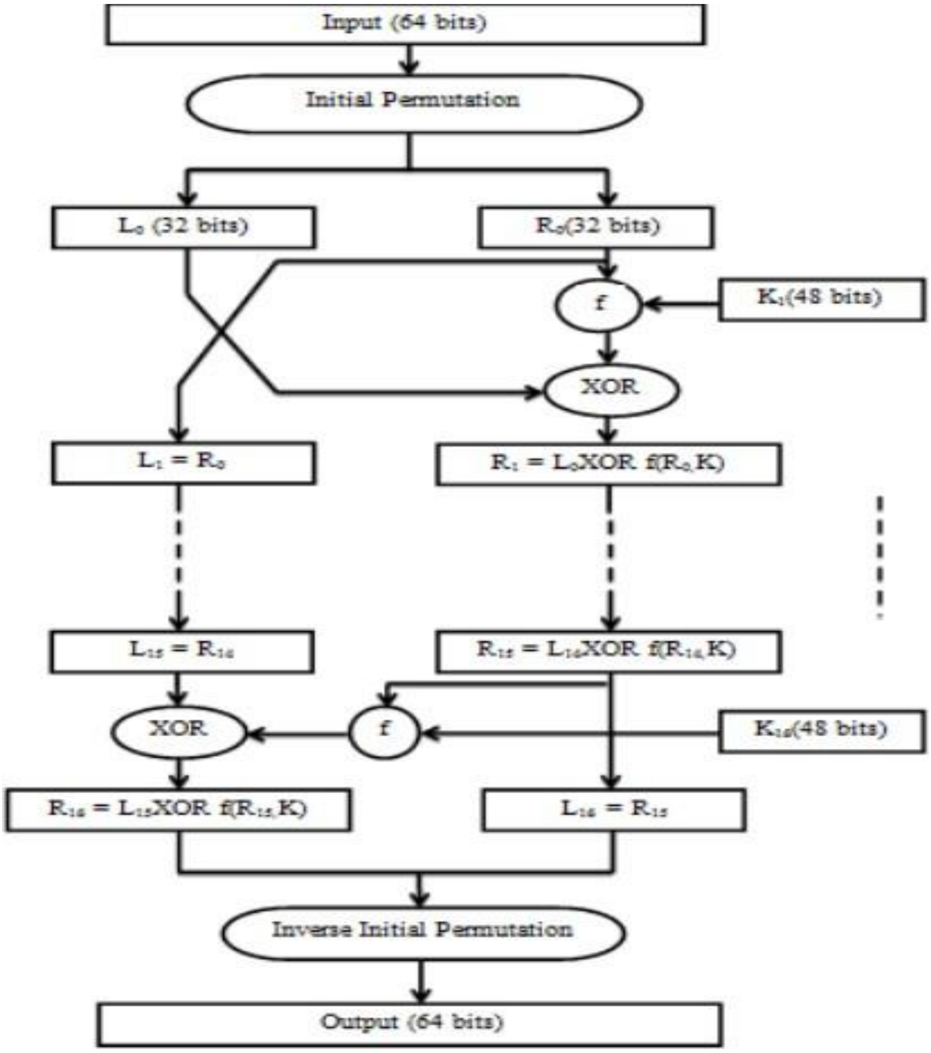


Figure 4.1: Data Encryption Standard (DES)

DES algorithm consists of the following steps

i. Encryption

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.

2. The plaintext block has to shift the bits around.

3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.

4. The plaintext and key will processed by following

i. The key is split into two 28 halves

ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.

iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.

iv. The rotated key halves from step 2 are used in next round.

v. The data block is split into two 32-bit halves.

vi. One half is subject to an expansion permutation to increase its size to 48 bits.

vii. Output of step 6 is exclusive-OR'ed with the 48- I it compressed key from step 3.

viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.

ix. Output of step 8 is subject to a P-box to permute the bits.

x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

4.8 Advanced Encryption Standard(AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure - 2. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

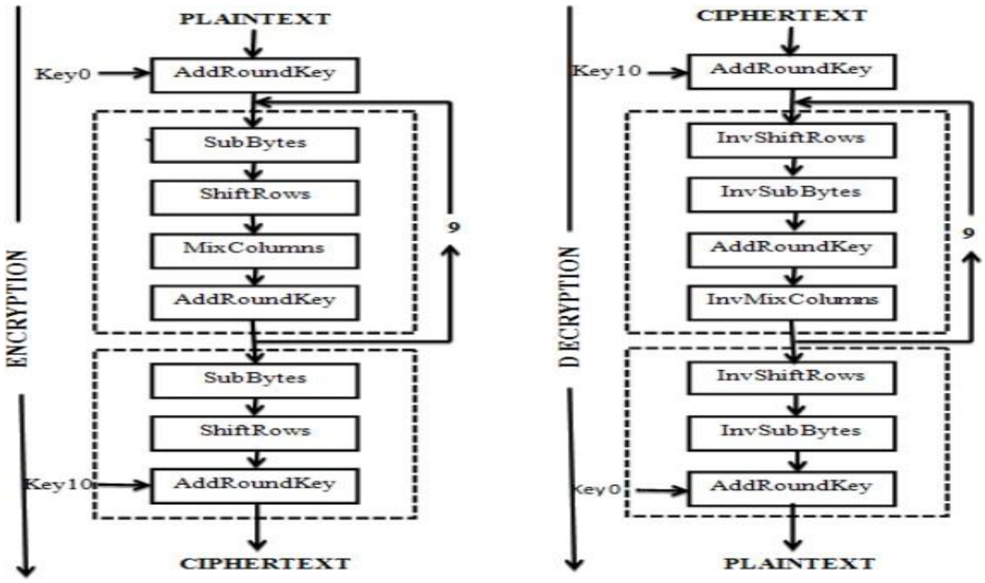


Figure 4.2: Advanced Encryption Standard (AES)

i. Algorithm Steps: These steps used to encrypt 128-bit block
1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. Usual Round: Execute the following operations which are described above.
1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K (round)

iii. Final Round: Execute the following operations which are described above.
1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K (10)

iv. Encryption:

Each round consists of the following four steps:

I. Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii. Shift Rows: In the encryption, the transformation is called Shift Rows.

iii. Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv. Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.ThelaststepconsistsofXORingtheoutputofthepreviousthreestepswithfourwords from the key schedule. And the last round for encryption does not involve the “Mix columns” step. [8]

v. Decryption:

Decryption involves reversing all the steps taken in encryption using inverse functions like:

- Inverse substitutebytes,
- Inverse shift rows,
- Add round key, and
- Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the “Inverse mix columns”step.

4.9 Comparison

In the table 2 below a comparative study between AES, DES and RSA is presented in to eighteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, InherentVulnerabilities, Key used, Rounds, Stimulation Speed, Trojan horse, Hardware & Software Implementation and Ciphering & DecipheringAlgorithm.

Table 4.2: Comparison AES, DES, RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 129, 256 bits	56 bits	>1024 bits
Block Size	128	64	Minimum 512 bits
Ciphering & Deciphering Key	Same	Same	Different
Scalability	No Scalable	It is Scalable Algorithm due to varying the key size and Block Size	No Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent	No Secure Enough	Least Secure
Deposit of Key	Needed	Needed	Needed

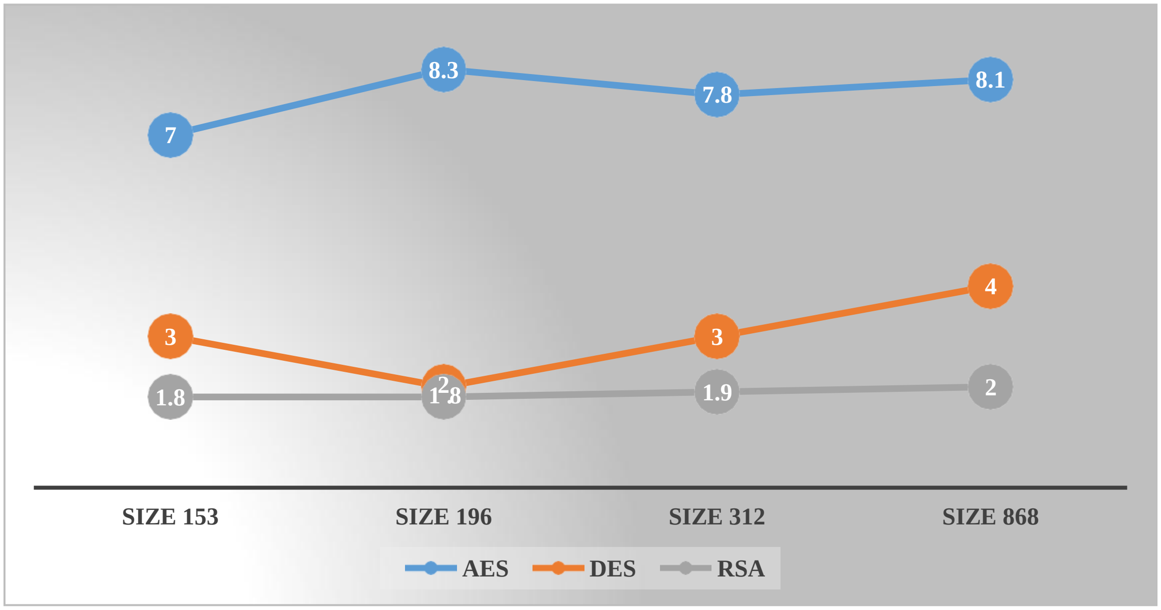
Inherent Vulnerabilities	Brute Forced	Brute Forced, Linear and Differential Cryptanalysis attack	Brute Forced and Oracle Attack
Key Used	Same key Used For Encrypt and Decrypt	Same Key Used for Encrypt andDecrypt	Different Key Used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation	Faster	Faster	Faster
Trojan Horse	Not Proved	No	No
Hardware & Software Implementation	Faster	Better In Hardware Than in Software	No Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

Table 4.3: Comparison AES, DES, RSA

S.NO	Algorithm	Packet size (kb)	Encryption size (sec)	Decryption size (sec)
1. 2. 3.	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9
1. 2. 3.	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
1. 2. 3.	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
1. 2. 3.	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

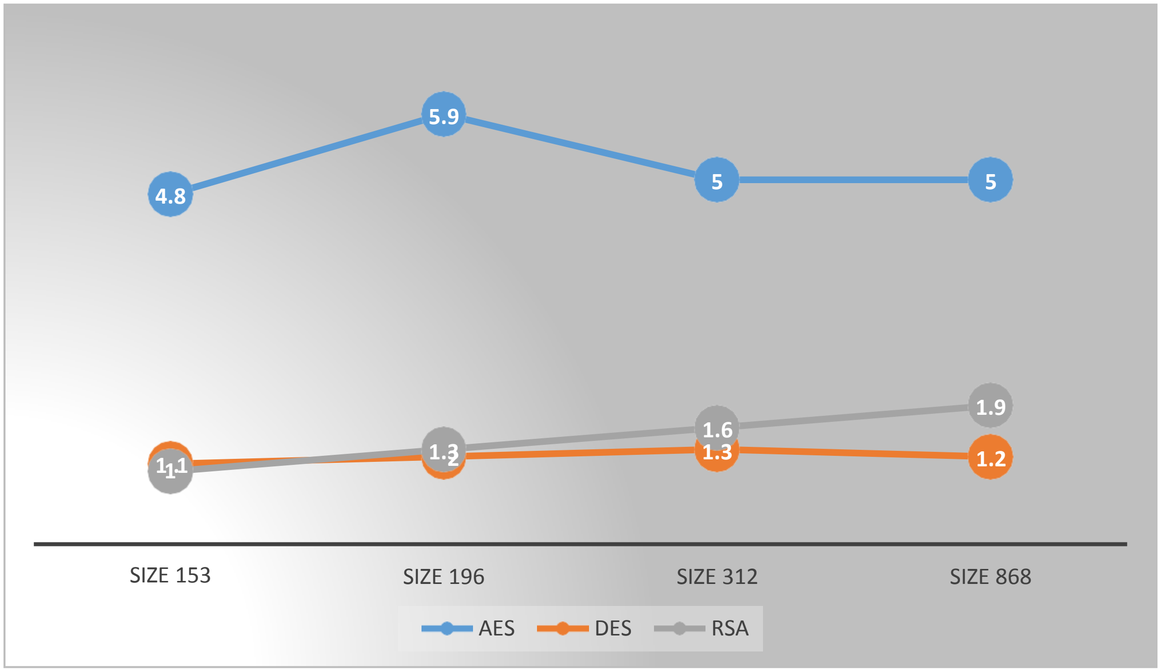
By analyzing table-3, Time taken by RSA algorithm for both encryption and decryption process is much higher compare to the time taken by AES and DES algorithm.

Figure 4.3: Comparison of DES, AES, and RSA Encryption Time Among



By analyzing, tab-4 Tab-5 which shows time taken for encryption and decryption on various size offilebythreealgorithms.RSAalgorithmtakesmuchlongertimecomparetotimetakenbyAES and DES Algorithm. AES and DES algorithm show very minor difference in time taken for encryption and decryptionprocess.

Figure 4.4: Decryption Time among DES, AES, and RSA Comparison



Chapter 5
Proposed Model

5.1 Flow Diagram

The data security in almost every field is a challenging concern all around the globe. The applicationareamaybeaswideintheareaofbanking,internet,networkandmobiledataetc.The main focus of this paper is to secure the text data and provide a comparison with different parameters. DES and RSA are being used for comparison. A hybrid approach has been proposed inthispaperbasedonthecombinationofDESandRSAalgorithm.Thecomparisonisdoneonthe basisofsize,length,numberofkeysandthetimeofencryptionanddecryption.Theoverallresults suggest the hybrid encryption approach for the encryption and decryptionprocess.

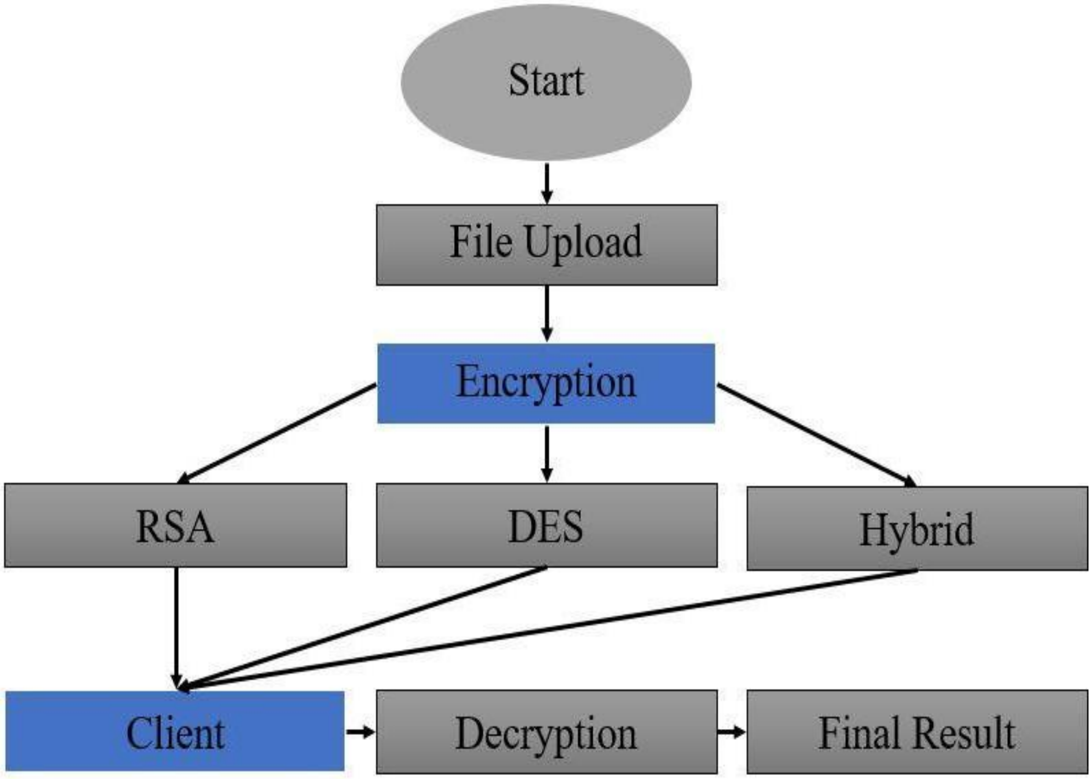


Figure 5.1: Hybrid Algorithm Process

5.2 RSA Flowchart Process

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs. RSA is an algorithm for public key encryption. It was the first algorithm knowntobesuitableforsigningaswellasencryption,andoneofthefirstgreatadvancesinpublic key encryption. It involves threesteps:

- KeyGeneration
- Encryption
- Decryption

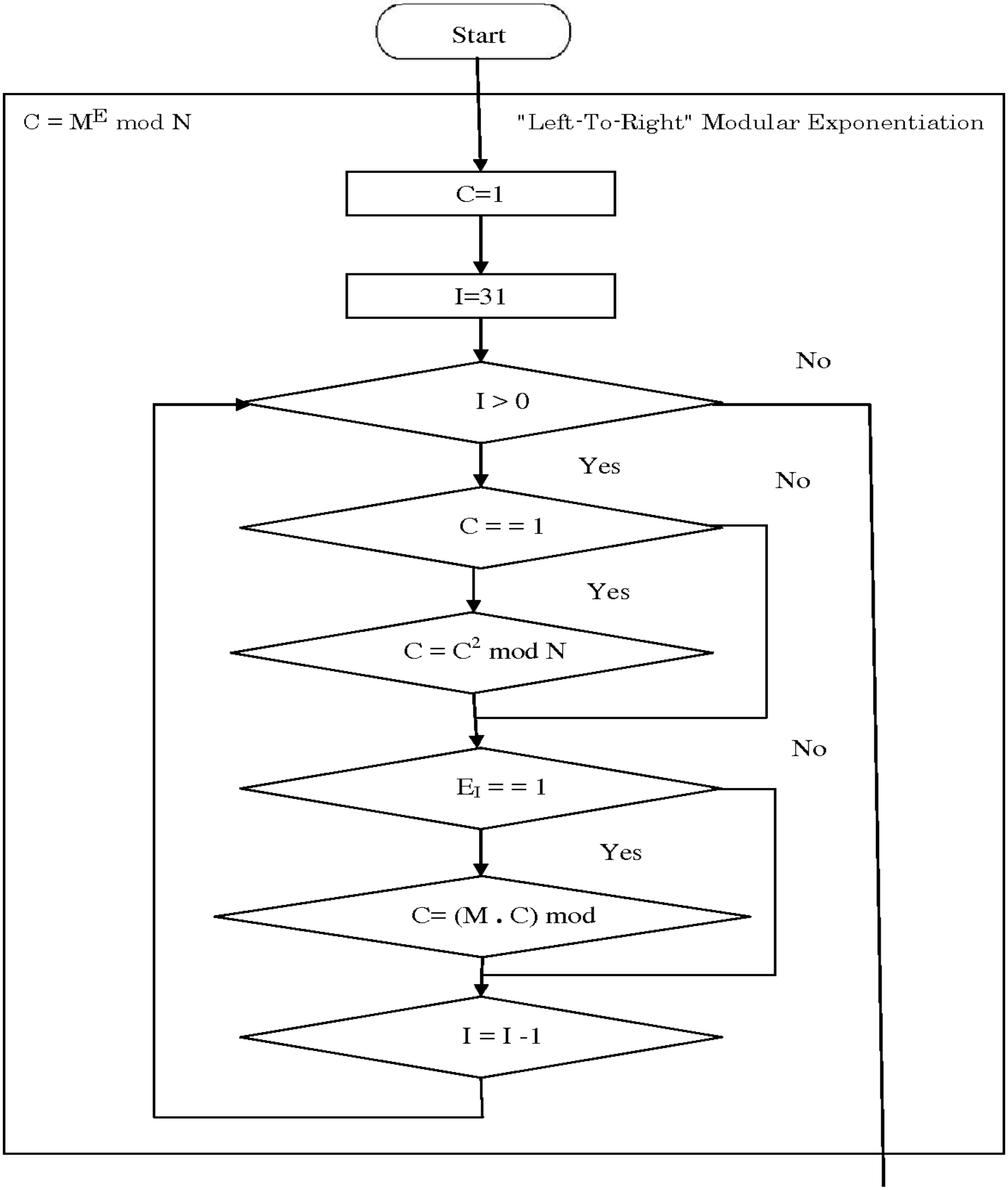


Figure 5.2: RSA Flowchart Process

If we take the two prime numbers very large it enhances security but requires implementation of Exponentiation by squaring algorithm and square and multiply algorithm for effective encryption and decryption. For simplicity the program is designed with relatively small prime numbers.

5.3 Proposed Solution

This research is the extension of card less electronic payment system whose framework is shown in following:

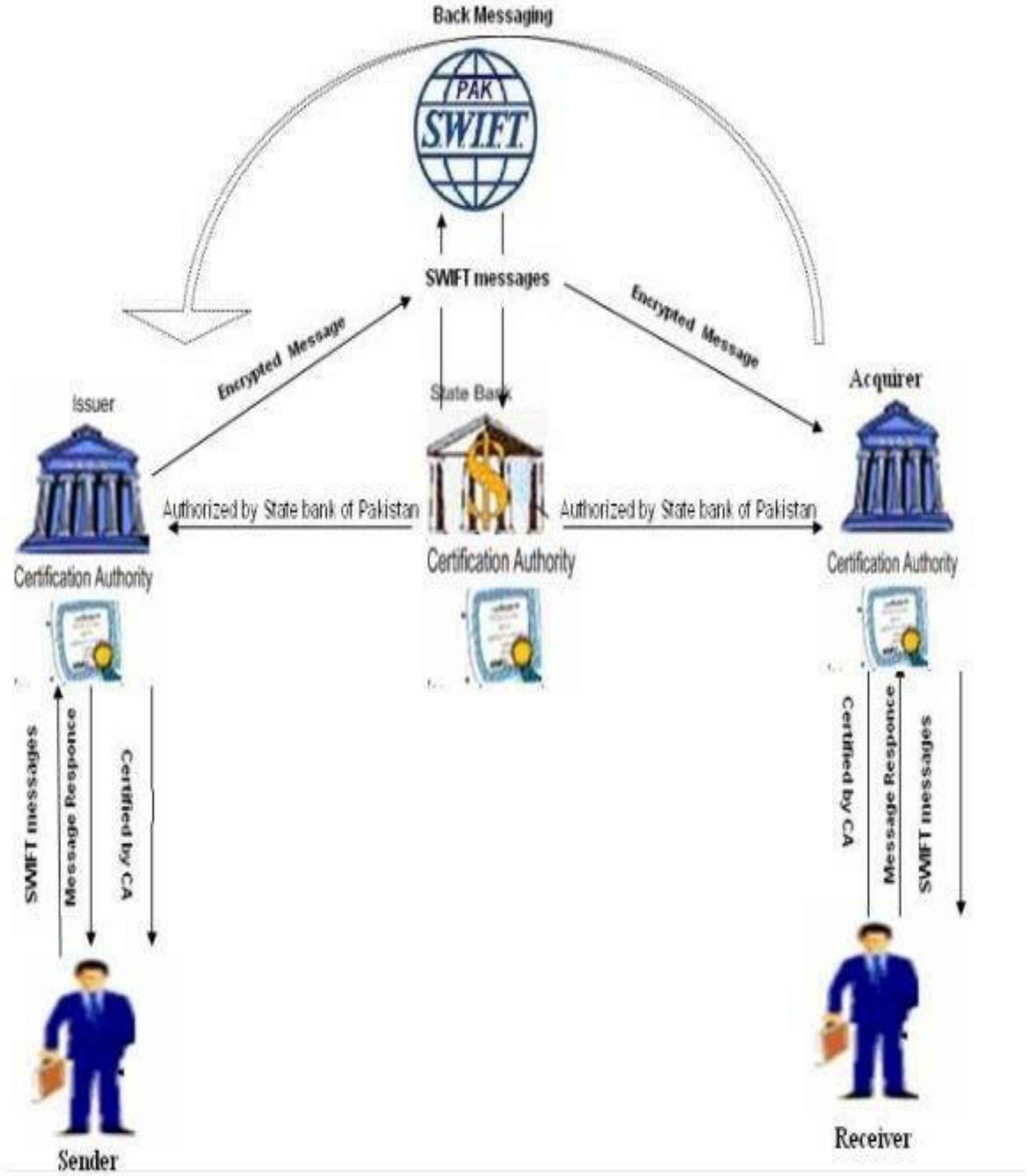


Figure 5.3: Card less Electronic System

In figure 7 a model is presented for the card less electronic transactions and messages were used instead of cards. A modified model is proposed in this research as shown in figure 8 which make the electronic transactions secure by enhancing the confidentiality of messages in a card less electronic payment system.

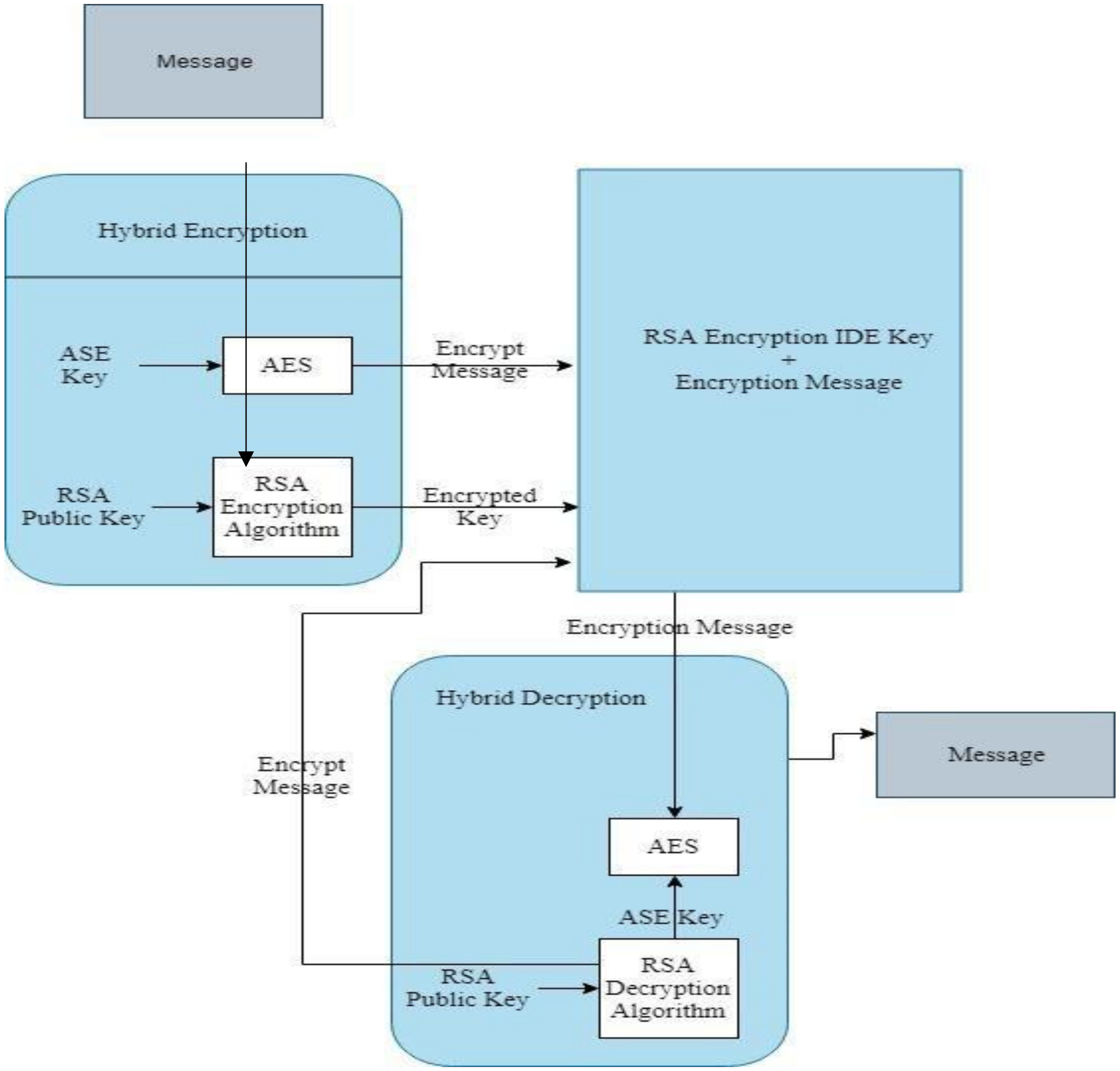


Figure 5.4: Electronic Transactions Secure By Enhancing the Confidentiality of Messages

In this model message is encrypted using both the symmetric and asymmetric algorithm. Symmetric encryption is used for its convenience and asymmetric encryption is used for its efficiency. Sender encrypts the message with the key of symmetric algorithm (AES) and then encryptsthiskeywiththepublickeyofanasymmetricalgorithm(RSA).Thereceiverfirstdecrypts the symmetric key with the private key of the asymmetric algorithm (RSA) and then the actual message with this symmetric key(AES).

The basic steps of the proposed model are as follows:

- Message is encrypted with the key of AES algorithm (symmetric algorithm).
- The symmetric key is then encrypted with the public key of RSA (asymmetric algorithm)
- Both the message and the key are sent to the receiver.
- The receiver receives the encrypted message and the key.
- The receiver decrypts the key with the private key of RSA (asymmetric algorithm).
- The receiver then decrypts the message with decrypted symmetric key of AES.

Chapter 6
Experimentation and Result

6.1 Introduction

In this model message is encrypted using both the symmetric and asymmetric algorithm. Symmetric encryption is used for its convenience and asymmetric encryption is used for its efficiency. Sender encrypts the message with the key of symmetric algorithm (AES) and then encrypts this key with the public key of an asymmetric algorithm (RSA).

6.2 Experiment

Threepairofencryption/decryptionalgorithmsiscomparedonthebasisoftimeconsumptionand memory consumption to check which pair of algorithms is more efficient for hybrid encryption/decryptionofmessages.Threedifferentmessagelengthsareusedandresultsaredrawn as shown in the followingtable

Table 6.1: Comparison 3 Pair

Message Size	RSA-AES		RSA-DES		RSA-3DES	
	Time Consumed	Memory Consumed	Time Consumed	Memory Consumed	Time Consumed	Memory Consumed
56 bits	273ms	3311 4kb	216ms	3276 8kb	287ms	3768 3kb
256 bits	307ms	5046 7kb	266ms	3768 3kb	290ms	3772 3kb
512 bits	311ms	5734 4kb	278ms	3768 3kb	309ms	4096 0kb

Figure 9: shows results of time consumed by the three pairs of algorithm in graphical form. It illustrates the execution time in milliseconds taken by each pair of algorithms to hybrid encrypt/decrypt the message of three different sizes.

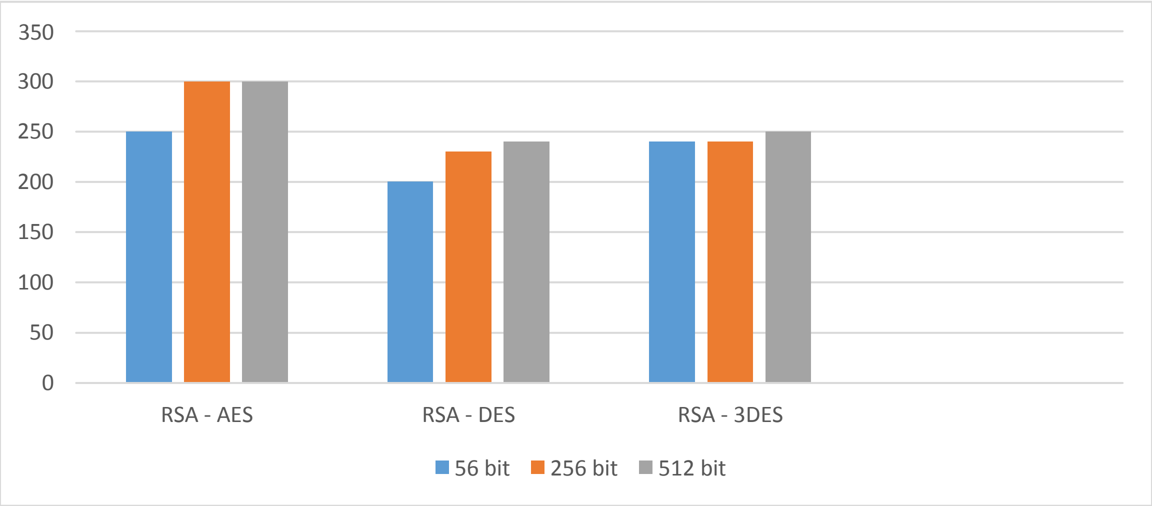


Figure 6.1: Hybrid Encrypt/Decrypt the Message of Three Different Sizes

The graph shows that the combination of RSADES takes minimum time so it executes faster than others. Figure 10 shows the graph of memory consumption. Three different message sizes were taken. The memory consumed is in kilo bytes. It shows that RSA-DES consumes less memory.

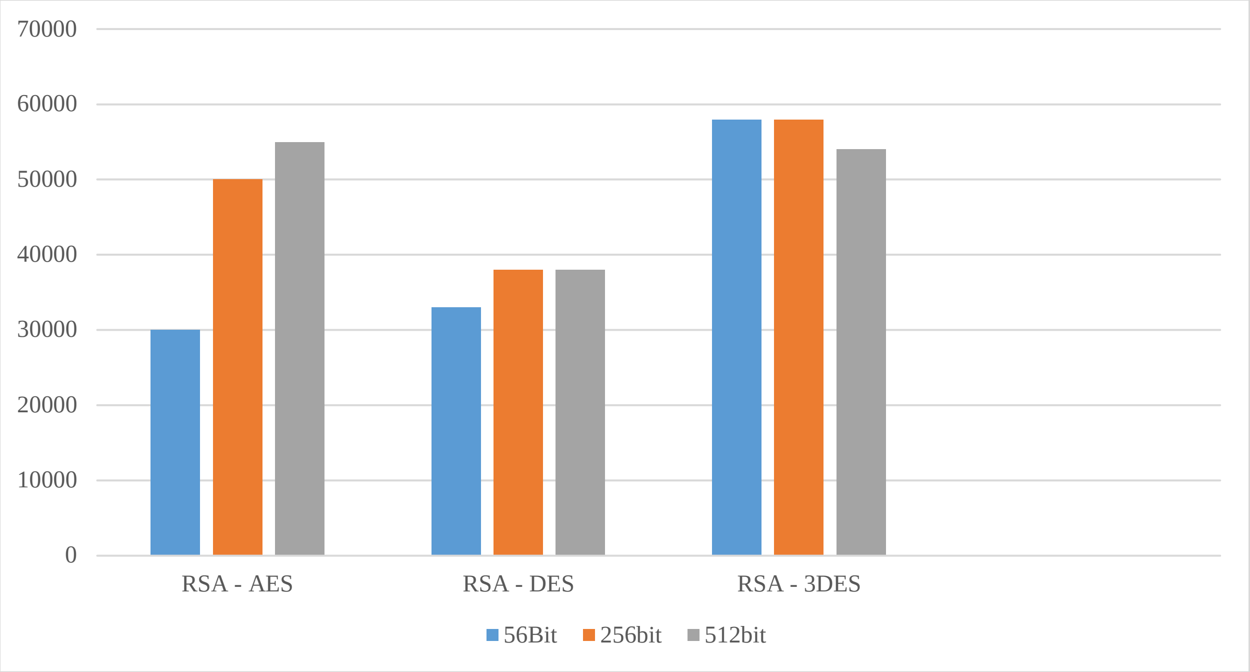


Figure 6.2: RSA-DES Consumes less Memory

Chapter 7
Conclusion

7.1 Conclusion

Electronictransactionshaverevolutionizedtheworldbutiftheyarenotsecurethenhugefinancial damages can occur. Developing countries need a secure system on which they can easily and securelydotransactions.Thisresearchpurposedasystemwhichenhancesthesecurityofthecard less e-payment system by increasing the confidentiality of messages thus minimizing the risk of critical information leakage. Only authorized persons can send, view and receive the messages whichholdthetransactioninformation.Asecureelectronictransactionisachievedinthepurposed system by applying the hybrid encryption/decryption technique on the messages. For future work the integrity and availability of messages can be done and it can be achieved by applying hashing algorithms on themessages.

7.2 FutureScope

This system is flexible to be implemented by the user in many ways as he desires i.e. the number of algorithms to be used, the sequence of algorithms and even the algorithms to be used mayvary from user to user. This ideally makes it strenuous for the attacker to attack or decipher the plain inputtextunlessheknowsthealgorithmsusedintheprocessof encryption,thesequencetheyare used in, etc. as the sequence is vital for decryption. This flexibility enables a wide range of uses and also enables accommodation of new algorithms as and when they are developedin the future. Inanotherinnovativeapproach,apasswordmaybesetwhichwouldhelpdecidethealgorithmsto be used from an array of them and also the sequence of those algorithms to be used would be decided by the unique password which would also be needed for decryption. A software can be built for this purpose consisting many algorithms and then as soon as it receives password and data, it computes the algorithms to be used and their sequence based on the password and applyit to the data and during decryption, follow the same process and input the encrypted text and password to decrypt. This would improve the efficiency of the hybrid systemgreatly.

REFRENCES:

[1] Book “cryptography and network security: Principles and practice” by William stalling 3rd edition, volume: 7, August2004.

[2]http://en.wikipedia.org/wiki/Hybrid_cryptosystem

[3] Beenish Khan Baloch, Naveed Khan Baloach, Aihab Khan, Shiraz Baig, “Design level Architecture and Messaging of Cardless System for Electronic Payments”, BSE (st) research thesis, Fatimah Jinnash Women University, The Mall Rawalpindi,2009.

[4] M.Ayoub Khan, Y.P.Singh, “On the security of Joint Signature and Hybrid Encryption”, Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication, vol.1, no.,pp.1-4,

[5] Mathew, S Jacob, K.P, "A Novel Fast Hybrid Cryptographic System: MARS4," India Conference, 2006 Annual IEEE, pp.1-5, 15- 17 Sept.2006

[6] Ganesan, R.; Vivekanandan, K, "A Novel Hybrid Security Model for E-Commerce Channel," Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09, pp.293-296,27-28-Oct.2009

[7] Ravi Kalakota and Andrew B. Whinston, Frontiers of Electronic Commerce, Pearson Education Ltd., Singapore,2004.

[8] KamleshK.BajajandDebjaniNag,E-Commerce-theCuttingedgeofBusiness,TataMcgraw-Hill Publishing Co. Ltd., Delhi, 2003

[9] Rachna and Priyanka Singh, “Issues and Challenges of Electronic Payment Systems”, InternationalJournalforResearchinManagementandPharmacy,Vol.2,Issue9,December2013 (IJRMP) ISSN: 2320-0901

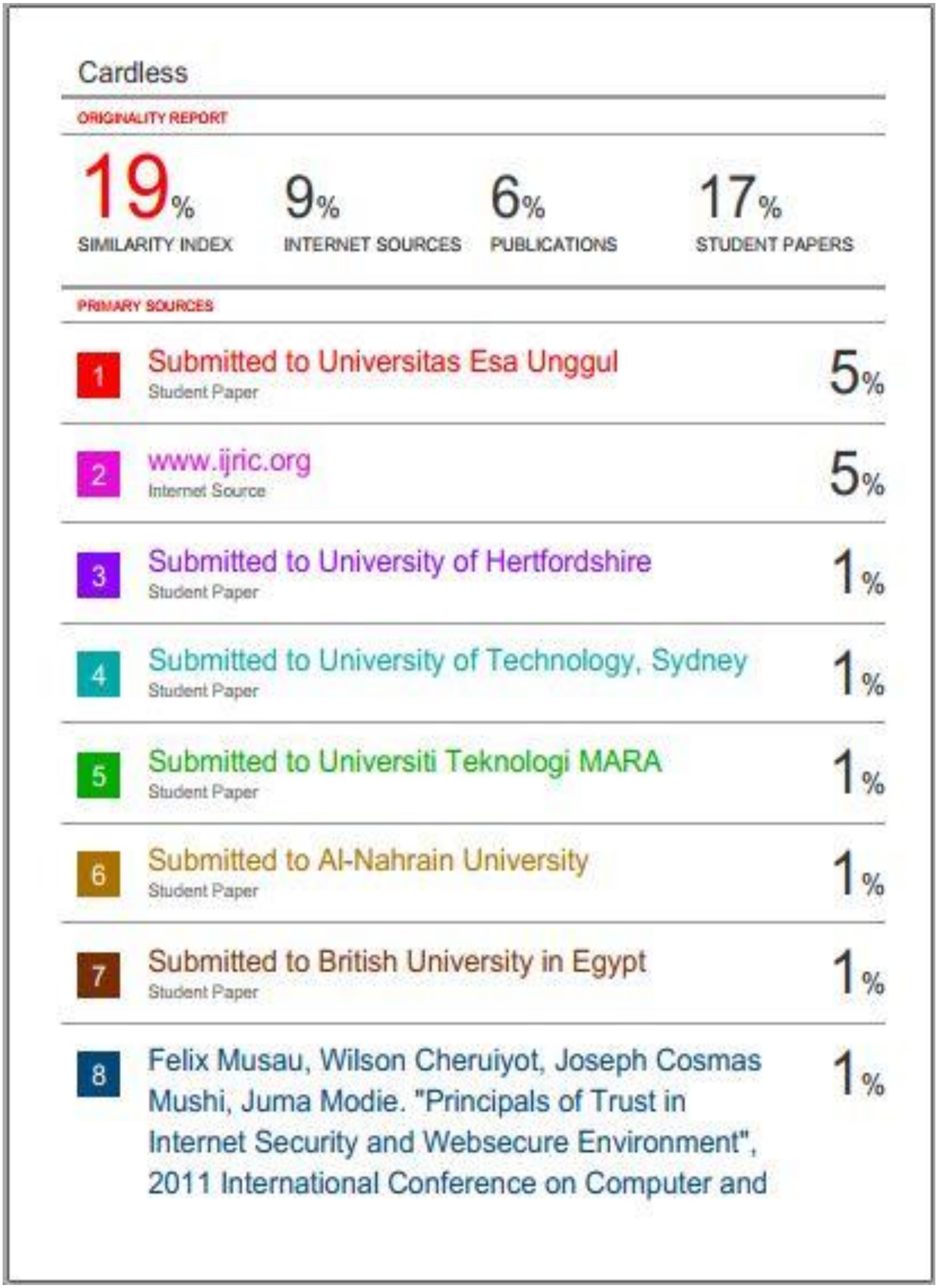
[10] Robert Nzaro and Norest Magid, “Assessing the Role of Electronic Payment Systems in FinancialInstitutions”,GlobalJournalofManagementandBusinessResearch:CFinanceVolume 14 Issue 2 Version 1.0 Year 2014.

[11] Berry Schoenmakers, “Basic Security of the ecash Payment System”,unpublished

[12] K. Böhle, M. Krueger, C. Herrmann, G. Carat, I. Maghiros, “Electronic PaymentSystems”, Institute for Prospective Technological Studies , World Trade Center, 2000

[13] Karamjeet Kaur and Dr. Ashutosh Pathak, “E-Payment System on E-Commerce in India”, Journal of Engineering Research and Applications, ISSN : 2248- 9622, Vol. 5, Issue 2, (Part -1) February 2015, pp.79-87

[14] Deepankar Roy and Amarendra Sahoo, “Payment Systems In India: Opportunities And Challenges”, Journal Of Internet Banking And Commerce, April 2016, Vol. 21, No.2.



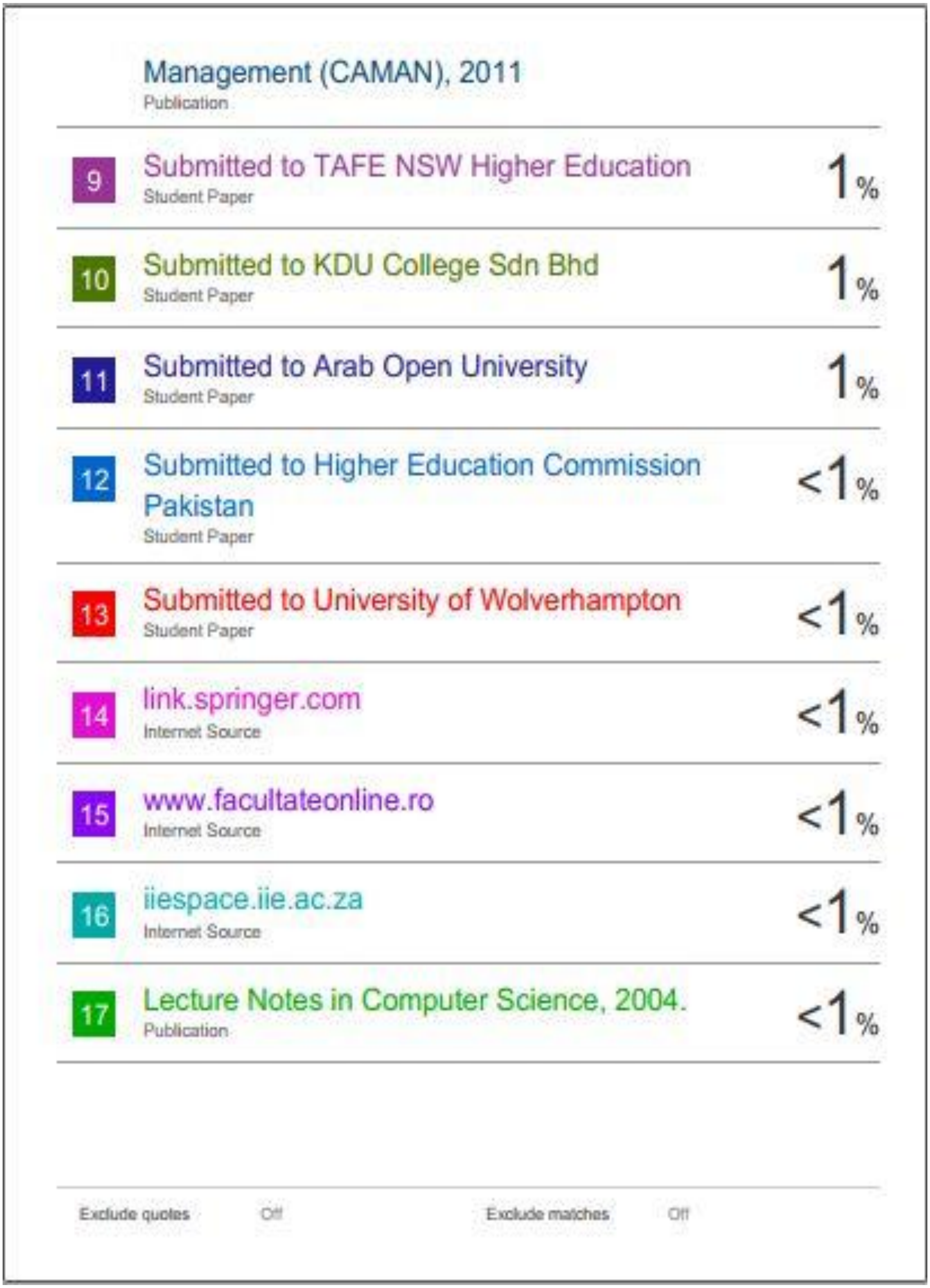
Cardless

ORIGINALITY REPORT

19%	9%	6%	17%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Esa Unggul Student Paper	5%
2	www.ijric.org Internet Source	5%
3	Submitted to University of Hertfordshire Student Paper	1%
4	Submitted to University of Technology, Sydney Student Paper	1%
5	Submitted to Universiti Teknologi MARA Student Paper	1%
6	Submitted to Al-Nahrain University Student Paper	1%
7	Submitted to British University in Egypt Student Paper	1%
8	Felix Musau, Wilson Cheruiyot, Joseph Cosmas Mushi, Juma Modie. "Principals of Trust in Internet Security and Websecure Environment", 2011 International Conference on Computer and	1%



	Management (CAMAN), 2011 Publication	
9	Submitted to TAFE NSW Higher Education Student Paper	1%
10	Submitted to KDU College Sdn Bhd Student Paper	1%
11	Submitted to Arab Open University Student Paper	1%
12	Submitted to Higher Education Commission Pakistan Student Paper	<1%
13	Submitted to University of Wolverhampton Student Paper	<1%
14	link.springer.com Internet Source	<1%
15	www.facultateonline.ro Internet Source	<1%
16	iiespace.iie.ac.za Internet Source	<1%
17	Lecture Notes in Computer Science, 2004. Publication	<1%

Exclude quotes Off

Exclude matches Off