Computer Communications 153 (2020) 125–134

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# Enhancement of e-commerce security through asymmetric key algorithm

Dijesh P. [a,*], SuvanamSasidhar Babu [b], Yellepeddi Vijayalakshmi [c]

[a] Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India
[b] School of Computing and Information Technology, Reva University, Bengaluru, 560064, India
[c] Department of CSE, Karpagam University, Coimbatore, Tamilnadu, India

ARTICLE INFO

*Keywords:*
E-commerce security
Encryption
Decryption
RSA algorithm
Fernet cipher algorithm

ABSTRACT

Electronic commerce offers reduced transaction costs and much convenient mode of business to all over global consumers. This paper explains asymmetric methods which uses electronic commerce transactions and other assisted algorithms of cryptography that are important in set up of electronic commerce working. This study explains the essential security problems in electronic commerce. To avoid the issues of security certain secure conditions must be followed which offers sufficient security to transaction data for every entity in transaction of electronic commerce. In this study a multi-layer encryption algorithm namely RSA encryption algorithm and Fernet cipher encryption algorithm is proposed based on security. Multi-layer encryption algorithm is used to construct a sophisticated and complex approach of encryption. This algorithm integrates the strength of several techniques of encryption at the same time. This study reveals how much safe consumer and payment data order will be managed effectively by security-based approaches. Encryption technique discussed in this study is the major technique to make the transaction over internet secure. A better technology of encryption can decrease the fraudlent activities easily and effectively. This study proposes a multi-layer encryption algorithm and implemented it in order to enable delivery of messages through network in a secure way. This study will be helpful to control the decryption and encryption with the use of private and public key of receiver and sender.

## 1. Introduction

With the development of online technology, an establishment is now existing i.e. electronic commerce based on the technology of multimedia and network. It arranges operation through online sites which is known as open public network i.e. efficient to run different methods of electronic business process. Electronic commerce is an online trade of business which offers secured trade in electronic commerce form. The security of web service plays an essential part in such methods of business. Security is the major problem on internet to develop electronic commerce [1]. Security is on the mind of every electronic commerce entrepreneur who stores, interacts or solicits any data that may be sensitive if lost. Any business that intends to gain competitive advantage over other business must acquire a comprehensive policy of security in discussion with distributors, suppliers and partners that offer secure surroundings for electronic commerce based activities [2]. Due to the rise in warnings by media from privacy and security breaches like financial fraud and identity theft and the extended awareness of internet consumers about the threats of carrying out online transactions, electronic commerce has not been capable to accomplish its full importance. Several customers refuse to carry out internet transactions and associate that to lack of fear or trust for their personal data. The online transaction needs customers to mention their sensitive personal data to vendor placing themselves at essential hazard. Understanding the trust of customer is important for the continuing growth of electronic commerce [3]. Rathi and Gupta [4] have stated that the security of electronic commerce has their own definite distinctions and is one of the biggest noticeable security components that influences end users through their day-to-day payment communication with businesses. Electronic commerce security is the security of electronic commerce properties from illegal access, modification, use or destruction. The electronic security dimensions are non repudiation, integrity, confidentiality, privacy, availability and authenticity. Patro et al. [5] has stated that non repudiation is the deterrence against a single party from another party reneging on a contact after the circumstance. Integrity is the deterrence against illegal change of information. The protection against illegal revelation of information is known as confidentiality whereas privacy is the delivery of data

*Abbreviations:* RSA, Rivest Sharmir Adleman; PKE, Private Key Encryption; PKC, Private Key Cryptography; IFP, integer factorization problem; DLP, Discrete Logarithm Problem; PGP, Pretty Good Privacy; ECC, Elliptic Curve Cryptography; CPK, Cryptographic Public Key; PKI, Public Key Infrastructure; AES, Advanced Encryption Standard; MD5, Message Digest-5; MAC, Message Authentication Code; SHA, Secure Hash Algorithm

* Corresponding author.
*E-mail addresses:* dijeshtirur@gmail.com (P. Dijesh), sasidharmails@gmail.com (S. Babu), vijayasasi11@gmail.com (Y. Vijayalakshmi).

https://doi.org/10.1016/j.comcom.2020.01.033
Received 28 May 2019; Received in revised form 13 August 2019; Accepted 17 January 2020
Available online 31 January 2020
0140-3664/© 2020 Elsevier B.V. All rights reserved.


**Fig. 1.** Major issues in e-commerce industry.
*Source:* TestingExperts, 2019.

control and disclosure. The deterrence against data delays or removal is known as availability whereas authentication is the authentication of data source. The below Fig. 1 shows the major issues in electronic commerce industry:

To resolve the security issues in electronic commerce Secure Electronic transaction, message digest, symmetric key encryption and asymmetric key encryption techniques are used. Secure Electronic Transaction is an extensive protocol of security which uses cryptography to offer confidentiality of data, assure integrity of payment and enable authentication of identity. It depends on digital certificate, cryptography and authentication by messages of text to assure data security and confidentiality [6]. Illayaraja et al. [7] has mentioned that Symmetric key encryption is also referred as private key encryption (PKE) and private key cryptography (PKC). The same key is employed for message decryption and encryption. The symmetric key encryption is known as secret and the encryption technique have 2 issues. The 1st issue is simple symmetric encryption employed which not offers good security of data and 2nd issue is to interchange secret key. Suguna et al. [8] has mentioned that the Public Key Cryptography or Asymmetric key encryption is a set of keys employed for the decryption and encryption process namely Public key for encryption and private or secret key for decryption. To encrypt the text public key is used and to decrypt the encrypted text private key is used. The Public Key Cryptography depends upon the existence called mathematical function or one way functions'. Garg and Yadav [9] has stated that the Public Key Cryptography allows to exchange messages safely that the user who has no pre-existing security arrangement. Here the private key never be shared or transmitted, all the communications are through the public keys. Asymmetric encryption is the technological revolution that provides the strong cryptography.

The asymmetric key algorithms used for electronic commerce security enhancement are RSA algorithm, digital signature, Diffie Hellman, ElGamal and Elliptical curve cryptography algorithm. According to Kaur et al. [10] in asymmetric key encryption RSA is the vastly used algorithm. The plain and cipher text are numbers between $n-1$ and 0 in a block cipher for certain n is known as RSA algorithm. A typical size of n is 309 decimal digits or 1024 bits. The block size must be similar or less than log2(n). The value must be known by the sender and the d value must be known by the receiver. The RSA is used by receiver with their secret or private key to decrypt the message and for recovery of session key [11]. Kumar and Vincent [12] have stated that Diffie Hellman is one of the first public key processes and is a way of exchanging the keys of cryptography securely. In Diffie Hellman algorithm the receiver and sender make a similar secret key and they initiate communicating with each other over public channel which is known to all. The Diffie Hellman algorithm is based on the fact that it is simple to estimate the integer powers in a finite field and it is difficult to evaluate the discrete logarithms [13]. Shi et al. [14] has mentioned that the schemes of digital signature allows a signer who has set up a public key to sign a message such that other party can assure that the originated message from signer was not changed in any way. Similarly Kamalakannan and Tamilselvan [15] has stated that Elgamal cryptosystem is used on the criticality of the discrete logarithm issue for limited fields and the system is easy for sender and receiver in operations of cryptography. Elliptic curve cryptograph offers powerful security and effective performance than other asymmetric key encryption algorithms [16]. Thus, security in transaction is essential in electronic commerce and security over internet is an essential problem which must be taken care seriously. This study describes the security in electronic commerce through asymmetric key algorithm.

## 2. Literature review

Kuppuswamy and Al-Khalidi [17] proposed a study on securing the business of electronic commerce using Hybrid combination based on RSA algorithm and new symmetric key. In security, electronic commerce is becoming much interesting as the transformation from transactions and traditional shopping pass away from traditional to online stores. Electronic commerce has made a huge influence on worldwide economy and has enhanced over years quickly into trillions of dollars every year. Securing payment with application of web users' and the systems of application needs an integration of physical, technical and managerial controls. A hybrid cryptosystem is suggested in this study that integrates both the RSA algorithm and symmetric key algorithm. The effectiveness of security methods are distinguished and such capability rises as security methods are integrated with each other.

Shetty, ShravyaShetty and Krithika [18] stated in their research that cryptography is employed to make secure and safe exchange of data over networks. For cryptography the chosen algorithm must meet the situations of confidentiality, non-repudiation, integrity and authentication. The deterrence of data from illegal contact is the major factor in the field of cryptography. There are several cases where a safe file transmission is needed for example in banking transactions, electronic shopping etc. The asymmetric key cryptography namely ElGamal and RSA algorithm, also known as public key cryptography. In this study two asymmetric algorithms namely El gamal and RSA algorithm are reviewed.

According to the study of Arora and Pooja [19] cryptography is produced to create secure transmission of data over networks. For cryptography the algorithm chosen must fulfill the conditions of confidentiality, non-repudiation, integrity and authentication. This study designs an algorithm to combine both ElGamal and RSA algorithm to offer users with a greater data security level. The enhanced RSA algorithm enables rapid decryption and encryption process and producing private and public key rapidly than original RSA algorithm. The enhanced cryptosystem of RSA is used on integer factorization problem

(IFP) while the ElGamal cryptosystem is used on Discrete Logarithm Problem (DLP). This model performs based on integrating the problem of Discrete Logarithm and Integer Factorization.

In the research of Kallam [20] key exchange is a strategy in cryptography by which cryptographic keys are exchanged between 2 gatherings and those keys are used as a part of certain cryptographic algorithms like Advanced Encryption Standard. Using those keys, the recipient and sender exchange encrypted messages public key cryptography provides a secured strategy to exchange secret keys. The major exchange problem is the means by which gatherings exchange the data or keys in a channel of communication so that nobody else other than recipient or sender can acquire those. This study presents Diffie Hellman key exchange a process which is one of the first PKC (public key cryptographic) protocols employed to construct a private or secret key between two gatherings over a frail channel. Diffie Hellman is proper for usage in communication of information however it is used less frequently for storage of information or archived over a long period of time.

According to the study of Nwoye [21] electronic commerce has provided a new way of performing transactions all over the globe using website. This success of electronic commerce relies highly on how its IT is used. Every firm needs to assure that its electronic commerce data is secured. There is a requirement for electronic commerce information transmitted through internet and computer networks to be secured. Amongst users are hackers that undertaken identity theft and credit card fraud in several ways facilitated by bad online security. Electronic commerce is slowly resolving security problems on their internal networks but protection of security for customers is still in its development stage thus posing a challenge to the growth of electronic commerce. The technology solution suggested for solving this issue of security is the RSA cryptosystem. This study focuses of securing electronic commerce data sent through internet and computer network using RSA cryptography.

Jain and Kapoor [22] proposed secure communication using RSA algorithm for network environment. In network environment secure communication is an essential need to access remote sources in an efficient and controlled way. For authentication and validation in electronic commerce and electronic banking transactions, digital signature using public key cryptography is used extensively. To manage confidentiality Digital Envelope which is the integration of signature and message which is encrypted is used with symmetric key encryption. This study has developed a hybrid approach using asymmetric and symmetric key cryptography. It also involves message authentication code to manage message integrity. Therefore the proposed method will not only support to manage authentication and confidentiality of user and message but data integrity too.

In the research of Jaju and Chowhan [23] digital signature has been offering security services to secure electronic transaction. RSA algorithm was employed vastly to provide methods of security for several applications namely transfer of electronic funds, electronic mails exchange of electronic data, distribution of software, storage of data, e-commerce and secure access of internet. In order to involve cryptosystem of RSA proficiently in several protocols it is wished to plan rapid decryption and encryption operations. This study explains a systematic examination of RSA and its different digital signature schemes.

In the research of Fernando et al. [24] e-commerce is a huge benefit which helps them to develop on operations of supply chain, step into new markets, developed service of customers, simple operations with customers as well as suppliers. As a business when they enter into electronic commerce they required to secure their online transactions securely with trusting problems and privacy safeness that exists with different kinds of intruders. This study will be discussing about the significance of electronic commerce security, various kinds of protocols, public key infrastructure, certificate based cryptography and digital signature using biometric cryptography and using techniques that are in cryptography and that assists with the security of electronic commerce. This research has been designed for securing transactions of electronic commerce using the algorithm of PKE (public key encryption) based on discrete logarithms in finite groups or integer factorization.

According to the study of Ahmad and Alam [25] electronic commerce is regarded as an outstanding alternative, reduced transaction costs and much accessible approach of business to all over the global customers. Several asymmetric methods which employ secure electronic transactions of electronic commerce and other algorithms of cryptography are the major attractions in the setup of e-commerce. In this study a framework of electronic transaction based on PGP (Pretty Good Privacy) and Elliptical curve cryptography is proposed. It will describe how much secured consumer and payment data order will be managed effectively by pretty good privacy based on dual digital signature.

Rane [26] proposed a study on services provided by digital signatures in electronic commerce. The digital signature is generated for the aim of transmitting the actual information without any alterations. The service of digital signature may perform as application of web server on users or client system. The client can pass documents to server as well as acquire back relevant document or vice versa. The core specifications of digital signature assure the basic elements and protocols which are adopted to base the particular use cases in the profiles of digital signature services. The study is carried out in the field of electronic commerce and particularly digital signature has been used in electronic commerce field. Some authors have already initiated researching on digital signature to assure message integrity as it supports in assuring whether actual messages is transmitted or not the factor of integrity supports in assuring the message accuracy that is exchanged between two parties through unsecured modes.

In the study of Shaikh et al. [27] the customer percentage using e-commerce is developing rapidly and the transaction security of electronic commerce is a major concern for electronic commerce sites along with their customers. The basic needs for any electronic commerce transaction are authentication, privacy, non-repudiation and integrity. To satisfy the electronic commerce security needs RSA cryptography algorithm is used widely. Due to the limitations of RSA algorithm a new public key cryptographic scheme referred as elliptic curve cryptography is developing a better choice for RSA. In this study ECC (elliptic curve cryptography) performance system is investigated in terms of computation time taken by elliptic curve when employed for elliptic curve cryptography application. This study describes by comparing how elliptic curve cryptography is good than traditional RSA.

According to the study of Halim et al. [28] security of classified or sensitive information from unauthorized access, other personals and hackers is virtue. Data storage is performed in devices such as external hard disk, USB, I-pad, laptops or at cloud. Cloud computing presents with both pros and cons. However storing data raises the hazards of being attacked by hackers. Besides the hazard of being stolen or losing device is raising in storage case in portable devices. There are array of communication medium and electronic mails used to send information or data but these techniques exist along with serious drawbacks such as confidentiality absence where message sent can be changed and sent to recipient. An e-mail authentication is proposed in this study namely hybrid encryption system. The hybrid encryption standard is secured using asymmetric and symmetric key algorithm. The asymmetric algorithms are RSA and symmetric algorithm is Advance Encryption Standard.

Liu et al. [29] has mentioned that online communication technique in real time has become essential in modern business applications. It permits users to connect simply with business partners over internet through the lens of camera on digital tools. In spite of the fact that users can confirm and recognize the identity of person in front of camera; they cannot assure the message authenticity between the partners of communication. To secure confidential messages it is important to set up a secure channel of communication between users. This study

suggests a RSA cryptosystem biometric to protect real time interaction in business. This study generates a CPK (cryptographic public key) based on biometric user information without using PKI (public key infrastructure) and set up a secured public network channel.

Matte et al. [30] has mentioned that in nowadays world the need for securing electronic commerce is on a huge demand. It involves privacy of electronic commerce transaction, authentication, maintenance of its non-repudiation and integrity. These are essential problems in nowadays time for trade which is taken over internet through the means known as electronic commerce. This study discusses about different techniques known as cipher approach that develops the key exchange of Diffie Hellman using truncated polynomial to issue of discrete logarithm that develops the electronic commerce transaction security which rules over internet. It also comprises algorithms namely AES and MD5 where MD5 is an asymmetric key algorithm and AES is a symmetric key algorithm.

Table 1 shows the reviews of e-commerce security using asymmetric key algorithm:

## 3. Design of the system

This part describes the design of an e-commerce security using asymmetric key algorithm. Security plays an essential part in e-commerce web services because security is the major problem faced by all users nowadays. This study proposes an algorithm and implements an approach for the encryption and decryption of message. The traditional methods implement a single layer of encryption to the messages which is sent through the network. The approach used in this study is the multi-layer encryption algorithm which makes the delivery of messages through network in a secure way. The below Fig. 2 shows the proposed system flow diagram:

From the above flow diagram, the proposed system uses two types of encryption in two different layers. The first layer of encryption is applied using RSA encryption algorithm and the second layer of encryption is applied using Fernet cipher encryption algorithm. The message is passed initially and gets encrypted by RSA algorithm and then the Fernet cipher algorithm is applied which is based on AES encryption algorithm. From the RSA output the message is generated and the last message is provided by network through receiver. This encrypted message once received by the receiver is then passed through the inverse Fernet cipher algorithm which is then decrypted to the first layer and then the decrypted message is passed to the RSA algorithm which decrypts it to the original message. The RSA Encryption algorithm enables secret information transmission over an open channel without a relevant secret key shared between them. This algorithm is used for one way functions of encryption trapdoor that can be carried out in small amount of time while their inverse function execution occurs at infinite time.

### 3.1. Fernet cipher algorithm

Fernet cipher is a symmetric method of encryption which assures that the encrypted message cannot be read or manipulated without the key. It employs uniform resource locator secure key encoding. Fernet uses 128 bit Advanced Encryption Standard in mode of CBC and padding of PKCS7 with Hash based MAC (message Authentication Code) using SHA (Secure Hash Algorithm) 256 for authentication. The two parts used for the Fernet Cipher algorithm is the encryption and decryption of messages. The two parts are explained below in detail:

#### 3.1.1. Encryption

At the initiation of cipher using conventions the input is copied to state array. After an initial addition of round key, the state array is altered by using the function of round i.e. 10, 12 and 14 times with the last round varying slowly from the first rounds of Nr−1. Then the last state is copied to output. The round function is parameterized using

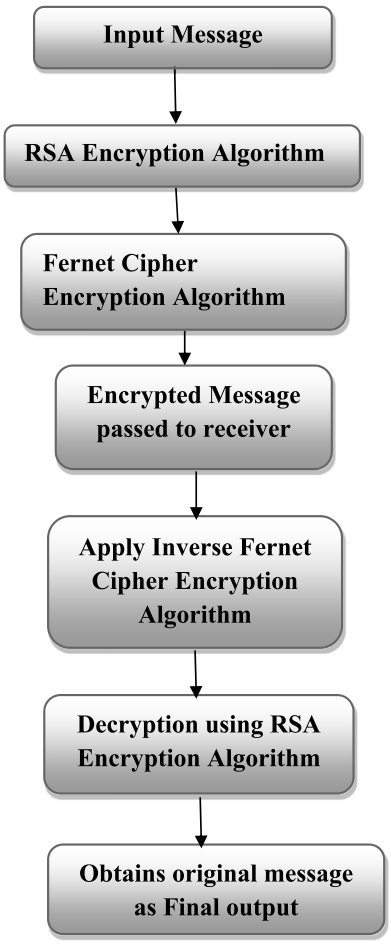


**Fig. 2.** Proposed flow diagram.
*Source:* Author

a major plan that comprises of a 1-dimensional array of 4-byte words derived using the key expansion routine. In the pseudo code the cipher is explained. The algorithm for the encryption is given below with pseudo code for cipher:

From the above Fig. 3 where ARK stands for AddRoundKey, SBT stands for SubBytes,

*3.1.1.1. Transformation of SubBytes().* In the transformation of SubBytes() the following affine transformation is applied (over GF (2)):

$$x_n = x_n \oplus x_{(n+4)mod8} \oplus x_{(n+5)mod8} \oplus x_{(n+6)mod8} \oplus x_{(n+7)mod8} \oplus y_n$$

For $0 <= n < 8$, where $x_n$ is the $n$th byte bit and $y_n$ is the $n$th byte bit of y byte with the value {0 1 1 0 0 0 1 1} or {3 6}. Elsewhere a prime on a variable represents that the variable is updated with the right side value.

*3.1.1.2. Transformation of RowsShift().* The equation of the transformation of RowsShift() is mentioned as follows:

$$z'_{C,R} = z_{R,(C+shift(R,nB))mod\ nB} \quad \text{for } 0 \le C < nB, \text{ for } 0 < R < 4$$

*3.1.1.3. Transformation of AddRoundKey().* In the transformation of AddRoundKey()an easy XOR bitwise operation is added to a round key to state. Every round key comprises of $nB$ words from the key schedule and those $nB$ words are added into the columns state each such that

$$[z'_{0,C}, z'_{1,C}, z'_{2,C}, z'_{3,C}] = [z_{0,C}, z_{1,C}, z_{2,C}, z_{3,C}] \oplus [W_{Round+nB+C}]$$
$$\text{for } 0 \le C < nB,$$

In this research the Add Round key is used to encipher block data using several numbers of rounds

**Table 1**
Reviews of e-commerce security using asymmetric key algorithm.

| S. No | Author | Year | Algorithm used | Findings of the study |
|---|---|---|---|---|
| **1** | Kuppuswamy and Al-Khalidi | 2014 | Symmetric key and RSA algorithm | Enhance the security of other network |
| **2** | Shetty, Shravya Shetty and Krithika | 2014 | RSA and El-Gamal Algorithm | Transmit files securely |
| **3** | Arora and pooja | 2015 | RSA and El Gamal Algorithm | Used over public networks for data transfer using various keys used for decryption and encryption |
| **4** | Kallam | 2015 | Diffie Hellman Key Exchange | Builds a mutual secret key between two gatherings and employed for secret interaction for transforming data over public channel |
| **5** | Nwoye | 2015 | RSA algorithm | Secures electronic commerce data sent through internet and computer using RSA cryptography |
| **6** | Jain and Kapoor | 2015 | RSA Algorithm | Develops a security process comprising of integrity, confidentiality and authentication on single platform |
| **7** | Jaju and Chowhan | 2015 | RSA algorithm | Faster decryption and encryption processes |
| 8 | Fernando et al. | 2016 | Public Key Encryption algorithm | Increase the performance of electronic commerce security |
| 9 | Ahmad and Alam | 2016 | Elliptical curve cryptography | Most secure and less time engrossing and also controls entire decryption and encryption with the support of private and public key of receiver and sender. |
| 10 | Rane | 2016 | Digital Signatures | Used for distribution of software along with transactions of electronic commerce and it is much secure to detect forgery |
| 11 | Shaikh et al. | 2017 | RSA and Elliptic curve cryptography | Helps to develop the online business rapidly. |
| 12 | Halim et al. | 2017 | RSA and AES | Help users to secure their valuable data documentation from illegitimate third party user |
| 13 | Liu et al. | 2018 | RSA algorithm | Secure the communication content |
| 14 | Matte et al. | 2018 | MD5 and AES | Communication security is exchange information in a time period |

```
C (input for byte [4 * nB], output byte [4 * nB], word W[nB * (nR + 1)])
Initiate
        State of byte [4, nB]
        State = in
         ARK(W[0, nB − 1], state)
         For first round first step to nR-1
                SBT (state)
                RowsShift (state)
ColumnsMix (state)
                ARK (W [round ∗ nB, (round + 1) ∗ nB− 1], state)
          End for
          SBT (state)
          RowsShift (state)
          ARK (W[nR ∗ nB, (nR + 1) ∗ nB − 1], state)
3
7       Output = state
end
```

**Fig. 3.** Cipher pseudo code.

*3.1.1.4. Transformation of MixColumns().* The transformation of MixColumns() performs on column by column state handling every column as a 4 term polynomial. As polynomials the columns are regarded over GF (28) and multiplied with $p4+1$ modulo with $f(p)$ fixed polynomial presented by the equation:

$$f(p) = \{03\}\, p^3 + \{01\}\, p^2 + \{01\}\, p + \{02\}$$

The above equation can be written as a multiplication of matrix. Let us assume that

$$z'(p) = f(p) \otimes z(p) :$$

*3.1.2. Decryption*

The transformations of cipher can be decrypted and then used in opposite order to generate a direct decrypted cipher for Fernet cipher algorithm. The separate transformations used in decrypted cipher are InvSubBytes(), InvShiftRows(), InvAddRoundKey() and InvMixColumns() state process are explained. The decryption algorithm with the pseudo code is presented in Fig. 4.

*3.1.2.1. Transformation of invrowsshift().* The transformation of InvRowsShift() initiates as follows:

$$z'_{R,(C+shift(R,nB))modnB} = z_{R,C} \quad \text{for } 0 \le C < nB \text{ and for } 0 < R < 4$$

*3.1.2.2. Transformation of InvSubBytes().* The transformation of InvSubBytes() is the transformation of inverse substitution of byte in which the inverse box of S is used at every state byte. This is acquired using the affine transformation inversely() followed by acquiring the GF multiplicative inverse (28). In the transformation the inverse S box of InvSubBytes is presented in the below Fig. 5.

*3.1.2.3. Transformation of InvMixColumns().* The transformation of InvMixColumns() is the transformation of MixColumns() inverse. InvMixColumns() performs on column by column state handling every column as a four term polynomial. These columns are regarded as polynomials over GF (28) and $p4 + 1$ modulo with $f^{-1}(p)$ fixed polynomial is presented by the equation:

$$f^{-1}(p) = \{0b\}\, p^3 + \{0d\}\, p^2 + \{09\}\, p + \{0e\}$$

The above equation can be written as a multiplication of matrix. Consider

$$z'(p) = f^{-1}(p) \otimes z(p) :$$

*3.1.2.4. Transformation of InvAddRoundKey().* The AddRoundKey() is its own inverse since it includes only the application of XOR operation.

*3.2. RSA algorithm*

The first familiar algorithm referred for encryption as well as signing is the RSA and it is regarded as one of the biggest growths in PKC (public key cryptography). RSA is employed in 100 s of products of software and can be employed for digital signatures, key exchanges or little blocks of data encryption. RSA employs a key of variable size key

```
InvCipher (input for byte [4 * nB], output byte [4 * nB], word W[nB * (nR + 1)])
Initiate
        State of byte [4, nB]
        State = in
         ARK (W[nR + nB, (nR + 1) ∗ nB − 1])state)
         For nR–first round first step downto 1
                  InvSubBytes (state)
InvRowsShift (state)
InvColumnsMix (state)
                  AddRoundKey (W [round ∗ nB, (round + 1) ∗ nB– 1], state)
   3.           End for
          InvSubBytes (state)
InvRowsShift (state)
          AddRoundKey (W[0, nB − 1], state)
           Output = state
end
```

**Fig. 4.** Pseudo code for Decrypted cipher.

| x \ y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
| 1 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
| 2 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
| 3 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
| 4 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
| 5 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
| 6 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
| 7 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
| 8 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
| 9 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
| a | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
| b | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
| c | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
| d | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
| e | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
| f | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

**Fig. 5.** Inverse box of S used in InvSubBytes Transformation().

and a variable size block of encryption. The set of keys is derived from huge number n i.e. the two prime numbers product selected according to special norms and these prime numbers may be 100 or greater than 100 in length generating n with twice as several digits as major factors. The steps used for the RSA Algorithm are:

**Step 1:** The 2 prime numbers namely a and b are chosen
**Step 2:** The N is calculated N = a, b
**Step 3:** Phi = (a−1) (b−1)
**Step 4:** Chose E randomly
**Step 5:** Evaluate the D value such that ED = 1 (mod phi)
**Step 6:** Public Key = (N, E) Private Key = (N, D)

*3.2.1. Encryption*

For certain cipher text C and plaintext M

C = M ^ e mod N

*3.2.2. Decryption*

M = C ^ D mod N = (M ^ e) ^ D mod N = M ^ ED mod N

The code is executed using Python Language. Python is a greater level programming language which assists to construct big scale applications namely electronic commerce. Python will permit developers to denote their notions rapidly. Within small number of codes, the developers can bring their notions easily so that the developers will have the right to imagine much. With the assistance of extensive library, the user can evolve a huge website in little number of days and it performs on different systems. Python is highly effective with enhanced readability and as an outcome several developers tend to choose this language. Python is the perfect match for construction an electronic commerce site.

```
##################################################################################################
What is the message to be encrypted(-1 to exit)?642

 Beginning Encryption
----------------------
642  --> Encryption Layer 1 : 22818  --> Encryption Layer 2 : b'gAAAAABc0-z9ta5_pQhZZYBkkPscUEEV9yVJku35cEcZHw5mz9Pnre2ycAOfGTnQywy0GxY69wckhxh
yQipQqAmiSf-mWbHQUg=='

Encrypted Message is : gAAAAABc0-z9ta5_pQhZZYBkkPscUEEV9yVJku35cEcZHw5mz9Pnre2ycAOfGTnQywy0GxY69wckhxhyQipQqAmiSf-mWbHQUg==

 Beginning Decryption
----------------------
b'gAAAAABc0-z9ta5_pQhZZYBkkPscUEEV9yVJku35cEcZHw5mz9Pnre2ycAOfGTnQywy0GxY69wckhxhyQipQqAmiSf-mWbHQUg==' --> Decryption Layer 1 : b'22818' -->
 Decryption Layer 2 : 642

Decrypted Message is : 642

##################################################################################################

What is the message to be encrypted(-1 to exit)?3314

 Beginning Encryption
----------------------
3314  --> Encryption Layer 1 : 31925  --> Encryption Layer 2 : b'gAAAAABc0-0JT5fFC2busmk3CZjU0lS-P6gs3wORSVtluyVuf0ZJFOK7i3AtEw3BiPdPRWwebqfbHn
6R_XqPugqaGhsi9EmI3Q=='

Encrypted Message is : gAAAAABc0-0JT5fFC2busmk3CZjU0lS-P6gs3wORSVtluyVuf0ZJFOK7i3AtEw3BiPdPRWwebqfbHn6R_XqPugqaGhsi9EmI3Q==

 Beginning Decryption
----------------------
b'gAAAAABc0-0JT5fFC2busmk3CZjU0lS-P6gs3wORSVtluyVuf0ZJFOK7i3AtEw3BiPdPRWwebqfbHn6R_XqPugqaGhsi9EmI3Q==' --> Decryption Layer 1 : b'31925' -->
 Decryption Layer 2 : 3314

Decrypted Message is : 3314

##################################################################################################
```

**Fig. 6.** Input text.

```
##################################################################################################

What is the message to be encrypted(-1 to exit)?921

 Beginning Encryption
----------------------
921  --> Encryption Layer 1 : 16670  --> Encryption Layer 2 : b'gAAAAABc0-13J_HG-fHj8b9oKaj-2lsSTRJgfXGA0GUGZG_82dOYBahwwQiOk454IrvFttN3RWkKPPo
bvT95LnWcxUB1nHVyww=='

Encrypted Message is : gAAAAABc0-13J_HG-fHj8b9oKaj-2lsSTRJgfXGA0GUGZG_82dOYBahwwQiOk454IrvFttN3RWkKPPobvT95LnWcxUB1nHVyww==

 Beginning Decryption
----------------------
b'gAAAAABc0-13J_HG-fHj8b9oKaj-2lsSTRJgfXGA0GUGZG_82dOYBahwwQiOk454IrvFttN3RWkKPPobvT95LnWcxUB1nHVyww==' --> Decryption Layer 1 : b'16670' -->
 Decryption Layer 2 : 921

Decrypted Message is : 921

##################################################################################################

What is the message to be encrypted(-1 to exit)?0021

 Beginning Encryption
----------------------
21  --> Encryption Layer 1 : 9261  --> Encryption Layer 2 : b'gAAAAABc0-15FxpkTUwDq09cB8RnWhAIRB5h8ARkWgsMkNeowWo4vvas8CmIgWj1HI_LYUvSs-Z8abGB7
fc-XbbEbGC3R7grlw=='

Encrypted Message is : gAAAAABc0-15FxpkTUwDq09cB8RnWhAIRB5h8ARkWgsMkNeowWo4vvas8CmIgWj1HI_LYUvSs-Z8abGB7fc-XbbEbGC3R7grlw==

 Beginning Decryption
----------------------
b'gAAAAABc0-15FxpkTUwDq09cB8RnWhAIRB5h8ARkWgsMkNeowWo4vvas8CmIgWj1HI_LYUvSs-Z8abGB7fc-XbbEbGC3R7grlw==' --> Decryption Layer 1 : b'9261' -->
Decryption Layer 2 : 21

Decrypted Message is : 21

##################################################################################################
```

**Fig. 7.** Encryption.

## 4. Discussion and results

In electronic commerce the transaction security is very important. Hesitation in security of transaction over internet is an essential problem which must be taken care seriously. Users are happy with the web development where they can search internet and predict data which they require easily. However, when it comes to determine to purchase a service or product over internet several users worry about the security in transaction. Similarly, organizations also concern about the frauds taking place in online nowadays. So, the main purpose of this study is to design an electronic commerce security using asymmetric key algorithm. Encryption technique is the major technique to make online transaction secure. Similarly, fraud will occur even though the encryption technique in electronic commerce is better enough to secure the transactions of electronic commerce. This study uses multi-layer encryption algorithm namely RSA encryption algorithm and Fernet cipher encryption algorithm. Fernet cipher encryption is much stronger than RSA algorithm when there is no requirement for communication

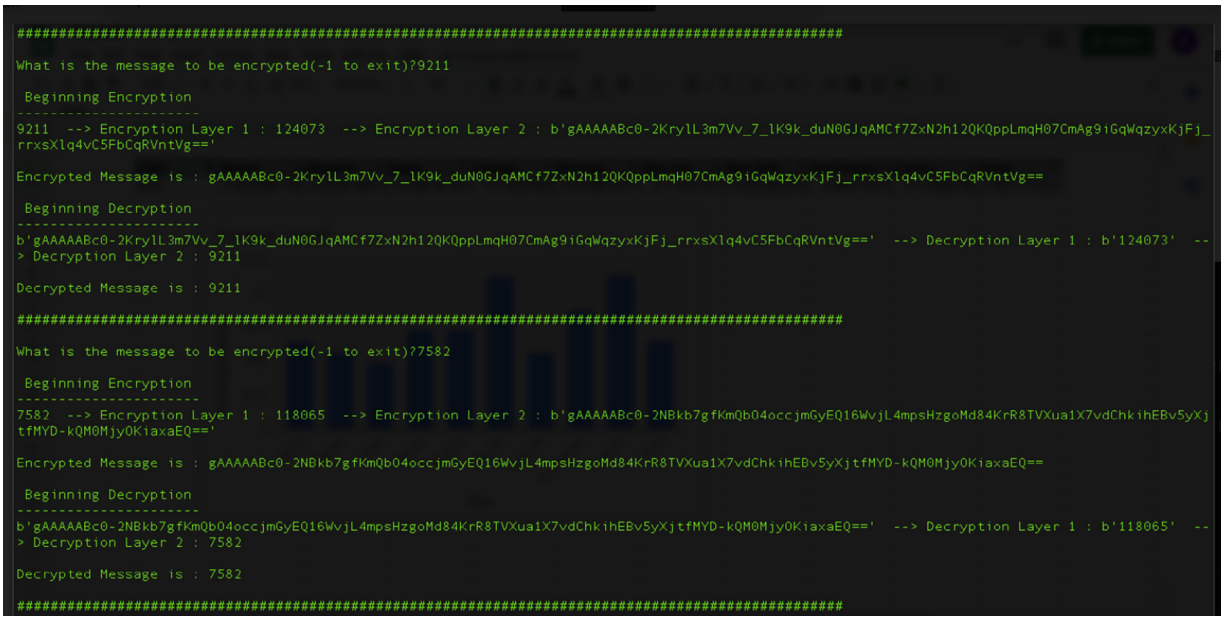


**Fig. 8.** Encryption and decryption — Sample 1.


**Fig. 9.** Encryption and decryption — Sample 2.

but RSA is also a strong tool to pass the data over wire. Thus, when these two powerful algorithms are used together provides a good result to secure electronic commerce. The RSA encryption algorithm enhances secret information transmission over an open channel without a similar secret key shared between them. This algorithm is used for one-way function encryption that can be implemented in a short span of time while their inverse function execution occurs at infinite time. RSA algorithm can be used as a block cipher because of its huge computation overhead and it is also used for authentication of server and for switching a session key secretly. A generated session key with the use of encryption based on RSA which can be employed for content encryption using SKC (symmetric key cryptography). Fernet assures that an encrypted message using it cannot be read or manipulated without the key. Fernet is a symmetric authenticated cryptography implementation. Fernet has support for implementing key rotation through multi Fernet. The Fernet cipher encryption algorithm offers both decryption and encryption facilities. Fernet is ideal for data encryption that fits in memory easily.

*The output results obtained from the proposed approach is given below:*

Step 1: The encryption algorithm is applied in the input text (see Figs. 6–9)

Step 2: Decryption is also undertaken in the input text (see Figs. 10 and 11)

Step 3: The final output of the encryption and decryption message is obtained (see Fig. 12)

## 5. Conclusion

Satisfying needs of security is one of the most essential targets for the designers of electronic commerce system security. The main aim of this study is to expand the security of electronic commerce

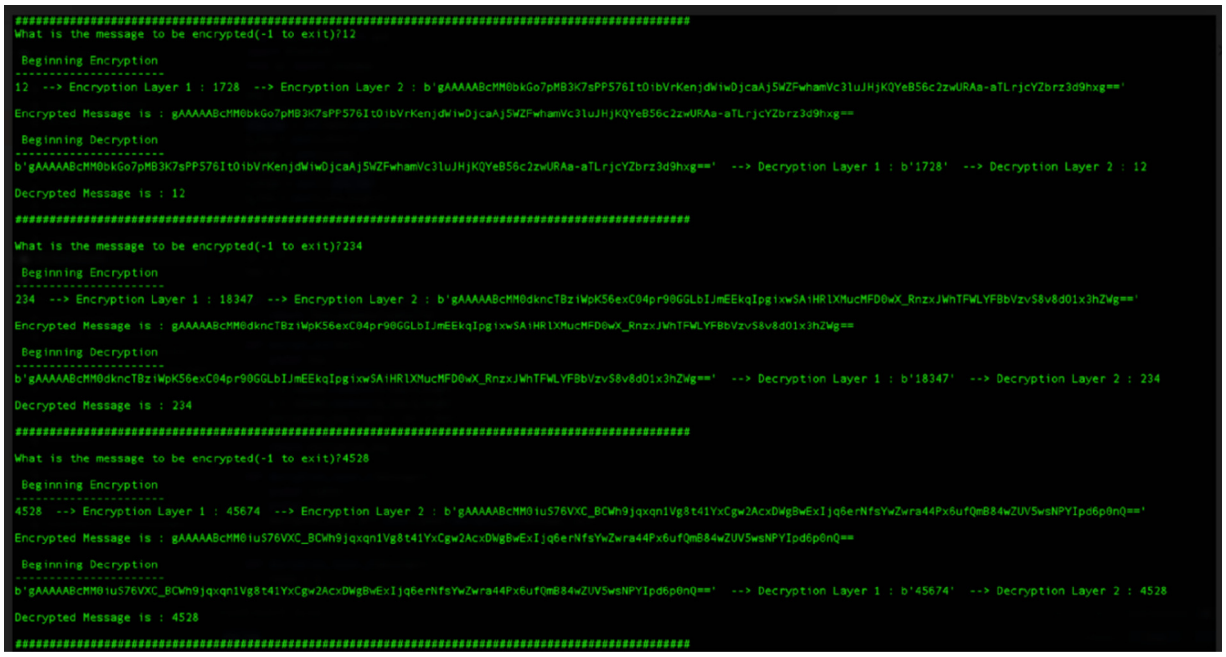


**Fig. 10.** Encryption and decryption — Sample 3.


**Fig. 11.** Encryption and decryption — Sample 4.

through different asymmetric key encryption algorithms. Integrity, privacy, non-repudiation and confidentiality are major dimensions of security to secure transactions of electronic commerce against security threats. Security has developed as an essential problem in the success and growth of an electronic commerce firm. The proposed model in this study focuses on certain factors namely its cost, consumption of time and security factors. It produces several cycles and takes huge amount of time for data processing where the information in verification but this study used algorithms of RSA which is time consuming and much secure. It will handle the complete decryption and encryption process with the help of private and public key of receiver and sender. This study mainly proposes RSA encryption and Fernet cipher algorithm to enhance the security of electronic commerce. In future for secured and resourceful transmission of data cryptography is an essential solution. Different applications can be constructed using asymmetric and symmetric algorithm for developing their security. The greater the security of system the lesser will be the opportunities of breaking into it. The security system future relies on algorithms which makes the intrusion impossible.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

**Ethical approval** This article does not contain any studies with human participants or animals performed by any of the authors.

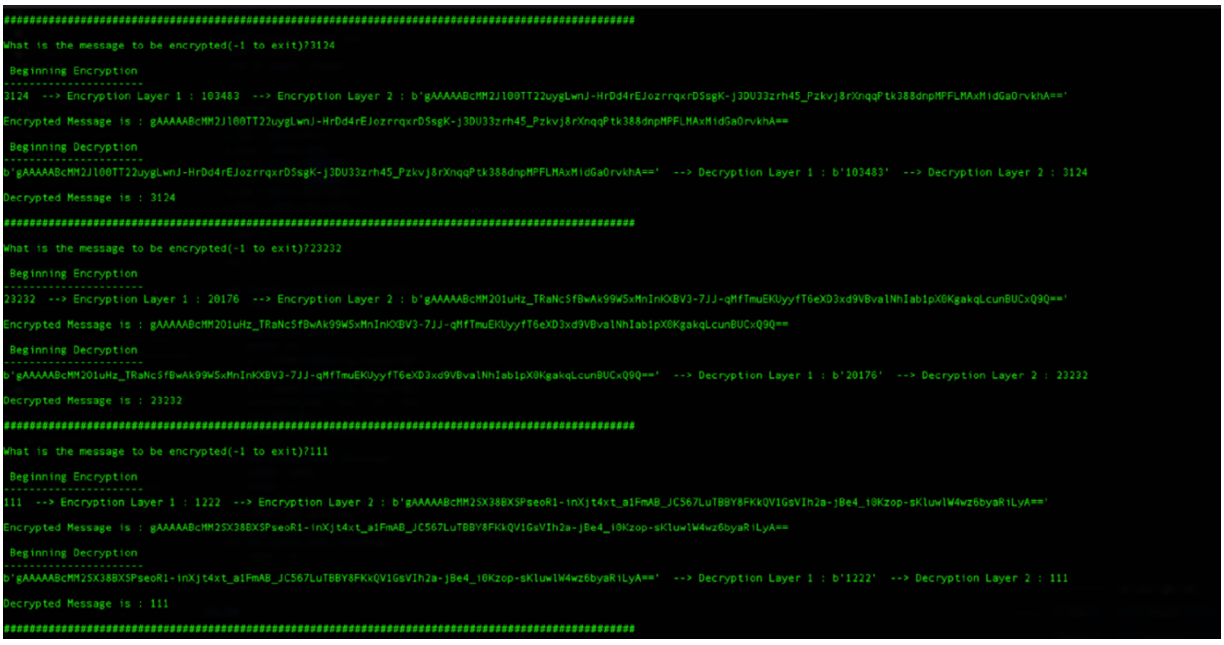


**Fig. 12.** Encryption and Decryption — Sample 5.

## References


[1] A. Chaudhary, K. Ahmad, M.A. Rizvi, E-commerce security through asymmetric key algorithm, in: Communication Systems and Network Technologies, CSNT, 2014 Fourth International Conference on, IEEE, 2014, pp. 776–781.

[2] Ritu, Crytography based E-commerce security, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 6 (7) (2016) 359–362.

[3] M.P. Gupta, A. Dubey, E-commerce-study of privacy, trust and security from consumer's perspective, Transactions 37 (2016) 38.

[4] N.A. Rathi, S.R. Gupta, Analysis of security mechanism in E-commerce transaction, Int. J. Adv. Res. Comput. Eng. Technol. 5 (1) (2016) 131–134.

[5] S.P. Patro, N. Padhy, R. Panigrahi, Security issues over E-commerce and their solutions, Int. J. Adv. Res. Comput. Commun. Eng. 5 (12) (2016) 81–85.

[6] P. Churi, E-commerce security with secure electronic transaction protocol: A survey and implementation, 2017, Available at https://www.researchgate.net/publication/320758708_E-COMMERCE_SECURITY_WITH_SECURE_ELECTRONIC_TRANSACTION_PROTOCOL_A_SURVEY_AND_IMPLEMENTATION. (Accessed on 17th January 2019).

[7] M. Illayaraja, K. Shankar, G. Devika, A modified symmetric key cryptography method for secure data transmission, Int. J. Pure Appl. Math. 116 (10) (2017) 301–306.

[8] S. Suguna, V. Dhanakoti, R. Manjupriya, A study on symmetric and asymmetric key encryption algorithms, Int. Res. J. Eng. Technol. 3 (4) (2016) 27–31.

[9] N. Garg, P. Yadav, Comparison of asymmetric algorithms in cryptography, Int. J. Comput. Sci. Mob. Comput. 3 (4) (2014) 1190–1196.

[10] K. Kaur, A. Pathak, P. Kaur, K. Kaur, E-commerce privacy and security system, Int. J. Eng. Res. Appl. 5 (5) (2015) 63–73.

[11] S. Verma, D. Garg, An improved RSA variant, Int. J. Adv. Technol. 5 (2) (2014) 161–169.

[12] C. Kumar, P.D.R. Vincent, Enhanced Diffie-Hellman algorithm for reliable key exchange, in: IOP Conference Series: Materials Science and Engineering, vol. 263, (4) IOP Publishing, 2017, p. 042015.

[13] A. Kak, Certificates, digital signatures, and the Diffie-Hellman key exchange algorithm, 2018, Available at https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture13.pdf. (Accessed on 18th January 2019).

[14] Y. Shi, J. Lin, G. Xiong, X. Wang, H. Fan, Key-insulated undetachable digital signature scheme and solution for secure mobile agents in electronic commerce, Mob. Inf. Syst. (2016).

[15] V. Kamalakannan, S. Tamilselvan, Security enhancement of text message based on matrix approach using elliptical curve cryptosystem, Procedia Mater. Sci. 10 (2015) 489–496.

[16] I. Setiadi, A.I. Kistijantoro, A. Miyaji, Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems, in: Advanced Informatics: Concepts, Theory and Applications, ICAICTA, 2015 2nd International Conference on, IEEE, 2015, pp. 1–6.

[17] P. Kuppuswamy, S.Q. Al-Khalidi, Securing E-commerce business using hybrid combination based on new symmetric key and RSA algorithm, MIS Rev. Int. J. 20 (1) (2014) 59–71.

[18] A. Shetty, K. Shravya Shetty, K. Krithika, A review on asymmetric cryptography – RSA and El-Gamal algorithm, Int. J. Innov. Res. Comput. Commun. Eng. 2 (5) (2015) 98–105.

[19] S. Arora, Pooja, Enhancing cryptographic security using novel approach based on enhanced-RSA and elamal: Analysis and comparison, Int. J. Comput. Appl. Technol. 112 (13) (2015) 35–38.

[20] S. Kallam, Diffie-Hellman: Key exchange and public key cryptosystems, 2015, Available at http://cs.indstate.edu/~skallam/doc.pdf. (Accessed on 17th January 2019).

[21] C.J. Nwoye, Design and development of an E-commerce security using RSA cryptosystem, Int.J. Innov. Res. Inf. Secur. 6 (2) (2015) 6–17.

[22] A. Jain, V. Kapoor, Secure communication using RSA algorithm for network environment, Int. J. Comput. Appl. 118 (7) (2015).

[23] A.S. Jaju, S.S. Chowhan, Analytical study of modified RSA algorithms for digital signature, Int. J. Recent Innov. Trends Comput. Commun. 3 (3) (2015) 944–949.

[24] A.D.N.M. Fernando, H.M.P.M.B. Herath, M.L.R.K. Senarathne, D.P. Brandiwatta, T. Kiroshan, M.P. Madushika, P.A.D.A. Senarathne, M.D. Dharmmearatchi, Biometric encryption: E-commerce security using cryptography techniques, Int. J. Sci. Res. Publ. 6 (10) (2016).

[25] K. Ahmad, M.S. Alam, E-commerce security through elliptic curve cryptography, Procedia Comput. Sci. 78 (2016) 867–873.

[26] Y.S. Rane, Study on services provided by digital signatures in E-commerce, Int. Res. J. Eng. Technol. 3 (5) (2016) 3039–3041.

[27] J.R. Shaikh, R. Kumar, M. Nenova, G. Iliev, H. Singh, Enhancing E-commerce security using elliptic curve cryptography, Int. J. Curr. Adv. Res. 6 (8) (2017) 5338–5342.

[28] M.A.A. Halim, C.C. Wen, I. Rahmi, N.A. Abdullah, N.H.A. Rahman, Email authentication using symmetric and asymmetric key algorithm encryption, in: AIP Conference Proceedings, vol. 1891, (No. 1) AIP Publishing, 2017, p. 020047.

[29] X. Liu, W.B. Lee, Q.A. Bui, C.C. Lin, H.L. Wu, Biometrics-based RSA cryptosystem for securing real-time communication, 2018, Available at https://www.mdpi.com/2071-1050/10/10/3588/pdf. (Accessed on 17th January 2019).

[30] S. Matte, A. Dubey, N. Shirsat, A. Kale, Hybrid model for securing E-commerce transaction, Int. J. Sci. Eng. Res. 9 (4) (2018) 25–26.