Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019)
IEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4

# A New Approach of Digital Signature Verification based on BioGamal Algorithm

Rashmi Kasodhan
M.Tech Scholar
Department of CSE, TIT, Bhopal
kasodhan.rashmi@gmail.com

Neetesh Gupta
Professor
Department of CSE, TIT, Bhopal
gupta_neetesh81@yahoo.com

**Abstract- In recent times, online services are playing a crucial role in our day-to-day life applications. Inspite of their advantage, it also have certain security challenges in the communication network. Security aspects consists of authentication of users, confidentiality of data/information as well as integrity of data. In order to achieve all these parameters, the sensitive information must be digitally signed by the original sender and later verified by the intended recipient. Therefore, research on digital signatures should be further developed to improve the data security and authenticity of the transferred data. In this paper, a secured digital signature algorithm is designed. The design of secure digital signature uses the concept of hybridization of secure hash code, DNA encryption/decryption technique and elgamal encryption/decryption techniques. The use of SHA algorithm generates a secure hash code and hybridization of encryption algorithm reduces the computational complexity and this research method is then compared with existing PlayGamal algorithm with respect to encryption/decryption time complexity.**

***Keywords- Security, Cryptography, Digital signature, Verification***

## I. INTRODUCTION

In the current scenario, internet is the major need of everyone's day-to-day life. There is need of internet access in everyone's life as well as in every field either in the field of education, business, marketing or entertainment. With increase of these requirements there is more and more possibility of data theft. So, there is need of secure communicating channel in order to prevent data theft or forgery. One of the security issues is interception of data while in transmitting channel. So, to prevent these issues there is need of digital signature in order to ensure that data is coming from authentic user.

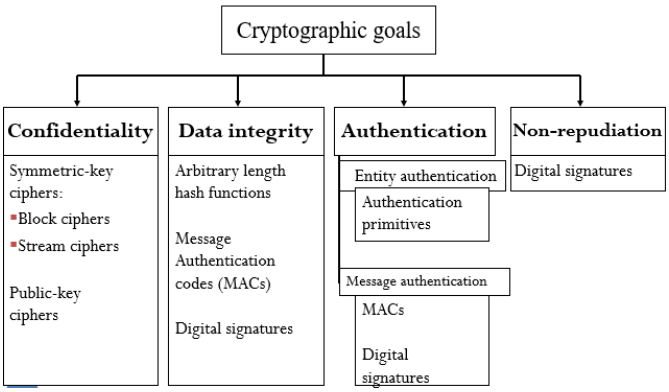


Fig.1. Cryptographic Goals

A digital signature is used for authentication of data as well as user in order to determine whether the correct data is coming from the authenticate sender, then it is necessary to verify it. Digital signature is used for authentication, integrity checking as well as for non-repudiation [5].

One way to avoid non-repudiation condition is to create a unique character that guarantees the authenticity of the data as well as user. Cryptography has been used as a data protection method [3] [4]. To do this, you can use one of the network security technologies called Digital Signature.

In their implementation, digital signatures simultaneously combine two algorithms, namely hashing algorithms and public key algorithms [6]. A Message digest of information is created with hashing algorithm which is used to check the integrity of the data at the cloud server. Whereas the public key encryption technique is used to create encrypted data for transmission over the network [7].

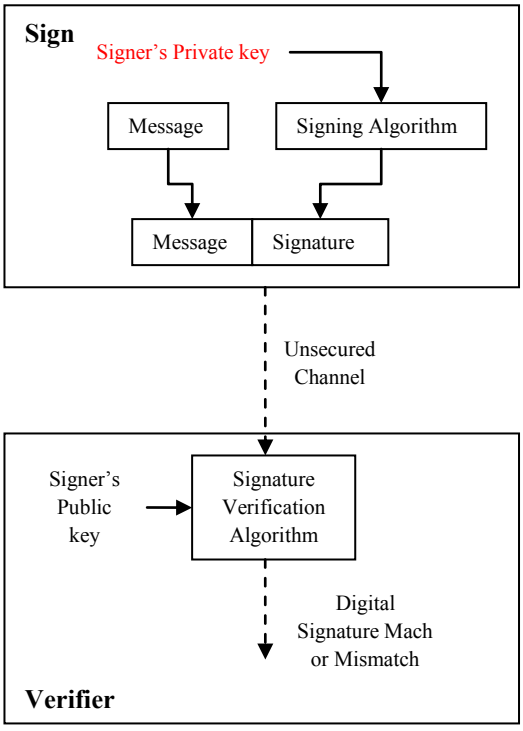


Fig.2. Digital Signature Mechanism

Digital signature is performed in two steps: In the very first step a hash value is generated out of message that is termed as signature and further this hash value is encoded by applying any asymmetric key algorithm and transmit the data to the receiver.

In the send step the receiver receives the message enclosed with hash value and determines whether the signature is authentic or not. If match is found then it represents the credibleness of the sender and therefore the information or message. If signature isn't verified then message received is rejected.

Furthermore, digital signature schemes is classified into the subsequent categories:

*A. Direct Digital Signature*

Direct Digital Signature (DSS) algorithm is directly employed among sender and receiver of the information. Following steps are performed in DSS:

a. Sender send his public key to the receiver.
b. Sender further generates hash/digest by using its own private key and send it to the communicating channel by encrypting it with private key along with message.
c. After receiving these information receiver verifies it by generating hash/digest from the message and matching it with received hash/digest value. If match is found then user is authentic.

In this type of signature, security issue of private key is main area of concern.

*B. Arbitrated Digital signature*

Third party auditor (TPA) is used to verify digital signature of data on behalf of the receiver. The digitally signed message is send to the TPA from sender for further verification. Whenever sender sends data, TPA on behalf of receiver verifies the digital signature of the data and send the verification report to the receiver for intimating that data is authentic and all security checks had been performed.

As keeping the concept and need of the digital signature, i.e. authentication, integrity checking and verification of sender after transmission from the sender side to the receiving side. Whereas integrity checking is performed using other cryptographic algorithms but they may be not feasible with respect to computational cost, time and resources.

Whereas for integrity checking digital signature is generated which is a message digest that represents the authenticity of whole document. This prevents entire document to be processed and encrypted.

Digital signature schemes are vulnerable to many attack types as:

a. Attack in which the attacker only has access to the public key.
b. Attack in which attacker can access signatures of various messages.
c. Attack in which attacker can access signatures of any message of his choice.

In addition to the aforementioned attacks, digitally signed documents are also vulnerable to other attacks such as universal counterfeit attacks, selective counterfeit attacks and existential counterfeit attacks. Although there are several standard digital signature schemes, none of these attacks can handle them efficiently. In fact, the effectiveness of these digital signature schemes depends on the size of the key, the calculation process used, the hash function used, etc. On the road to developing the efficiency and suitability of various electronic mechanisms, digital signature techniques are improved day by day and eventually combined with elliptical curve cryptography techniques to generate ECDSA from DSA, EC-ElGamal at ElGamal.

## II. Related Work

Abdul Ghofar et al. (2017) [1] proposed a digital signature technique by combining features of playfair cipher and elgamal algorithm and termed as playgamal.

Kadek Dwi Budi Utama et al. (2017) [2] designed a digital signature algorithm by combining MAC address with AES-128.First of all SHA-256 is used to generate hash code and further this hash value is encrypted using encryption technique generated by combining features of MAC address and AES algorithm.

Sergei G et al. (2017) [3] designed a digital signature algorithm for Maritime Industry using ECDSA algorithm.

S. Alam et al. (2015) [4] performed digital signature application on image data and further encrypting image digital signature using RSA algorithm.

Gerić et al (2012) [8] designed digital signature for XML transactions. This research work is only intended for XML data and their storage.

Xuan et al (2009) [11] performed comparative analysis of digital signature generated by RSA, ECDSA and DSA algorithm and found that ECDSA outperforms best.

Jian-zhi et al (2009) [12] designed a digital signature approach by using features of DSA algorithm and hyperelliptical curve algorithm which results in high security level and identity of data is verified.

Can et al (2009) [13] research a new cone-shaped digital signature scheme that uses two private keys and enhances the difficulty level to reveal signature keys.

## III. Research Work

In this research work, the secure digital signature is created in three steps as :

- Generation of message digest using hashing algorithm.
- Encryption of generated message digest using BioGamal algorithm and send as digital signature.
- Further decryption of received message is performed using Biogamal algorithm for verification of digital signature.
- If the message digests of received and generated at receiver end is matched, then it indicates that the message is from intended sender.

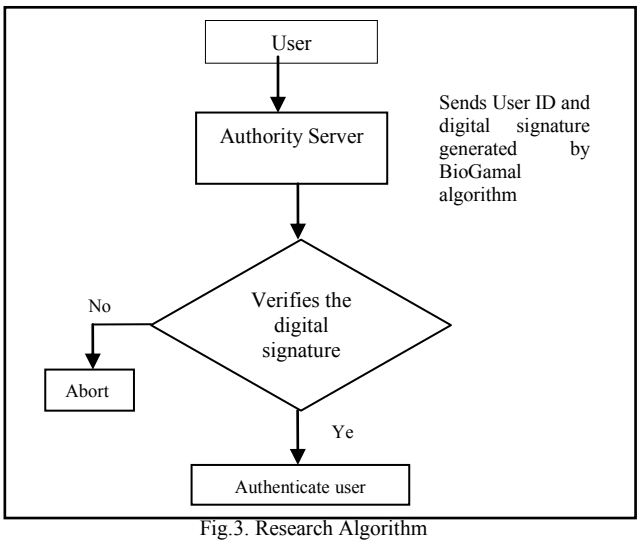


Fig.3. Research Algorithm

*Flowchart of research algorithm*

Flowchart of research algorithm is discussed below in figure 4. In this research work a digital signature algorithm is designed termed as BioGamal which is being performed at sender and receiver end as well.

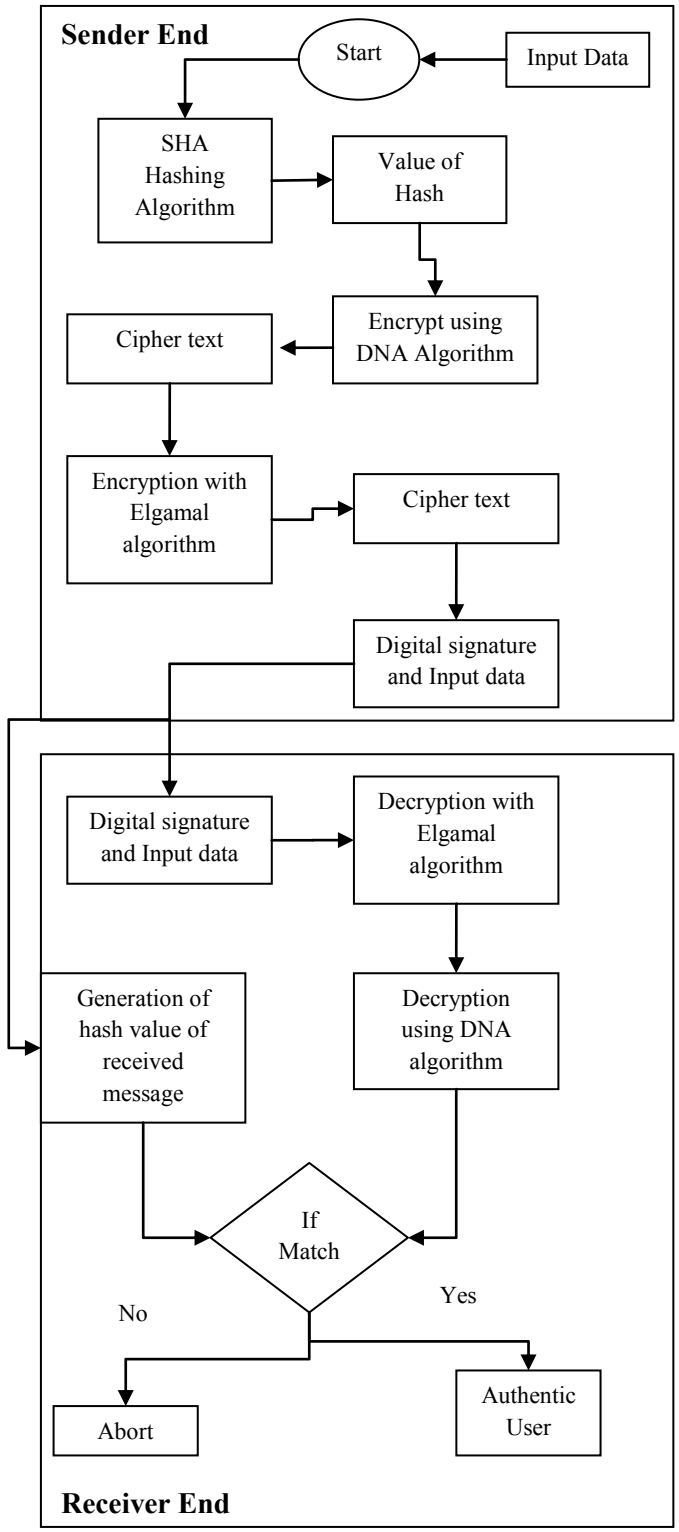


Fig.4. Flowchart of Research Algorithm

In this process a message digest is formed using hashing algorithm i.e. SHA algorithm and further this message digest is encrypted using Biogamal algorithm. The encryption process is done using DNA encryption algorithm and ElGamal encryption. The process of the two algorithms is combined so that a digital signature of the message is sent. As the DNA and ElGamal encryption flow process in Figure 4.

The process of digital signature decryption process is done using decryption algorithm DNA and ElGamal decryption.

### *A. BioGamal Algorithm*

The BioGamal algorithm process is performed by combining two algorithms i.e. DNA encryption/decryption algorithm and Elgamal encryption/decryption algorithm.

#### *1) DNA Algorithm*

DNA Cryptography is used to encrypt the hash value of the data file in first level. In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1.

| Binary Value | DNA Digital Coding |
|---|---|
| 00 | A |
| 01 | T |
| 10 | G |
| 11 | C |

DNA coding is performed as biological sequence of four kind of base as:

ADENINE (A)

THYMINE (T)

CYTOSINE (C)

GUANINE (G).

Every message bit is represented as in the form of 2 bits as mentioned above.

After using these ATGC sequences 15 different keys are formed which is given in table I.

TABLE I DNA KEY COMBINATION

| Key Combination | Pattern | Value |
|---|---|---|
| AA | 0000 | 0 |
| AT | 0001 | 1 |
| AG | 0010 | 2 |
| AC | 0011 | 3 |
| TA | 0100 | 4 |
| TT | 0101 | 5 |
| TG | 0110 | 6 |
| TC | 0111 | 7 |
| GA | 1000 | 8 |
| GT | 1001 | 9 |
| GG | 1010 | 10 |
| GC | 1011 | 11 |
| CA | 1100 | 12 |
| CT | 1101 | 13 |
| CG | 1110 | 14 |
| CC | 1111 | 15 |

To understand the scenario of research DNA cryptography flow chart is illustrated in figure 5.

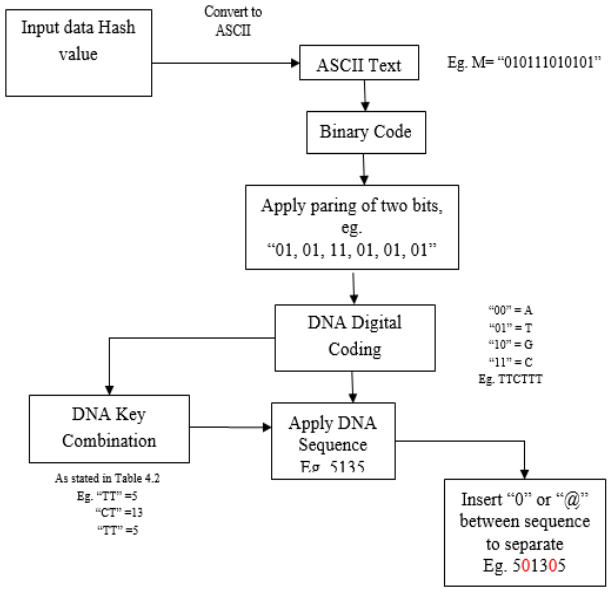


Fig.5. DNA Encryption

*Notations: M= plaintext and C1′ =Encrypted Cipher-text by DNA*

*DNA Encryption Algorithm*

```
Cipher (byte M′, byte C1′)
        State =M′;
        begin {
            convert ASCII code(state);
            convert binarycode(state);
            pairing(state);
            DNA digital coding(state);
            DNA sequencing(state);
            C1′ = DNA sequencing(state);
      end
      }
```

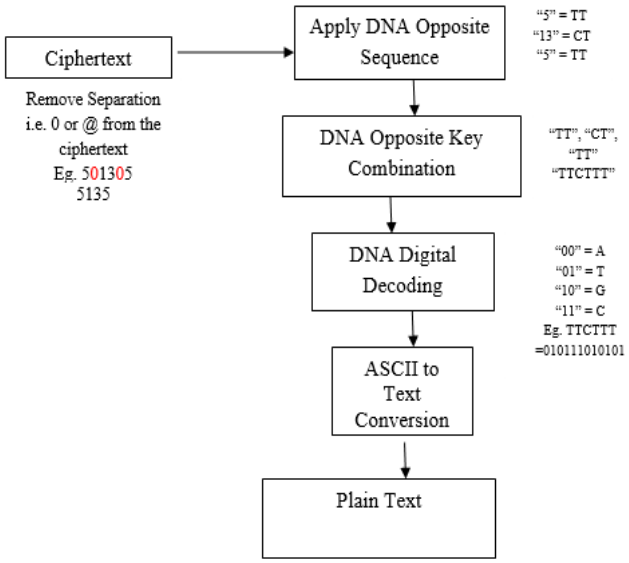


Fig.6. DNA Decryption

*DNA Decryption Algorithm*

```
Decipher (byte C1′, byte M′)
State = C1′;
begin {
DNA_op.sequencing(state);
[//op.sequencing applies for opposite DNA sequence]
DNA_digital.decoding(state);
Convert binarycode(state);
Convert ASCII(state);
M′ = convert byte(state);
end
}
```

*2) Elgamal Algorithm*

ElGamal algorithm is performed in three stages:

i. Key formation
ii. Encryption of message
iii. Decryption of message

It is a type of block cipher which divides the original message into sub blocks for further performing encryption over the data [6]. Encryption algorithm process the original data blocks and convert original data into cipher data blocks which all sub blocks are combined to form one cipher data block which is transmitted to the receiver end.

The elgamal algorithm is performed as follows:

- Generate a prime number p and primitive group **Z**p*
- Generate public and private key. For that generate another primitive element α and free element a Ɛ {0,1,…,p-2}.
- Public key is formed by three pair of numbers as:

$$\beta = \alpha^{\alpha} mod\ p$$

- Where, a is the confidential key which is undisclosed value.

The receiver is involved in the formation of public and confidential key whereas sender is unaware of confidential key. Sender only know about public key of the receiver for encryption of the data.

- Encryption Process El Gamal uses public key and random confidential integer k, (k Ɛ {0,1,…, p-2}).
- Each character in the message is encrypted using a different k number. From an integer number of ASCII that is a representation of one character that will generate code in the form of a block consisting of two values (r,t).
- A message character is choosen in the message and transformed into ASCII code and encrypted as:
  Calculate r value and t values with the equation

$$r = \alpha^{k} (mod\ p)$$
$$t = \beta^{k} M (mod\ p)$$

- Ciphertext is obtained as (r,t).
- This process is repeated for all message blocks in the data.
- *Decryption Process is performed by using* confidential key *a and public keys* (p, α, β). From received ciphertext (r,t), plaintext is performed as :

$$M = t(r^{a})^{-1} mod\ p$$

With M is plaintext with value $r^a$

$$(r^{a})^{-1} = r^{p-1-a} mod\ p$$

## IV. RESULT ANALYSIS

Moreover, we only evaluate the performance execution time between encryption and decryption process of the propose BioGamal compare with Playgamal. Playgamal algorithm [1] is designed for secure digital signature by combining features of two different algorithms i.e. Playfair

cipher and elgamal algorithm. In this existing work time complexity was increased due to features of playfair algorithm as it was designed with 6*6 playfair matrix. So, to reduce time complexity of the playgamal biogamal is designed.

In standalone PC (CPU Core i5, 8GB RAM). The Biogamal algorithm is tested on numeric, alphanumeric and alphabetic characters and compared with playgamal algorithm with respect to encryption time as well as decryption time.
The total time taken to encrypt data files is called encryption time or time taken to decrypt encrypted data files is called decryption time.

$$\text{Encryption Time} = (\text{Stop time of encryption} - \text{Start time of encryption})$$

$$\text{Decryption Time} = (\text{Stop time of decryption} - \text{Start time of decryption})$$

TABLE II ENCRYPTION TIME EVALUATION

| Message | Playgamal [1] Enc_time | Biogamal Enc_time | Difference in % |
|---|---|---|---|
| Numeric Value | 9671490 | 1043711 | 89.20% |
| Alphanumeric Value | 9483318 | 1319259 | 86.08% |
| Alphabetic Value | 20056212 | 2203361 | 89.01% |

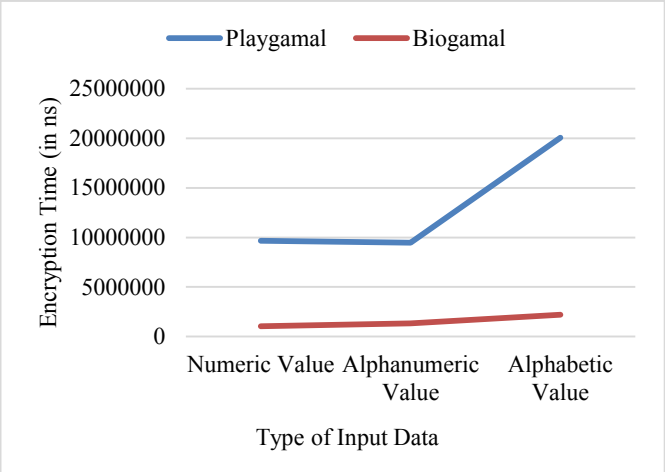


Fig.7. Biogamal Vs Playgamal Encryption Time Evaluation

Table II and figure 7 represents the encryption time calculation of different types of messages. From result it has been analysed that biogamal algorithm gives better performance as compared to Playgamal algorithm. The encryption time of Playgamal is about 89% higher than biogamal.

TABLE III DECRYPTION TIME EVALUATION

| Message | Playgamal [1] Dec_time | Biogamal Dec_time | Difference in % |
|---|---|---|---|
| Numeric Value | 3445705 | 639385.2 | 81.44% |
| Alphanumeric Value | 2237733 | 675378.2 | 69.81% |
| Alphabetic Value | 4491046 | 1347664 | 69.99% |

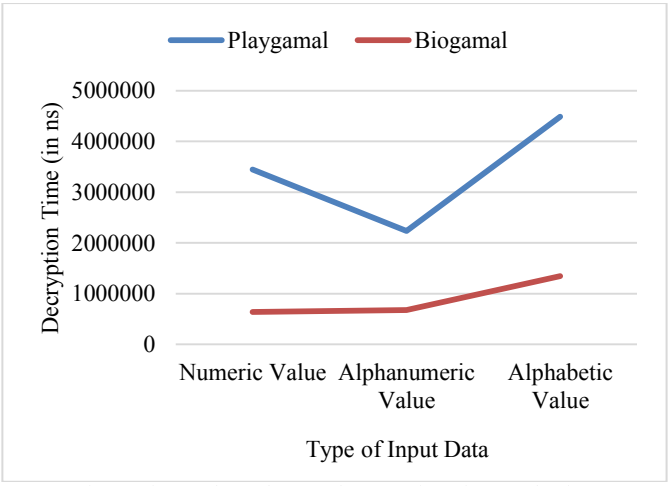


Fig. 8. Biogamal Vs Playgamal Decryption Time Evaluation

Table III and figure 8 represents the decryption time calculation of different types of messages. From result it has been analysed that biogamal algorithm gives better performance as compared to Playgamal algorithm. The decryption time of Playgamal is about 70% higher than biogamal.

## V. CONCLUSION

Digital signatures is used to check integrity of data and user authentication purpose. This research work is focused towards the designing an algorithm for secure digital signature of the data files. For this Biogamal algorithm is designed which is formed by combining features of DNA and ElGamal algorithms. ElGamal is a type of asymmetric algorithm which uses different key pairs for encryption and decryption process whereas DNA algorithm uses the biological sequencing in order to generate ciphertext.

In the encryption, process is done using DNA encryption algorithm and ElGamal encryption. The features of these two algorithm enhances security aspects of the system as well as reduces the time complexity.

At receiver end received digital signature is validated by using decryption process of Biogamal algorithm. It is observed that it is about 30-40% efficient with respect to playgamal algorithm with encryption/decryption time.

## REFERENCES

[1] Abdul Ghofar, Muhamad Hardi, Muhammad Nuur Firdaus, Guruh Fajar Shidik, “Digital Signature Based on PlayGamal Algorithm”, International Seminar on Application for Technology of Information and Communication (iSemantic), IEEE, Oct. 2017, pp. 58-65.

[2] Kadek Dwi Budi Utama , M. Rizqia Al-Ghazali Q. , Leonardus Irfan Bayu Mahendra, Guruh Fajar Shidik, “Digital Signature using MAC Address based AES128 and SHA-2 256-bit”, International Seminar on Application for Technology of Information and Communication (iSemantic), IEEE, Oct. 2017, pp. 72-78.

[3] Sergei G. Chernyi, Aslamin A. Ali,Vycheslav V. Veselkov, Ivan L. Titov, Vlad Yu. Budnik, ”Security of Electronic Digital Signature in Maritime Industry”, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Feb 2017, pp. 29-32.

[4] S. Alam, A. Jamil, A. Saldhi, and M. Ahmad, “Digital Image Authentication and Encryption using Digital Signature,” in International Conference on Advances in Computer Engineering and Applications (ICACEA), March 2015, pp. 332 – 336.

[5] S. A. Jaju and S. S. Chowhan, “A Modified RSA Algorithm to Enhance Security for Digital Signature,” in International Conference and Workshop on Computing and Communication (IEMCON), Oct 2015, pp. 1-5.

[6] M. C. A. Kioon, Z. Wang and S. D. Das, "Security Analysis of MD5 algorithm in Password Storage," in International Symposium on Computer, Communication, Control and Automation, 2013, pp. 0706-0709.

[7] Prakash Kuppuswamy, Peer Mohammad Appa,Dr. Saeed Q Y Al-Khalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher", IOSR Journal of Computer Engineering (IOSRJCE) Volume 7, Issue 1, Nov. - Dec. 2012, PP 47-52.

[8] Sandro Gerić, Tomislav Vidačić, "XML Digital Signature and its Role in Information System Security", MIPRO 2012, May 21-25,2012, Opatija, Croatia.

[9] Minh H. Nguyen, Duy N. HOi, Dung H. Luu, Alexander A. Moldovyan, and Nikolay A. Moldovyan, "On Functionality Extension of the Digital Signature Standards", International Conference on Advanced Technologies for Communications (ATC 2011).

[10] Qiuxia Zhang , Zhan Li , Chao Song, "The Improvement of digital signature algorithm Based on elliptic curve cryptography", International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), IEEE, August 2011, pp. 1689 - 1691.

[11] Zuguang Xuan, Zhenjun Du, Rong Chen, "Comparison Research on Digital Signature Algorithms in Mobile Web Services", National Natural Science Foundation of China, IEEE, sept-2009.

[12] Deng Jian-zhi, Cheng Xiao-hui, Gui Qiong, "Design of Hyper Elliptic Curve Digital Signature", International Conference on Information Technology and Computer Science, july 2009, pp.45-47.

[13] Xiang Can, You Lin, "A New Conic Curve Digital Signature Scheme", Information Assurance and Security, Aug-2009, pp. 623-626.

[14] Chen Hai-peng, Shen Xuan-jing, Wei Wei, "Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System", International Workshop on Education Technology and Computer Science, May 2009, pp. 618-624.

[15] Gordon W. Romney, "Digital signature signing engine to protect the integrity of digital assets", IEEE, April 2007.

[16] Santi Jarusombat and Surin Kittitornkun, "Digital Signature on Mobile Devices based on Location", IEEE, 2006.

[17] Scott Campbell, "Supporting Digital Signatures in Mobile Environments", IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03), IEEE, 2003.

[18] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multi signature", IEEE Proc.- Comput. Digit. Tech., Vol. 141, No. 5, September 1994.