International Journal of Industrial Engineering & Production Research June 2020 Vol. 31, No. 2: 301-308
DOI: 10.22068/ijiepr.31.2.301

RESEARCH PAPER

Comparative Analysis of MOD-ECDH Algorithm and Various Algorithms

O Sri Nagesh*[1] & Vankamamidi S Naresh[2]

Received 18 April 2020; Revised 28 April 2020; Accepted 3 May 2020; Published online 30 June 2020

ABSTRACT
Cryptography has remained a well-known and well-researched topic for ages. It is the first line of defense for any networked system. A lot of algorithms have been developed using symmetric and asymmetric cryptographies. From the security point of view, Asymmetric Cryptography is more popular due to its enhanced security. RSA, DSA, ECS, DES, ECC, and other algorithms have been developed for realizing Asymmetric Cryptosystem. These algorithms are primarily used to ensure a secure and reliable communication. These algorithms play a vital role in establishing a secure line of communication. Elliptic Curve Cryptography (ECC) provides the same level of security with a smaller key size. In the present paper, a developed MOD-ECDH was proposed and, then, it was compared with other various popular algorithms like ECDH, RSA, and ECS. Empirical and simulation results of applying the algorithms of ECDH and MOD-ECDH were described in detail. According to the result analysis, it is evident that the proposed algorithm outperforms other algorithms in terms of processing time and key size.

KEYWORDS: *Elliptic curve diffie-hellman algorithm (ECDH); Modified elliptic curve diffie-hellman algorithm (Mod-ECDH); Elgamal cryptosystem (ECS); Rivert shamir adelman (RSA); diffie-hellman (DH); Voice over internet protocol (VoIP).*

1. Introduction

Two keys in asymmetric cryptography are used: one is the public key given to all users and the other is the private key known by the owner only. Public key is generated by the end user using mathematical derivation. An elliptic curve is drawn using ECDH algorithm and, based on the agreed-upon points, both parties will exchange data. By using these parameters, both parties perform encryption and decryption operations during the conversation between sender and receiver.

In the asymmetric key cryptosystem, a secret key is not shared between sender and receiver, which will not make data communication insecure. Symmetric key cryptography is faster than asymmetric cryptography because of generating two keys. A lot of researchers have developed many algorithms to increase the speed of asymmetric cryptography. Elliptic Curve Cryptography (ECC) [11] has been developed with a smaller key size that enjoys high security. ECC is the best alternative to RSA-based cryptosystem [4]. RSA requires 1024 bits of key size because ECC requires only 160 bits for equal security [2, 3].

Cloud paradigm is used for offering high-quality, fast services to users and it is the best delivery model used globally. Bernstein et al. [5] proposed group operations on Edwards curve. Cloud paradigm is also used as the best Customer Relationship Management (CRM) tool. Cloud paradigm is also useful for IOT and Mobile communication technologies.

Data flows in communication networks and they are always at risk to more vulnerabilities or security breaches. These security threats may include breach of confidentiality, data integrity problems, authenticity problem by impersonation, man-in-the-middle-attack, and insider attacks. In order to overcome these breaches, some algorithms have been developed [9]. These

* Corresponding author: ***O Sri Nagesh***
osrinagesh@srivasaviengg.ac.in

1. *Department of CSE, Sri Vasavi Engineering College, Tadepalligudem-534101, A.P, India, Department of CSE, Sri Vasavi Engineering College, Tadepalligudem-534101, A.P, India.*
2. *Department of CSE, Sri Vasavi Engineering College, Tadepalligudem-534101, A.P, India.*

algorithms include RSA, Elgamal, ECDH, etc, [15, 26]. With regard to these algorithms, there is a need to consider security issues, privacy issues, bandwidth issues, speed, etc. [10]. Among all these algorithms, ECDH is efficient because of its smaller key size and higher security.

Motivation: Cloud computing is used as the latest emerging technology in Banking, E-Commerce, and many more sectors. Cloud technology eliminates the overheads of vendors and enterprises of cost per use paradigm. By using virtualized technology, cloud computing provides dynamic data retrieval and storage. Users can utilize cloud services from any point in the world. In order to use this technology, it is very crucial to realize and perceive cloud technology in total. Web services and virtualization are the key concepts associated with cloud technology. Mobile computing also uses cloud technology. Cloud technology supports four deployment models: public model, private model, hybrid, and community clouds. Different service models are also available such as Infrastructure as Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). SLA is also very important between the service provider and customer and provides security services, as well.

The major motivation behind this work is to overcome the security issues in the cloud environment. Identified problems are resolved using a new algorithm such as time for processing the data and key, the time taken for encryption and decryption, and the time taken for uploading files. To refine the above problems, various existing algorithms should be studied and compared with the proposed algorithm.

Contribution: The key contribution of this work is to build MOD-ECDH algorithm. Further, a comparative analysis of the proposed and various existing algorithms such as ELGAMAL, ECDH, and MOD-ECDH was made, and it was shown that the proposed algorithm was optimal in terms of various parameters such as key size and processing time such as key generation, encryption/decryption time, and and upload time.

Organization: The organization of the paper is as follows: Section 2 discusses works related to the security measures of encryption speed and security analysis. Section 3 describes the significance of ECDH algorithm based on ECC. In this algorithm, the key size is small and security is high. In Section 4, the proposed algorithm is discussed. The experimental setup and different analysis parameters are discussed in Section 5. Section 6 discusses the future work followed by concluding remarks in Section 7.

2. Related Works

Faiqa Maqsood et al. [6] applied DES and Blowfish that are symmetric algorithms in cloud servers on the parameters of power consumption, encryption speed, and security analysis. H T Loriya et al. [7] applied five asymmetric keys of RSA, DH, ECC, ECS, and NTRU and compared their key sizes. Jaspreet et al. [8] studied Elgamal cryptosystem that is also a public key cryptographic algorithm. In this algorithm, three major processes are included: encryption, decryption, and key generation. In this system, a sender, Alice, needs to send a private message to the recipient Bob, and a third-party Eve who is a man in the middle tries to gain access to this message. The ElGamal PKC procedure works as shown below. In the first step, Bob (Receiver) should compute a public key and send it to the Alice (Sender). After receiving Bob's public key, she does the encryption, which comprises of computing the cipher text from the plaintext. She sends this cipher text to Bob. Then, Bob decrypts the cipher text to compute a plaintext using his private key. In doing so, the third person (EVE) will remain unaware of, or have no access to, the secret key since it has been derived from Discrete Logarithmic problem. ELGamal algorithm is one of the important algorithms in the encryption process, which is used to randomize the process.

Rahman et al. [14] implemented RSA for speech data encryption and decryption. The RSA system uses one-way functions of more complex nature. Being complex in nature, RSA is more reliable. Specifically, the system uses modular arithmetic to transform a message into an unreadable ciphertext. The security of RSA is higer with larger key sizes.

Bafandehkar et al. [15] compared RSA with ECC in resource-constrained devices. In terms of the usage of key sizes, ECC is smaller and RSA is larger. Therefore, upload time, encryption time, and decryption time are longer for RSA than ECC for the same security level.

Baban et al. [16] carried out a comparative study of leach, Leah-Egenetic algorithm, and elliptic curve cryptography techniques to ensure security against Sybil attack in wireless sensor networks. Because of smaller key size, power consumption is low because WSN networks are energy-hungry nodes. Rafael et al. [17] analyzed different public key cryptosystems with respect to the key sizes. Ravi Kishore et al. [19] used ECDH-based security model for IoT using ESP8266. Subashri et al. [21] used Modified ECDH algorithm for VoIP Networks. Vijayakumar et al. [25] conducted an analysis of RSA and ECC for key generation time, memory requirement time, and

encrypt/decrypt time [12, 13]. Ahirval et al. [18] considered the role of ECDH key exchange algorithm in securing hypertext information in a wide area network. Rifaqat et al. [20] developed a smartcard-based remote-user authentication scheme in a multi-server environment. Hafizul et al. [22] identified some deficiencies in Tan's 3PAKE protocol and, then, devised an improved 3PAKE protocol without symmetric key en/decryption technique for mobile-commerce environments. Natanael et al. [1] described the role of ECC algorithm in securing text messages in messaging application of a smart phone. Ziad et al. [27] proposed converting Hill cipher from symmetric technique to asymmetric one, increased its security and efficiency, and promoted its resistance against the hackers. Naresh et al. developed an algorithm for provable secure group key agreement protocol based on ECDH algorithm [23] and, also, a provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks [24].

3. Elliptic Curve Diffie-Hellmann Key Exchange (ECDH)

In this section, ECDH is discussed. Elliptic curve Diffie-Hellmann key exchange (ECDH) is an FHE scheme that provides parties engaged in communication with a pair of keys, namely public and private key, for encryption of the data that they transact among each other within an insecure channel. The message shared through the channel can be directly derived using public key or they may have to calculate the private key and decrypt the data. These derived keys can then be used as the key to the successive data transactions that take place between the committed parties in the channel. The work flow of an ECDH scheme will execute the following steps for transacting data between sender S and receiver R.

- Initially, an elliptic curve parameter should be agreed upon by all parties and an elliptic curve should be generated by them, as well.
- At the next step, each party should choose a pair of keys: one is the private key d, a random unique point chosen in the curve, and public key derived Q=dG, where G is the generator of curve.
- Let the keys of sender be (d_A, Q_A) and keys of receiver be (d_B, Q_B). Public key Q can only be shared with others during communication and, accordingly, only a person who has received the message sent by the sender can decrypt it.
- During the transmission of a message in the ECDH system, a message or data denotes a point in the elliptic curve (x, y).
- The point (x, y) can be calculated by the receiver and the message can be decrypted via the product $Q_B d_A$ or $Q_A d_B$.
- The ECDH encrypted messages always possess symmetric property as in the following: $d_A Q_B = d_A d_B G = d_B d_A G = d_B G$.

However, ECDH encrypts data efficiently using symmetrical encryption property and it is more vulnerable to chosen plain text attacks and ciphertext attacks. Its larger key size will be a major issue concerning the encryption and decryption time, which contributes to a major delay in the cloud framework or CS. To resolve the vulnerability of CS against attacks and improve the speed of encryption and decryption, the Mod-ECDH is proposed and explained in the later section.

4. The Proposed Algorithm: MOD-ECDH

The limitations mentioned in the previous section were solved by integrating the encryption and hashing scheme directly into the elliptic curve module. Thus, the time required to complete the encryption and decryption processes is shortened and, also, the communication overhead is reduced; therefore, the key size is smaller than that of ECDH.

4.1. Modified elliptic curve diffie-hellmann key exchange (MOD-ECDH):

Mod-ECDH is an improved encryption scheme which is capable of provisioning semantic privacy confidentiality over external attacks like ciphertext attacks and plain text attacks. The following steps describe the performance of the Mod-ECDH algorithm:

- In Mod-ECDH, the sender learns the receiver's public key g^x where x is the private key of the receiver.
- Then, sender generates a new key value y and its associated value g^y
- The sender calculates the symmetric key, k, using Key Generation Function (KGF) $k=KGF(g^{xy})$
- Now, the sender encrypts the data using k to generate the ciphertext c of the message, which needs to be sent: c=E (k: m) where m is the message.
- Then, the sender transmits both the ciphertext and public key (c; g^y). Since the receiver has both the x and g^y values, it can

able to decrypt the ciphertext and retrieve the original message.

Thus, the Mod-ECDH algorithm encrypts the data with fewer complexities and in a shorter amount of time which is also a secure hashing method that resists external attacks. Since the ECDH algorithm is integrated into the key generation parameters, its communication cost or communication overhead is also reduced. The encryption and decryption using Mod-ECDH are detailed as follows.

4.1.1. Encryption

To encrypt a message msg, the Mod-ECDH should undergo the following steps:

- Manipulating a random integer 'r' at the interval $r \in [1, n-1]$ and computing R=rG where G is the generator of the elliptic curve
- Computing the shared secret sec=pub_x, where pub=(pub_x, pub_y) = rK_R and K_R= public key of receiver and $pub \neq \emptyset$.
- Deriving symmetric encryption keys and Message Authentication Code (MAC) keys using $k_E \parallel k_M = KGF(S \parallel S_1)$.
- Encrypting the message msg through encryption key k_E c=Encryption(k_E;msg)
- Calculating the MAC of the encrypted message $S_2 : d = MAC(k_M; c \parallel S_2)$
- Finally, sending the ciphertext output c to the receiver encrypted using private key d it is represented as $R \parallel c \parallel d$.

4.1.2. Decryption

In order to decrypt the ciphertext message, the receiver R should perform the following tasks:

- First, receiver needs to derive the shared secret $S = P_{ubx}$ where pub=(pub_x, pub_y)=K_RR =rK_RGand K_R= public key of receiver and output fails if $pub = \emptyset$
- Then, it computes the decryption key from $k_E \parallel k_M = KGF(S \parallel S_1)$
- Then, it calculates the MAC to verify the tag and whether output fails or not by $d \neq MAC(k_M; c \parallel S_2)$.
- Finally, it utilizes the symmetric encryption key to decrypt the original message $m = E^{-1}(k_E : c)$.

5. Experimental Setup

In this section, the experimental setup for the comparative study has been described. The proposed algorithm has been compared with RSA, ECS, ECDH, and Mod-ECDH. The empirical modeling has been done using JDK1.8 and NetBeans 8.2 IDE.

To evaluate the proposed algorithm, 150 different files from different sources are used, as shown in Table 1. The size and type of files are different, as depicted below.

Tab. 1. Set of files used to evaluate CA

S. No.	Type of File	No. of Files	Source
1	Document	37	Microsoft Word
2	Text	25	Notepad
3	Image	35	Internet
4	PDF	14	Internet
5	Video	24	YouTube
6	Audio	3	Internet
7	Power Point	12	Microsoft PowerPoint

Table 2 shows 25 different files with 25 different sizes. These files are used to calculate encryption, decryption, and upload times.

Tab. 2. Timing Measures of the proposed Mod-ECDH system (ms)

S. No.	Type of File	Size of File (KB)	Upload Time of Mod-ECDH algorithm	Encryption Time of Mod-ECDH algorithm (Proposed)
1	Text	10	127	108
2	Text	14	132	112
3	Text	16	145	125
4	Text	22	145	125
5	Text	25	146	132

6	Text	23	146	132
7	Text	31	148	136
8	WORD	37	148	136
9	WORD	125	157	142
10	WORD	1075	183	148
11	Photo	1248	189	153
12	Photo	1551	207	172
13	Photo	18464	213	187
14	Photo	33123	215	193
15	Photo	37420	224	206
16	Photo	72748	287	248
17	Photo	1154490	301	251
18	Photo	1155207	301	257
19	Mp3	3507764	326	258
20	Mp4	5120428	328	267
21	Mp3	10325038	331	268
22	Mp4	20570492	332	270
23	Mp3	21674900	334	281
24	Video Mp4	27233473	334	287
25	Video Mp4	2733537	335	293

Case 1: Encryption time: Fig1 shows the graph for Upload time for Mod-ECDH (Proposed) algorithm with different sizes of files.

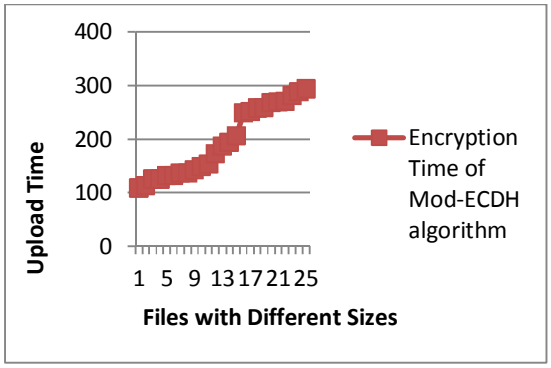
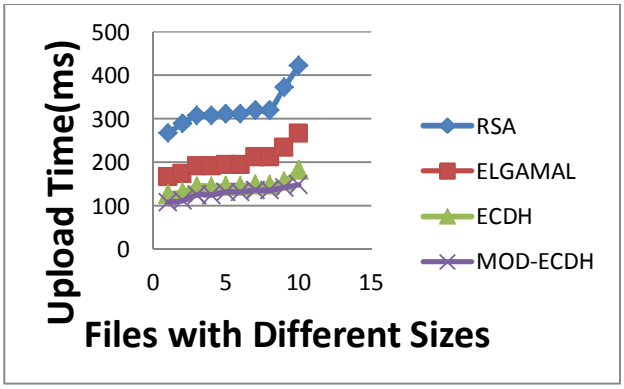


Fig. 1 Encryption Time for Files with Different Sizes

Case 2: Upload time: Table 3 and Fig. 2 show the comparison of various algorithms such as ECC, RSA, and ECS and the proposed algorithm.

Tab. 3. Upload time for various files in Milli Seconds

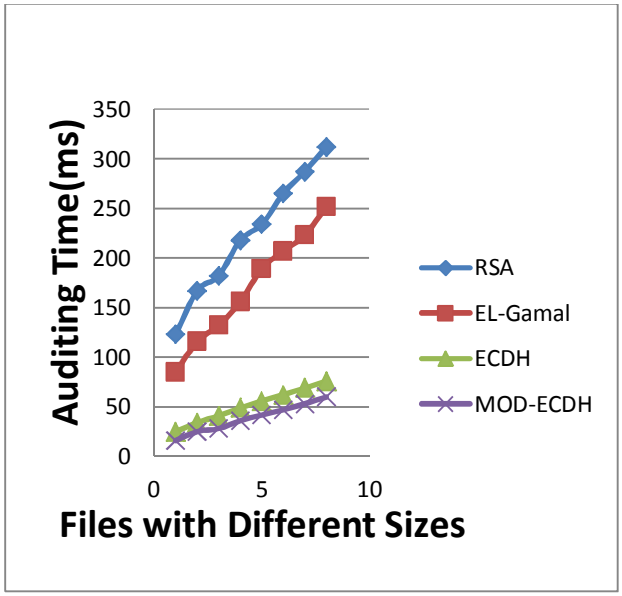
S.No	RSA	EL-GAMAL	ECDH	MOD-ECDH(Proposed)
1	267	166	127	108
2	289	173	132	112
3	308	191	145	125
4	308	191	145	125
5	312	194	146	132
6	312	194	146	132
7	320	212	148	136
8	320	212	148	136
9	372	234	157	142
10	422	266	183	148



Case. 3. Auditing Time: Table 4 and Fig. 3 show the analysis of Auditing time taken by various files in milli seconds.

Tab. 4. Auditing time for various files in ms

S.No	RSA	EL-GAMAL	ECDH	MOD-ECDH (Proposed)
1	123	85	25	16
2	167	116	34	25
3	182	132	41	28
4	218	156	49	36
5	234	189	56	42
6	265	207	62	47
7	287	223	69	53
8	312	252	76	60



6. Future Work

The asymmetric key algorithms can ensure a higher level of security**.** The security of the algorithm depends on its key size. The larger the key size, the more secure the algorithm. Greater computation power is needed when using a larger key size. Therefore, a larger key size will reduce the performance of algorithms. To improve their performance, one can use Mod-ECDH algorithm, which can be satisfied by the development of the scalar multiplication algorithm as the primary algorithm in ECDH. To attain this, there is a need to propose an efficient algorithm that can improve scalar arithmetic and point arithmetic. Furthermore, privacy and security calculations need to be enhanced to ensure the security of algorithms against side channel attacks. Mod-ECDH algorithm hopes to shine in terms of its low cost and high efficiency and will outperform

the other existing algorithms in terms of competence and efficiency.

7. Conclusion

It is a necessity to protect data from disclosure over cloud server. To this end, the data transmission should be monitored continuously as the data flows continuously over cloud. Thus, CA is used to monitor the Mod-ECDH (proposed) algorithm. To protect data integrity, confidentiality, and non-repudiation, we need to use the auditing technique continuously when data are flowing through an insecure channel. CA methodology and the Mod-ECDH encryption technique efficiently encrypt the blocks of data in a short amount of encryption time. Thus, the upload time of documents in a CS is also reduced. The modifications in blocks of data and challenges are continuously monitored. If the challenge is dealt with a response by data integrity verification from the user side, the previous block is removed from its cache; otherwise, it recovers the original block of data with the recently modified data. Thus, the privacy of the user's data is protected by block hashing using Mod-ECDH and is secure against external attacks. In the future, the challenge verification of the system can be done with the digital signature mechanism for each user to verify the originality of him/herself in the secured framework. The proposed algorithm encrypts data faster than the different algorithms shown above. Characterized by the smaller key size, the Mod-ECDH algorithm shows good performance when using WSN networks and Mobile networks as they are energy-hungry nodes. In Vehicular communication networks, the algorithm shows good results as plain text attack and minimizes cyphertext attacks. This algorithm shows positive results when using mobile Adhoc networks.

Rerefences

[1] Dimas Natanael, Faisal, Dewi Suryani, "Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC)" in the 3rd International Conference on Computer Science and Computational Intelligence (2018).

[2] Dindayal Mahto, Dilip Kumar Yadav "RSA and ECC: A Comparative Analysis",International Journal of Applied Engineering Research (2017).

[3] Dindayal Mahto, Member, IAENG, Danish Ali Khan, Member, IAENG and Dilip Kumar Yadav, Member, IAENG "Security Analysis of Elliptic Curve Cryptography and RSA", Proceedings of the World Congress on Engineering Vol. I, (2016).

[4] Dr. K.L. Vasundhara, Y. V. S. Sai Pragathi, Y. Sai Krishna Vaideek ,"A Comparative Study of RSA and ECC", Int. Journal of Engineering Research and Application , Jan (2018).

[5] D.J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. Asiacrypt, LNCS 4833, (2007), pp. 29-50.

[6] Faiqa Maqsood, Muhammad Ahmed , Muhammad Mumtaz Ali, Munam Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques", International Journal of Advanced Computer Science and Applications, (2017).

[7] H.T.Loriya, A. Kulshreshta, D. R. Keraliya,"Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network.", International Journal of Advanced Research in Computer and Communication Engineering, ISSN: 2278-1021, (2017).

[8] Jaspreet Kaur Grewal, "ElGamal:Public-Key Cryptosystem", Math and Computer Science Department Indiana State University Terre Haute,IN,USA, (2015).

[9] J. A. Buchman. Introduction to cryptography. Springer-Verlag, New York, second edition, (2004).

[10] J. Ho_stein, J. Pipher, and J. H. Silverman. An introduction to mathematical cryptography. Springer-Verlag, New York, (2008).

[11] J. Fan, K. Sakiyama, and I. Verbauwhede. Elliptic curve cryptography on embedded multicore systems. WESS (2007), pp. 17-22,

[12] J.C. Ha, J. Park, S. Moon, and S.M. Yen. Provably secure countermeasure resistant to several types of power attack for ECC. WISA, LNCS 4867, (2007), pp. 333-344.

[13] M. Benaissa and W. M. Lim. Design of flexible GF(2*m*) elliptic curve cryptography processors. IEEE Transaction Very Large

Scale Integr. (VLSI) Syst., Vol. 14, No. 6, (2006), pp. 659-662.

[14] Md. Mijanur Rahman, Tushar KantiSaha, Md. Al-Amin Bhuiyan,"Implementation of RSA Algorithmfor Speech Data Encryption and Decryption", IJCSNS International Journal of Computer Science and Network Security, Vol. 12, No. 3, (2012).

[15] Mohsen Bafandehkar, Sharifah Md Yasin, RamlanMahmod, ZurinaMohdHanapi, "Comparison of ECC and RSA Algorithm in Resource Constrained Devices", IEEE Explore, (2013).

[16] Omar BadeeaBaban ,"Comparative Study between Leach,Leah-EGenetic Algorithm and Elliptic Curve Cryptography Techniques to Secure Against Sybil Attack In WSN", International Journal of Computer Science and Information Technologies, (2017).

[17] Rafael Alvarez, Cándido Caballero-Gil, Juan Santonja, and Antonio Zamora "Algorithms for Lightweight Key Exchange",Sensors 2017, 17, 1517; doi:10.3390/s17071517.

[18] Ram Ratan Ahirwal, ManojAhke "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information onWide Area Network", International Journal of Computer Science and Information Technologies, Vol. 4, No. 2, (2013).

[19] Ravi Kishore Kodali and AshwithaNaikoti "ECDH based Security Model for IoT using ESP8266", IEEE Explore, (2017).

[20] Rifaqat Ali, Arup Kumar Pal "An efficient three factor–based authentication scheme in multiserver environment using ECC" Research article *in* International Journal of Communication Systems (2017).

[21] Subashri Thangavelu and Vaidehi Vijaykumar, "Efficient Modified Elliptic Curve Diffie-Hellman Algorithm for VoIP Networks", The International Arab Journal of Information Technology, Vol. 13, No. 5, (2016).

[22] S.K. Hafizul Islam, Ruhul Amin, G.P. Biswas, Mohammad Sabzinejad Farash, Xiong Li, Saru Kumari, "An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for King Saud University in (2017).

[23] Vankamamidi S Naresh, Nistale VES Murthy "Provable secure lightweight hyper elliptic curve based communication system for wireless sensor networks" John-Wiley-International Journal of Communication Systems (2018).

[24] Vankamamidi S Naresh, Nistale VES Murthy "Provably Secure Group Key Agreement Protocol based on ECDH with integrate signature" John-Wiley-International Journal of Communication networks (2016).

[25] Vijayakumar Perumal, Xiao- Zhi Gao,"Comparative analysis of Elliptic Curve Cryptosystem and its survey", Journal of Chemical and Pharmaceutical Sciences, (2017).

[26] William Stallings, "Cryptography and Network security Principles and Practice"Fifth Edition, (2006), Pearson Edition.

[27] Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cypher" in Journal of King Saud University in (2017).

Follow This Article at The Following Site:

Nagesh O S, S Naresh V. COMPARATIVE ANALYSIS OF MOD-ECDH ALGORITHM WITH VARIOUS ALGORITHMS. IJIEPR. 2020; 31 (2) :301-308
URL: http://ijiepr.iust.ac.ir/article-1-1061-en.html