Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

# Renowned Information Security Algorithms: A Comparative Study

K. Sujatha
Research Scholar,
GITAM University, Visakhapatnam

P V Nageswara Rao
Professor,
GITAM University, Visakhapatnam

A Arjuna Rao
Director and Principal,
Miracle Educational Society Group of Institutions,
Vizianagram

L V Rajesh
Associate Professor,
Miracle Educational Society Group of Institutions,
Vizianagram

*Abstract :* **Authentication and Encryption with Key Exchange are the key concepts in Cryptography, which have been continuously being targeted. Many Security Algorithms are developed as research outcome and they are broadly classified into Symmetric and Asymmetric algorithms. Symmetric Algorithms are conventional which use a common secret key that is transmitted by using physical or other communication channel. Data Encryption Standard, Triple Data Encryption Algorithm, International Data Encryption Algorithm, Blowfish and AES are the algorithms that are categorized into Symmetric. In order to make key distribution easy, Asymmetric Key algorithms such as Rivest Shamir Adleman, Diffie Hellman, Elgamal, Digital Signature Algorithm and Elliptic Curve Cryptography, are used for Encryption and Authentication where secret key remains with generating user. Rivest Shamir Adleman, ElGamal and Elliptic Curve Cryptography are the most widely used public key algorithms that perform Key Exchange and used for both authentication and confidentiality. Digital Signature Algorithm is a generally applied digital signature system where as Diffie Hellman is used only for Key Exchange. This paper presents a review of the renowned Symmetric and Asymmetric algorithms. The specified algorithms are developed and test results are presented comparing the performance and key sizes.**

***Keywords: Authentication, Encryption, Symmetric Algorithms, Asymmetric Algorithms, Data Encryption Standard(DES), Triple Data Encryption Algorithm(TDEA), International Data Encryption Algorithm(IDEA), Blowfish and Advanced Encryption Standard(AES), Rivest Shamir Adleman (RSA), ElGamal, Elliptic Curve Cryptography(ECC), Digital Signature Algorithm(DSA).***

## 1. INTRODUCTION

Encryption is the means of analytically modifying data to make it illegible to unauthorized users. Sender encrypts the Data which moves over the network in coded form. The computer at the receiving end then decrypts the data in order to read the message. Encryption methods have been around for centuries. The majority of computer encryption algorithms are outcome of the modifying operations of large prime numbers. The algorithms are intensely based on mathematics and Encryption techniques are used for ensuring confidentiality, integrity and authentication [1].

There are several encryption algorithms which are unique. Though they are strong to some extent there are flaws like some fail in confidentiality not resistant to existing attacks. Strength is ability of a cryptographic system to safeguard information from attack which depends on factors listed[2].

- Secret key : maintaining secrecy in key
- Key Search: difficulty in key guessing or using all possible keys.
- Known plaintext Attack: Decrypt with some known plaintext.
- Encryption Algorithm Breaking: Encryption algorithm is cracked without knowledge of the encryption key
- Create New Techniques: Decrypt the encrypted file more easily without knowing the key.

To prove the strength of an algorithm, a mathematician has to show that the algorithm is challenging to specific type of attacks that earlier proved on other algorithms. However even an algorithm that is resistant to each known attack cannot considered to be secure, as new attacks are constantly being developed.

## 2. SYMMETRIC ENCRYPTION

Symmetric encryption is now and then called conventional encryption since it is the initially utilized before the improvement of public key systems. Symmetric encryption is most regularly utilized even now, albeit open key uneven encryption has recently gotten significant thought. The decoding procedure is the converse of the encryption process thus it is called as the symmetric encryption [1].

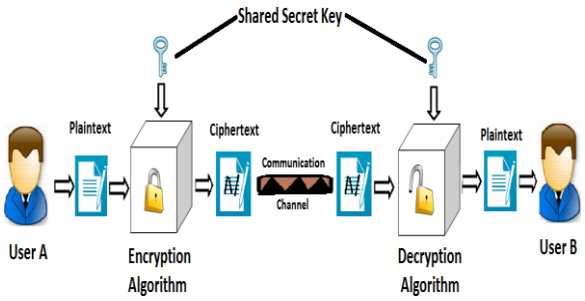


Fig 1: The symmetric encryption process.

Symmetric encryption/decryption process as shown in figure 1 follows the process as listed [2].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

1. One key value known as secret key is made available jointly to the sending and receiving users who wish to communicate.
2. The sending user applies secret key on the encryption algorithm and encrypts the data to generate cipher text.
3. The cipher text is delivered to the target user.
4. The receiving user applies the same secret key on a decryption algorithm to decrypt the data to obtain the plaintext.

Symmetric encryption should be carefully executed and then it can be extremely secure. The most significant considerations for enhancing the security of any encryption scheme are as listed [2]:

1. The encryption algorithm strength
2. The key strength
3. The key secrecy

128-bit key breaking might happen if the key is not kept to be sufficiently secure. The software system should offer some secure suggests that for delivering the key to the receiving laptop by mistreatment varied key delivery systems instead of sealed cover method of passing the key. If the secret key is derived, everything is disclosed. Periodic renewal of the secret key is done to beat this downside. The distinctive key utilized by a combine of human action computers could be make with each session or when a given quantity. Key renewal will increase the amount of keys crossing the network that compounds the requirement for effective key protection.

Several noted cryptography algorithms as shown in figure 2 a pair of create use of symmetric cryptography. the foremost illustrious symmetric algorithm could be the information cryptography customary (DES). DES is employed with many common cryptography techniques, together with Kerberos. DES uses a 56-bit key, that several specialists say is simply too small. The DES algorithm was truly cracked through brute-force techniques during a check work in 1998.

Triple DES (3DES) is that the common name for the Triple encoding algorithm or TDEA, a symmetric-key block cipher that applies the information cryptography DES cipher algorithm thrice to every data block. The Advanced cryptography customary or AES could be a symmetric block cipher utilized by the U.S. government to shield classified data and is enforced in software package and hardware throughout the globe to write in code sensitive knowledge. Different conventional cryptography algorithms embody the 128-bit key plan algorithm. The Blowfish usually uses a 128-bit key, though key length could vary to up to 448 bits.

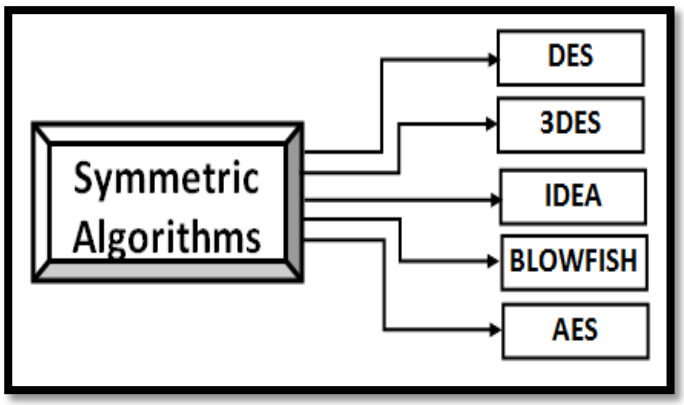


Fig. 2: Renowned Symmetric Algorithms

*2.1 Data Encryption Standard (DES)*

DES designed by IBM was the first encryption standard to be published by NIST which is minor variation of Feistel network. Feistel cipher structure uses basically two operations, Substitution and Permutation. This has sixteen rounds and generates 16 subkeys from original key, one for each round [3]. The DES was initially considered as a strong algorithm and is most widely used, but today the large amount of data and short key length of DES limits its use. The DES key size is only 56 bits which is very short for proper security, as this can be brute-forced[4]. DES uses 64-bit blocks that raise probable issues while encrypting huge amount of data with the same key. Encryption requires plaintext, P and key, K as input as shown in equation (1) generates ciphertext.

$$C = E(K, P) \quad -(1)$$

Decryption as shown in equation (2) uses ciphertext, C and Key, K as input, and generates plaintext, P, but uses subkeys $K_i$ in reverse order[5].

$$P = D(K, P) \quad -(2)$$

*2.2 Triple-DES (3DES)*

3DES was standardized to be used in 1985 however printed in 1999. 3DES was far more difficult version of DES achieving high level of security by encrypting the info exploitation DES 3 times exploitation with completely three different unrelated keys. 3DES remains approved to be used by U.S.A. governmental systems. 3DES is secure up to a minimum of 2168 security that is tough to interrupt as this uses a key length of 168 bits. However it is slow, particularly in package and hardware implementation is really crucial. The encoding operate follows encrypt-decrypt-encrypt (EDE) sequence, with Plaintext, P, Ciphertext, C, and 3 distinct keys $K_1$,$K_2$,$K_3$ with every key being fifty six bits, equation(3) shows this process[6].

$$C = E(K_3, D(K_2, E(K_1, P))) \quad -(3)$$

Decryption is the same processed while applying keys in reverse order as in equation (4).

$$P = D(K_1, E(K_2, D(K_3, C))) \quad -(4)$$

Multiple DES proposed by the authors of this paper uses DES encryption in random number of times and similarly decryption is also applied[7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

*2.3 International Data Encryption Algorithm (IDEA)*

James L. Massey and Xuejia Lai in 1990 developed an encryption algorithm named as International Data Encryption Algorithm[8]. This is quick, secure and impervious to both linear and differential analysis. This uses non-invertible hash function that does not use lookup tables or S-boxes and hence is one of secure block ciphers used in public domain. This utilize 52 subkeys, which are 16 bits long. The block of plaintext in IDEA is segmented of 16 bits length four quarters. In IDEA, three operations are utilized to merge two 16 bit values and generate a 16 bit result, with XOR, addition and multiplication[9].

*2.4 Blowfish Algorithm*

Bruce Schneier planned block cipher, Blowfish that is taken into account as a extremely rated secure encoding algorithm, with completely different structure and practicality than the opposite mentioned encoding algorithms[10]. Blowfish may be a quick, compact, and straightforward block encoding algorithm with variable length key permitting a trade-off between speed and security. The block size is sixty four bit and uses 16-round Feistel Cipher and enormous key-dependent S boxes[11,12]. The algorithm keeps 2 subkey arrays; 18-entry P-array and 4 256-entry S-boxes. The S-boxes settle for 8-bit input and turn out 32-bit output. One entry of the P-array is employed each spherical, and once the ultimate spherical, every half the info block is XORed with one amongst the 2 remaining unused P-entries[13,14].

*2.5 Advanced Encryption Standard(AES)*

Rijndael developed by Joan Daemen and Vincent Rijmen, is chosen as final AES algorithm in 1997 by NIST[15]. AES victimization variable key size is phenomenally fast and smaller cipher. Its centro-symmetric and parallel structure gives decent adaptability to implementers, with successful resistance against cryptological attacks. AES will be well uniquely designed to a decent fluctuate of recent processors such as Pentium, abridged instruction set parallel and computing processors. AES acknowledges keys of 128, 192 or 256 bits, and is prudent in every hardware[16]. This completely was chosen through associate open competition involving numerous cryptographers all through numerous years. This algorithmic rule procedures entire block in parallel and isn't a feistal structure. Each stage utilizes 3 substitutions and one permutation round. Substitution rounds square measure Substitute bytes, join columns and Add round key and permutation spherical is shift rows. There square measure ten rounds during this algorithmic standard [17].

*2.6 Advantages and Disadvantages of Symmetric Algorithms*

Symmetric algorithms are widely used due to the following advantages

1. Symmetric algorithms are much faster compared to asymmetric algorithms
2. Security of algorithm is dependent on the length of the key. Large key size makes the algorithm hard to break.
3. Uses less computing power.

The disadvantages of symmetric algorithms can be listed as follows.

1. Secure mechanism is required to deliver secret key confidentially.
2. Every pair of users needs a unique secret key. Multiuser sharing requires maintaining multiple keys.
3. Only confidentiality is provided but not authenticity as the key is shared.

## 3. ASYMMETRIC (PUBLIC KEY) ENCRYPTION

Public Key cryptography is an alternate approach that has emerged over the last twenty five years to unravel secret key distribution issues implicit with conventionally symmetrical cryptography. Asymmetric cryptography is named asymmetric as a result of the key wont to cipher the information is totally different from the key wont to rewrite the data[1]. This method is shown in figure 3.

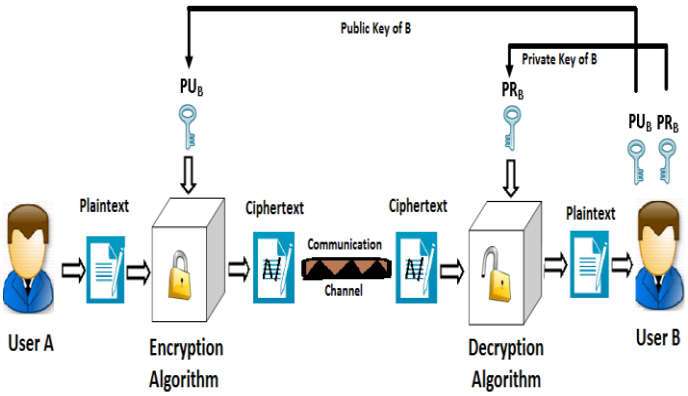


Fig. 3: Asymmetric encryption process.

Asymmetric encryption is an encryption method identified as public key encryption. However in public key encryption, out of the two keys, the private key is held securely with a sender. The other key, the public key is made available to users that need to move data to the possessor of the private key. The steps are as follows [2]:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

1. User A attempts to establish a communication channel with User B.
2. The user B produces a private key and a public key. The private key is not shared with anyone. The public key is made accessible to User A.
3. User A with the public key encrypts and transmits the data. The User B public key is stored on User A for future reference.
4. On receiving data User B decrypts it using the private key.

A significant side of public key strategies is that the coding performed through the general public key's a unidirectional operates. The general public key is accustomed encode the info, however solely the non-public key will decode the info once it's encrypted. Many renowned Asymmetric algorithms as listed in figure 4 supported Asymmetric coding [1].

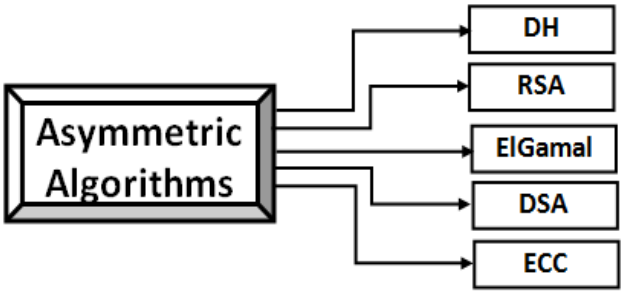


Fig. 4: Renowned Asymmetric Algorithms

*3.1 Diffie Hellman Key Exchange*

Diffie-Hellman uses a combine of keys, public and personal however is employed for key exchanges that generate shared keys [18]. This algorithmic rule uses arithmetic modulus because the basis of its calculation. Suppose user A and user B follow this key exchange procedure with Eve acting as a person in middle fighter. Here are the calculation steps followed during this algorithmic rule that create certain that eve never gets to understand the ultimate keys through that actual cryptography of information takes place. First, a hard and fast modulus (n) and generator (g) are shared among communication users A and B and exploitation them several personal and public key pairs is generated. personal key of A and B are chosen as xA and xB are generated and public secret's computed exploitation the personal key as in equation (5) [19]

$$yA = g^{xB} \bmod n$$
$$yB = g^{xA} \bmod n \quad - (5)$$

Then shared secret key, Key is generated at recipients end by user A and B, by using their private keys and sender's public keys as shown in equation (6).

$$Key = yA^{xB} \bmod n$$
$$Key = yB^{xA} \bmod n \quad - (6)$$

The result calculated using equations (8) and (9) produce identical result and hence a secret key is shared that can be used by symmetric algorithms [20,21].

*3.2 Rivest-Shamir-Adleman (RSA) Algorithm*

RSA is widely used in encryption and authentication using pair of keys, public and private. From each public key pair new modulus is generated. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman(RSA) [22]. The main operation of RSA is to compute modular exponentiation. Prime numbers generation gives good efficiency and strength to the algorithm. The cryptosystem based on RSA is on the assumption which factors large integers and computationally hard and mainly based on Primality Testing, Extended Euclidian's algorithm, Modular Exponentiation [23]. In Decryption, more computation time and capacity are required. This is included as part of the Web browsers from Microsoft and Netscape. RSA is a public-key cryptography based algorithm that presumes factoring problem, which is the difficulty of factoring large integers. There are three steps involved in the RSA algorithm that are key generation, encryption and decryption. RSA keys are of a power of two, like 512, 1024, or 2048 bits length [24].

First, a couple of large primes p and q are selected randomly and using p and q, n and Ø are calculated.

$n = p * q$

$Ø = (p-1)*(q-1)$

Exponent e is selected basing on n and private exponent d from e, p and q. Here, (n, e) is treated as the public key and (n, d) as the private key.The RSA encryption shown in equation (7) is the exponentiation tothe $e^{th}$ power modulo n

$$C = M^e \bmod n \quad - (7)$$

The decryption shown in equation (8) is performed as exponentiation to the $d^{th}$ power modulo n.

$$M = C^d \bmod n – (8)$$

*3.3 ElGamal*

The ElGamal algorithmic rule could be a public-key cryptosystem supported the separate exponent downside. It consists of each the coding and signature algorithms [25]. The ElGamal signature algorithmic rule is comparable to the coding algorithmic rule in this the general public key and personal key have a similar kind. However, coding isn't a similar as signature verification and signature creation depends on the ElGamal signature algorithmic rule.

The mathematical constructs needed area unit Cyclic teams, standard mathematical operation resolution algorithms etc. the most disadvantages of ElGamal area unit the necessity for randomness, and its slower speed and also the message growth by an element of 2 takes place throughout coding [26]. However, such message growth is negligible if the cryptosystem is employed just for exchange of secret keys ElGamal coding is employed

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

within secure package, recent versions of PGP and alternative cryptosystems. ElGamal isn't semantically secure. ElGamal algorithms can't solely be utilized in encoding, however in digital signature and also the security depends on the matter of divergence exponent in finite domains[27].

$$Y = g^x (\text{mod } p) - (9)$$

The private key is x. G and p can be shared by a group of user. ElGamal encryption consists of three components, the key generator, the encryption algorithm, and the decryption algorithm.

*3.4 Digital Signature Algorithm (DSA)*

NIST proposed DSA in August 1991 for digital signatures to employ in their Digital Signature Standard [28]. The DSA is employed by a person to come up with a digital signature on knowledge and to verify the believability of the signature. This uses a combine of keys, private and public for implementing digital signatures. The non-public key's employed in the signature generation method and also the public key's employed in the signature verification method [29].

For signature generation and verification, the info that is spoken as a message, M, is reduced by suggests that of the Secure Hash algorithmic rule (SHA) laid out in FIPS. In alternative words, signatures cannot be cast. However, by mistreatment the signatory's public key, anyone will verify a properly signed message[30]. Here, the generation of a new stored modulus is not done every time. The public key is composed of two pieces: the public key (y) and the modulus data (p, q, and g) where modulus size is in between 512 and 2048 bits with 64 bits increment. The personal key (x) may be a random 160-bit range. for each signature, a brand new 160-bit k is made. Once the signature is made, k may be destroyed. what is more, the signature method creates r and s, they're utilized in the verification method to come up with v that is compared to r to verify a signature [31].

A means of associating public and personal key pairs to the corresponding users is needed. That is, there should be a binding of a user's identity and therefore the user's public key. This binding could also be certified by a reciprocally trustworthy party, for instance, a certifying authority might sign credentials containing a user's public key and identity to make a certificate. DSA is highly secure because of the difficulty of computing the discrete log. The goal is to find the smallest natural number x as shown in equation (10), after choosing a prime p and α and β that are nonnegative integers mod p, t.

$$\beta \equiv \alpha x \ (\text{mod } p). \ - (10)$$

The x is the number indicated by $L_\alpha(\beta)$, the discrete log of β with respect to α. Generally, α is considered to be a primitive root mod p. Also α is a primitive root mod p if and only if $\{i \bmod p \mid 0 \le i \le p-2\} = \{1, 2, \ldots, p-1\}$ [32].

*3.5 Elliptic Curve Cryptography (ECC)*

ECC was discovered in 1985 by Victor Miller and Neil Koblitz severally, as another mechanism for implementing public-key cryptography[33,34]. Public-key algorithms produce a mechanism for sharing keys among massive numbers of participants or entities in a very advanced data system. Most public-key cryptosystems square measure engineered over arithmetic in finite fields which are algebraic structures that have addition and multiplication operations every with inverses. Error correction code builds a finite field out of the set of solutions to associate degree elliptic curve equation together with associate degree additive identity that corresponds to the purpose at infinity.

ECC is efficacious as a result of it's believed to be more durable to cipher, e.g., separate logs over the finite fields of code than within the underlying whole number finite fields. this implies that key sizes in code will be smaller than the corresponding key sizes in cryptosystems supported different fields. ECC is not, however, famed to be more durable than the other system [35].

ECC Challenge has opened a chance for folks round the world to form new ways of assaultive the formula and exposing any weaknesses. The ECC Challenge started in Nov 1997 and still runs today[36,37]. An Elliptic Curve is a curve given by the equation (11) which is in the form shown below is the main heart of this cryptography.

$$y^2 = x^3 + ax + b \quad - (11)$$

$$\{\text{where } \Delta = 4a^3 + 27b^2 \quad \text{is nonzero}\}$$

For maximum efficiency, a Koblitz curve is used with a=0 or a=1 shown in equation (12)

$$y^2 + xy = x^3 + ax^2 + 1 \qquad -(12)$$

*3.6 Advantages and Disadvantages of Asymmetric Algorithms*

The advantages of asymmetric algorithms listed are follows are the reasons for extensive usage.

1. Key distribution is better as secret key need not be shared
2. Provides both authenticity and confidentiality
3. Uses mathematical operations rather than bitwise operations and substitutions.
4. Ideally suit for real world applications. Public keys can be available and other key is safe with user.

The disadvantages of asymmetric algorithms are listed as follows.

1. Slower than symmetric algorithms as many of them involve Modular Exponentiation.
2. Complex in mathematical tasks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

## 4. RESULTS

The symmetric algorithms and asymmetric which are specified in sections 2 and 3 are thoroughly compared by using both literature survey and test results obtained after executing the various algorithms.

### *4.1 Symmetric Algorithms*

The symmetric algorithms are developed and tested on sample data. The common features are summarized as listed in table 1

Table 1 : Salient Features of Renowned Symmetric Algorithms

| Algorithm | DES | TDEA (Triple DES) | IDEA | BLOWFISH | AES |
|---|---|---|---|---|---|
| Proposed Year | 1975 | 1985 | 1990 | 1993 | 1997 |
| Proposed By | IBM | IBM | James L. Massey, Xuejia Lai | Bruce Schneier | Joan Daemen, Vincent Rijmen |
| Structure | Feistal Structure | Feistal Structure | Lai-Massey scheme. | Feistal Structure | Not Feistal structure |
| Way of processing plaintext | Block Cipher | Block Cipher | Block Cipher | Block Cipher | Block Cipher |
| Plaintext Block Length | 64 bits | 64 bits | 64 bits | 64 bits | 128 bits |
| Key Length | 56 bits | 168 or 112 bits | 128 bits | Variable key length from 32 to 448 bits | 128, 192 or 256 bits |
| Number of Rounds | 16 | 16*3 | 8 | 16 | 10 |
| Security Level | Low | Medium | High | 16 | High |

Sample data of with varying sizes is taken and test results with the symmetric algorithms are drafted as in figure 5 and 6. Figure 5 shows the system mean time and follows figure 6 that shows the speed-up ratio.

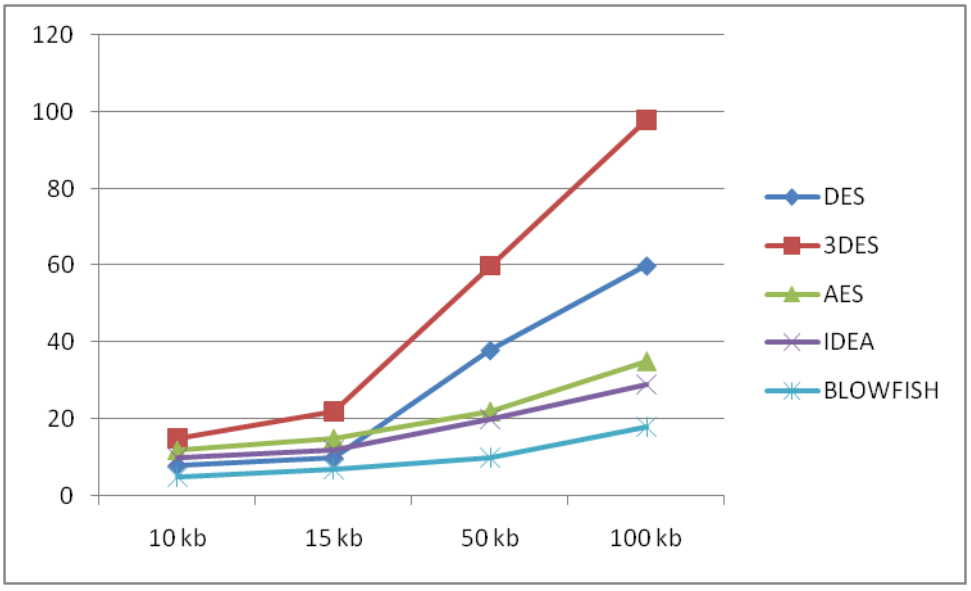


Fig. 5: Compare system mean time of symmetric algorithms with different inputs.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

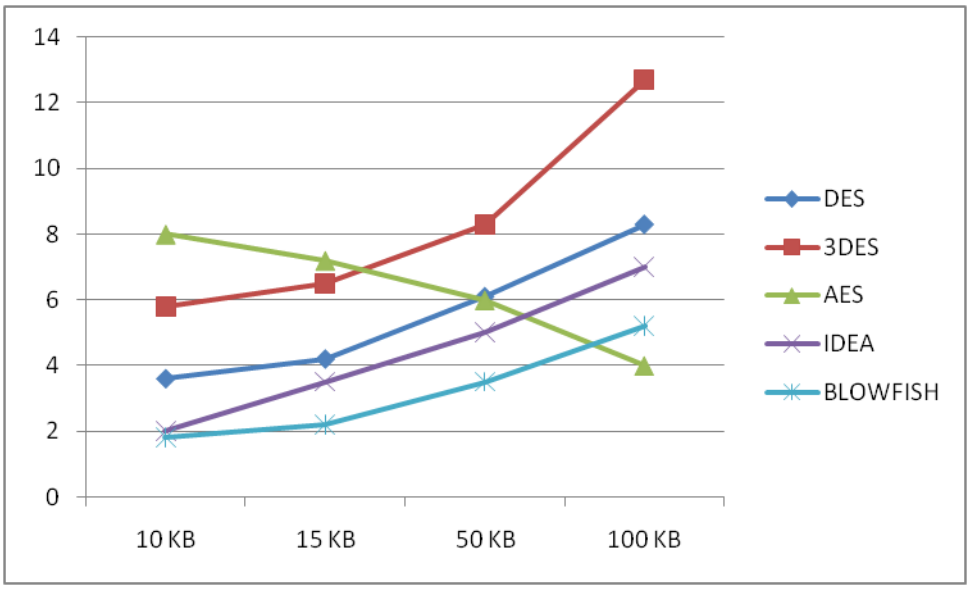


Fig. 6: Compare speed-up ratio of symmetric algorithms with different inputs.

### *3.2 Asymmetric Algorithms*

Similarly, the asymmetric algorithms are developed and tested on sample data. The most common features of asymmetric algorithms are as listed in table 2.

Table 2 : Salient Features of Renowned Asymmetric Algorithms

| Algorithm | DH | RSA | ElGamal | DSA | ECC |
|---|---|---|---|---|---|
| Proposed Year | 1976 | 1977 | 1985 | 1991 | 1985 |
| Proposed By | Whitfield Diffie, Martin E. Hellman | Ron Rivest, Adi Shamir, Leonard Adleman | Taher Elgamal | David Kravitz | Neal Koblitz, Victor Miller |
| Mathematical Construct used | modular exponentiation | modular exponentiation | modular exponentiation | Approved Hash Function | Elliptic Curve |
| Plaintext Block Length | - | Variable | Variable | - | Variable |
| Key Length | 512-2048 bits | 512-2048 bits (bit-length of RSA modulus n) | Variable | Length of parameter q in bits | Order of base point of elliptic curve; bit length of n |
| Usage | Key Exchange | Encryption & Signature | Encryption & Signature | Digital Signature | Encryption & Signature |

However as shown in table 2 the purpose of PKC algorithm varies, but the common factor is key generation. Secure key size of the specified PKC algorithms are as listed in table 3.

Table 3: Application based Secure Key size for Renowed PKC Algorithms

| Algorithm | Simple Applications | Moderate Applications | Highly Secured Applications | Near Future Applications |
|---|---|---|---|---|
| DH | 768 | 2048 | 3072 | 15424 |
| RSA | 768 | 2048 | 3072 | 15424 |
| ElGamal | 768 | 2048 | 3072 | 15424 |
| DSA | 768 | 2048 | 3072 | 15424 |
| ECC | 128 | 224 | 256 | 512 |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

The analysis of asymmetric algorithms on different applications basing on key size is shown in figure 7.

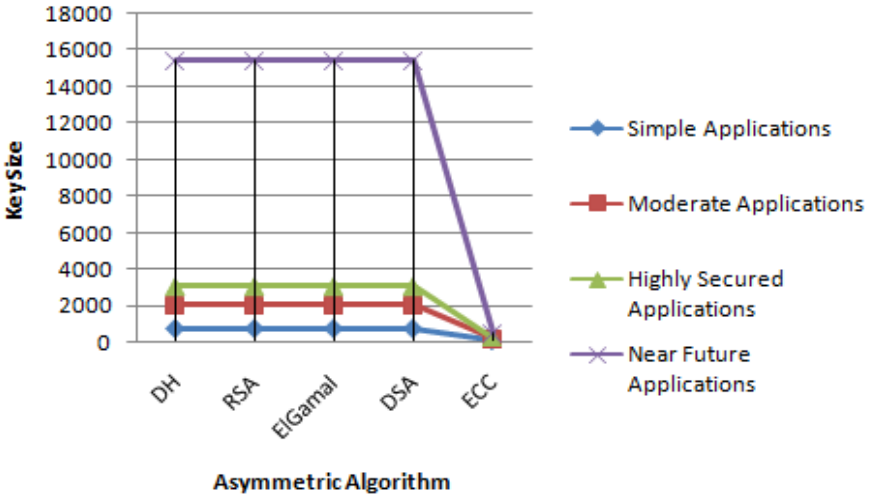


Fig. 7: Analysis of Asymmetric algorithms on different applications

The analysis shows that elliptic curve cryptography uses low key size comparative to all other comparable public key cryptographic algorithms. This is liable to any kind of application starting from simple to Highly Secured applications.

## 4. CONCLUSION

This paper presents the review of all the renowned Symmetric and Asymmetric Information Security Algorithms which are popular from past four decades. Symmetric algorithms are easy to develop and can be used by simple applications; however the key has to be shared secretly. Asymmetric algorithms overcome this problem by keeping the secret key with sender and sharing the secret key. The comparative analysis is given comparing all the specified algorithms and results specify that Elliptic Curve Cryptography is preferable in usage as this requires less key size though it involves complexity in mathematics compared to its neighboring algorithms.

## REFERENCES

[1] Text Book: "Cryptography and network security, Principles and practices", by William Stalling, Retrieved on 8 December 2006

[2] Text Book: "Network Security Essentials, Applications and Standards", Third Edition, by William Stalling, 2011

[3] Smid, M.E. , Branstad, D.K., "Data Encryption Standard: past and future", Proceedings of the IEEE, Vol 76 , Issue: 5, pp 550 – 559, May 1988.

[4] Davis R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, Vol 16 , Issue: 6, pp: 5 – 9, November 1978.

[5] Seung-Jo Han, Heang-Soo Oh ; Jongan Park, "The improved data encryption standard (DES) algorithm", Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium , Vol 3, Sep 1996, pp 1310 – 1314.

[6] Coppersmith, D. , Johnson, D.B. ; Matyas, S.M. "A proposed mode for triple-DES encryption", Vol 40, Issue: 2, pp 253 – 262, , March 1996, IEEE.

[7] K. Sujatha, P. V. Nageswara Rao, A. Arjuna Rao, L. V. Rajesh, V. Vivek Raja; "Secured Internet Voting System based on Combined DSA and Multiple DES Algorithms", ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II Advances in Intelligent Systems and Computing Volume 249, 2014, pp 643-650.

[8] Xuejia Lai,, James L. Massey, "A Proposal for a New Block Encryption Standard", LNCS, Advances in Cryptology - EUROCRYPT '90, pp 389-404

[9] Yong Qin, Oh, J.C. ; Kim, B., "CMOS implementation of the IDEA encryption algorithm", Circuits and Systems, 2000. Proceedings of the 43rd IEEE Midwest Symposium, Vol 1, 2000, pp 272-275, IEEE

[10] Bruce Schneier, "The Blowfish encryption algorithm", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994

[11] Tingyuan Nie, Teng Zhang, "A study of DES and Blowfish encryption algorithm", TENCON 2009 - 2009 IEEE Region 10 Conference, Jan. 2009, pp 1 – 4, IEEE

[12] Alabaichi, A. , Ahmad, F. ; Mahmod, R, "Security analysis of blowfish algorithm", Informatics and Applications (ICIA),2013 Second International Conference, Sept. 2013, pp 12 – 18, IEEE

[13] Meyers, R.K, Desoky, A.H., "An Implementation of the Blowfish Cryptosystem ", Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium , Dec. 2008, pp 346 – 351, IEEE

[14] Mousa, A. , "Data encryption performance based on Blowfish", ELMAR, 2005. 47th International Symposium, June 2005, pp 131 – 134, IEEE

[15] Xinmiao Zhang ; Parhi, K.K., "Implementation approaches for the Advanced Encryption Standard algorithm", Circuits and Systems Magazine, IEEE , Vol 2,Issue: 4 , pp 24 – 46

[16] Moh'd, A., Jararweh, Y. ; Tawalbeh, L., "AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation", Information Assurance and Security (IAS), 2011 7th International Conference, Dec. 2011, pp 292 – 297

[17] Alghazzawi, D.M. , Hasan, S.H. ;Trigui, M.S., "Advanced Encryption Standard - Cryptanalysis research", Computing for Sustainable Global Development (INDIACom), 2014 International Conference, March 2014, pp 660 - 667

[18] Whitfield Diffie and Martin E Hellman, "New Directions in Cryptography", Information Theory, IEEE Transactions, Vol:22, Issue: 6, Nov 1976, pp 644 – 654.

[19] RFC2631, "Diffie-Hellman Key Agreement Method", Network Working Group, E. Rescorla, Standards Track, June 1999

[20] Nan Li, "Research on Diffie-Hellman key exchange protocol", Computer Engineering and Technology (ICCET), 2010 2nd International Conference on (Volume:4 ), 16-18 April 2010, pp: V4-634 - V4-637.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

[21] Bhattacharya, P. , Debbabi, M. ; Otrok, H. "Improving the Diffie-Hellman secure key exchange", Wireless Networks, Communications and Mobile Computing, 2005 International Conference on (Volume:1 ), June 2005, pp: 193 – 197,vol.1, IEEE

[22] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM CACM Homepage archive, Vol 21, Issue 2, Feb. 1978, pp 120-126, ACM.

[23] Xin Zhou, Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption", Strategic Technology (IFOST), 2011 6th International Forum, Vol 2, Aug. 2011, pp 1118 – 1121, IEEE.

[24] Chhabra, A, Mathur, S., "Modified RSA Algorithm: A Secure Approach", Computational Intelligence and Communication Networks (CICN), 2011 International Conference, 7-9 Oct. 2011, pp Page(s): 545 – 548, IEEE

[25] Elgamal, T. , "A public key cryptosystem and a signature scheme based on discrete logarithms", Information Theory, IEEE Transactions , Jul 1985, Vol 31, Issue: 4 , pp 469 – 472, IEEE.

[26] Taher El Gamal. "A public key cryptosystem and a signature scheme based on discrete logarithms", in Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc., 1985.

[27] Fu Minfeng,Chen Wei, "Elliptic curve cryptosystem ElGamal encryption and transmission scheme", Computer Application and System Modeling (ICCASM), 2010 International Conference on (Volume:6 ), Oct. 2010, pp : V6-51 - V6-53, IEEE

[28] CORPORATE NISTGaithersburg, MD, "The digital signature standard", Communications of the ACM, Vol 35, Issue 7, July 1992, Pages 36-40, ACM

[29] "Digital Signature Standard", NIST, U. S. Department of Commerce, FIPS PUB 186, May 1994.

[30] Ronald L. Rivest, "On NIST's Proposed Digital Signature Standard", ASIACRYPT '91, Proceedings of the International Conference on the Theory and Applications of Cryptology: Advances in Cryptology, pp 481-484, Lecture Notes in Computer Science, Springer-Verlag

[31] Kitsos P, Sklavos N., Koufopavlou O.," An efficient implementation of the digital signature algorithm", Electronics, Circuits and Systems, 2002. 9th International Conference, Vol 3, 2002 , pp 1151 – 1154, IEEE

[32] Gilani J, Mir A.A.,"Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques", Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. SNPD '09. 10th ACIS International Conference, 27-29 May 2009, pp 399 – 404, IEEE.

[33] Neal Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol 48. Number 177, Jan I987. pp 203-209

[34] Victor S. Miller, "Use of Elliptic Curves in Cryptography", LNCS, Advances in Cryptology — CRYPTO '85 Proceeding, Sec V, pp 417-426, 1986, Springer Berlin Heidelberg

[35] Amara M, Siad A., "Elliptic Curve Cryptography and its applications", Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop, May 2011, pp 247 – 250, IEEE

Qizhi Qiu, QianXing Xiong, "Research on elliptic curve cryptography", Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on (Volume:2 ), May 2004, pp 698 - 701 Vol.2, IEEE

[36] Qiuxia Zhang, Zhan Li ; Chao Song, "The Improvement of digital signature algorithm based on elliptic curve cryptography", Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference, Aug. 2011, pp 1689 – 1691, IEEE