**Comparative Study of Cryptography algorithms and Its Applications**

**Abstract**:

In modern world, security is the most valuable term in the field of communication system. Security comes along with many technologies and methods, where one of the most secure one is Cryptography where ordinary plain text is converted into cipher text for transferring data to the valid user. Cryptography algorithms can be divided into two types based on the number of keys such as Symmetric and Asymmetric where Symmetric algorithm works with one single key and Asymmetric algorithm works with two different keys. However, selecting the appropriate algorithms for specific application has been always a challenging task because of the latency, key size, and security issues. Cryptographic algorithms faces different type of attacks like brute force attack, man in the middle attack and cycle attacks which are still remained as threads. This paper presents the performance analysis of different techniques of symmetric and asymmetric algorithms based on different performance metrics which will help to identify the suitable algorithms for different types of applications with considering the network threads.

**Keywords**: Encryption, Algorithms, Symmetric, Asymmetric, Applications

1. **Introduction**:

Cryptography is a process of translating the original plain text in to cipher text. The sender translates the plaintext in to cipher text. In this way when the data sends to receiver the sender translate the plaintext into chipper text. Then the receiver converts it to plaintext for reading data. The passion of the cryptography is to protect data from unauthorized access. When the data sends to receiver as chipper text, then third party can’t access the data as the original form. The way that the plaintext hides the data is called encryption. The way of the encrypting the input or plaintext which is unreadable is called chipper text. The way that takes encrypting message to the receiver and translates as readable form is called decryption.

In Symmetric, it’s uses only one key to send data from sender to receiver. It uses private key and secret key number which can be number, word and also string. The sender and the receiver share a single common key in order to use the technique. There are two common patterns in symmetric cryptosystem. These are stream cipher and block cipher. The stream cipher generates a sequence of bits used as a key called a key stream and the encryption is accomplished by combining the key stream with the plaintext. This process is usually completed with bitwise XOR operation. The key stream is not dependent on the plaintext and cipher text, in which case the stream cipher is synchronous. Otherwise it can depend on the data and its encryption, in which case the stream cipher is self-synchronizing. Block cipher converts a fixed-length block of plaintext into a block of cipher text which is same length. In decryption, same secret key is used by applying the reverse transformation of the cipher text block and original plain text is produced [2].

In Asymmetric method two keys are used, one to encrypt the data and another one to decrypt the data. These keys are generated together. One is named as Public key and is distributed freely. The other one is named as private key and it is kept hidden. Both the sender and recipient has to share their public key for encryption and has to use their private keys for decryption. The public key is distributed freely between the sender and receiver whether private key is only used [12].

On a paper [3] some of selected algorithm such as DES, 3DES, AES, Blowfish (Symmetric) and RSA and Diffie Hellmen (Asymmetric) are analyzed based on high key length where they found that DES works better.

In [4] performance analysis has been done based on security and challenge issues of different symmetric algorithms, such as - AES, DES, Blowfish and RSA algorithm in terms of using them in cloud computing was discussed.

In a paper [1] compared both symmetric (DES, 3DES, AES, Blowfish) and asymmetric (RSA, Diffe-Hellman, ECC) key algorithms based of advantages and disadvantages along with the importance of both types.

From the above literature study, it has been found that the performance of the symmetric or asymmetric algorithms varies greatly depending on different parameters, such as security threads, latency, key size.

In this paper we have focused on the performance analysis of the different algorithms for both symmetric and asymmetric cryptography based on their applications and security threads alongside with other parameters. This will enable the researchers or other network security service providers to select the appropriate algorithms for their system.

The paper presents the research works in according to the following sections, 2 Related Works where various research papers are provide on this topic then in 3.Symmetric Cryptographic Algorithms and 4.Asymmetric Cryptographic Algorithms where different techniques of this type are discussed. After that we provide 5.Result and Comparison of these algorithms and finally in 6.Discussion and 7.Conclusion presented based on the performance result.

1. **Symmetric** **Cryptography** **Algorithm**:

In this section various type of symmetric algorithms are individually discussed in terms of their working procedure, advantages and disadvantages.

* 1. **AES** **Algorithm:**

AES (Advanced Encryption Standard) was first presented by Rijndael in Oct-2000. It was Designed by Vincent Rijmen and Joan Daemen in Belgium. AES is a symmetric block cipher .it can Block size128bit, Cipher keys 128,192and 256 bits. Essentially, encryption calculations are separated into three noteworthy classifications; transposition, substitution, and transposition; substitution procedure. This calculation utilizes a round function that is thought about of four distinctive byte-arranged changes, for example, Sub byte, Shift row, Mix column, Add round key. Number of rounds to be utilized relies upon the length of key [3].

These numbers of rounds, AES compare between its own three block ciphers: AES-128, AES-192 and AES- 256. Each of this type both encrypts and decrypts data in block of 128 bits in measures of cryptographic keys. In this method of cryptography there is no extra room for acceptance additional block sizes and key length. The AES encryption algorithm performs in different stage of transformation. At first the cipher use the data to put into an array and after that it performs a number of encryption rounds. This round is based on key length such as 10 rounds for 128 bits, 12 rounds for 192 bit and 14 rounds for 265 bit keys. Then when this transformation is over creating a table of substitution with the data performs the second transformation with shifting the data in rows and then mixes columns. Finally there is an exclusive or XOR operation at the different part of the keys.

As AES implemented in system as robust security protocol, the higher length of keys such as 128, 192 and 256 bits are encrypted in this method easily. The main uses of AES come with applications of wireless communication, financial transaction and e-commerce business. While the limitation of AES based on simplified algebraic architecture and as every block is encrypted .

* 1. **BLOWFISH Algorithm**:

Blowfish is a keyed 64-bit block cipher with variable length .it was discovered in 1993 by Bruce Schneier [19][20[21]. Blowfish has a variable key length from 32 up to 448 bits. This calculation is a 16 round Fiestel figure and it utilizes a huge key ward S-boxes[20]. Blowfish requires around 5KB of memory. Blowfish as a rule utilizes a one of a kind type of key generation [22]. The second part of the Blowfish routine is a key expansion which converts a single key of up to 448 bits into a table of sub-keys that is 4168 bytes in size[22]. The creation of sub-keys increases security. Blowfish can make longer key with the goal that it's so hard to endeavor to hack the key.

The algorithm comprises of two sections: a key-expansion part and data encryption part[23]. Key expansion changes over a key of at most 448 bits into a few sub-key clusters totaling 4168 bytes. Data encryption happens commonly by means of a 16-round arrangement. Each round consists of a key-dependent permutation, and a key- and data dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round[23].

Blowfish is uninhibitedly utilized. After the key timetable has finished, Blowfish is a moderately quick block cipher, because of the modest number of rounds (sixteen) and the straightforwardness of the round[24].

Blowfish algorithm can't give confirmation and non-denial as two individuals have same key. The key timetable in Blowfish is somewhat tedious. The small block size of Blowfish (64 bits) is more helpless against the attacks than the 128 bits utilized by AES[24].

**2.3. DES Algorithm:**

Des (Data Encryption Standard) was developed in 1970 at IBM by Horst Feistel. This encryption standard was recommended by National Institute of Standards Technology [5].

DES deals with the input that is 64 bits of plain text where it constructs cipher text. The cipher text is 64 bits. Regardless of whether 64 bit key is the genuine input, the key length is 56 for this calculation. DES comprises of a16-round arrangement of substitution and permutation. Accordingly, data and key bits are shifted, permutated, XORed, and sent through 8 boxes. An arrangement of lookup tables are basic to the DES algorithm. The Decryption process is performed in reverse. This makes it a symmetric key algorithm [4]

The DES algorithm’s encryption and decryption speed is fast in terms of other symmetric algorithms. One of the important advantages is with having used DES; swifter public-key techniques can be made. DES uses the least memory while encryption time [6]. On the other hand, DES is considered weak and insecure because it was recorded with many attacks as the key length is 56 which are too small [5]. The application of DES is popular encryption technique where this processes images like JPEG format and Bitmap image.

**2.4. 3DES Algorithm:**

3DES or the Triple Data Encryption Algorithm was produced to address the conspicuous defects in DES without de-marking a radical new cryptosystem [7]. With the possibility that Double DES may not be sufficiently solid to keep a compromise assault has prompted the advancement of 3DES, which was produced in 1999 by IBM by a group drove by Walter Tuchman [8]. This kind of attack is one of the primary reasons why 2DES was supplanted by 3DES.

3DES works similarly as DES, with the exception of that experiences three cycles amid the encryption procedure, utilizing three keys: encryption, unscrambling, and another encryption. It has a key length of 192 bits (64 bits x 3 keys), however its genuine quality is 168 bits (56 bits x 3 keys).3 DES is three times as solid as DES, yet it additionally implies that it is three times slower in light of the triple preparing [9]. One thing is critical that every one of the three keys must be extraordinary. On the off chance that any of the keys are observed to be same, it will be less demanding for a programmer or hacker to find the plaintext. Therefore, a few methods of activity were planned by researchers for symmetric block cipher, for example, 3DES.

3DES cipher experiences a crucial shortcoming connected to its little (64-bit) block size. Additionally there is currently a reasonable, moderately quick attack on 64-bit block cipher that gives aggressors a chance to recoup validation treats and different qualifications from HTTPS-secured sessions[11]. Along with this still 3DES use in password protection of user content and system data.

1. **Asymmetric** **Cryptography** **Algorithms**:

In this section various type of asymmetric algorithms are individually discussed in terms of their working procedure, advantages and disadvantages.

* 1. **RSA Algorithm:**

In 1978 RSA was composed by Ron Rivest, Adi Shamir, and Leonard Adleman .It is the most well-known public key algorithm. It's a standout amongst other known open key cryptosystems [13].

RSA is an asymmetric cryptosystem. There are two diverse keys. RSA is most widely known as public key cryptosystem, since one of them is shared with everybody. The other key is private since its kept secret. RSA is based on mathematical fact. RSA works in three steps:

1. Key Generation: Data is encrypted after Key generation is done.

Steps:

1. Pick two particular expansive irregular prime numbers c and d with the end goal that c ≠d

2. Register z= c × d.

3. Figure: ∅ (z) = (c-1) (d-1).

4. Pick a whole number e with the end goal that 1<e< ∅ (z)

5. Register g to fulfill the consistency connection g × e = 1 mod phi (z); g is kept as private key example.

6. The public key is (z, e) and the private key is (z, g). Keeping every one of the qualities g, c, d and ∅.

1. Encryption: Encryption is the process of converting original plain text into cipher text.

Steps:

Plaintext: J< n

Cipher text: K= Je mod n.

1. Decryption: Decryption is the way toward changing over the cipher text to the first plain text content.

Steps:

Cipher text: A

Plaintext: B=Ad mod n [13] [14].

The RSA is considered reliable and safe for its secrecy and privacy features. RSA also offers integrity where the content stays in its original form in exchange phase. Disadvantages of RSA is that it takes longest encryption time.it requires of similar lengths for c and which is not easy to meet the requirement .Padding techniques are required in this case which leads to more processing time [14]. RSA is used mostly in hybrid encryption schemes and digital signatures and also in web browsers, chat applications, email, VPNs and some other kinds of interchanges that require safely sending information to servers or individuals.

* 1. **DSA Algorithm:**

A digital signature algorithm (DSA) alludes to a standard for digital signatures [15]. It was presented in 1991,by the National Institute of Standards and Technology (NIST) as a superior technique for making digital signatures. DSA does not encode message digests utilizing private key or decode message digests utilizing public key. Rather, it utilizes extraordinary scientific capacities to make a digital signature comprising of two 160-bit numbers [15].

DSA Signature Generation:

INPUT**:** Domain parameters (a, b, c); signer's private key e; message-to-be-signed, S, with message digest d= Hash(S) [16].   
OUTPUT**:** Signature (x, y).

1. At first we’ll have to choose a random i in the range [1, b − 1].
2. Then K = ci mod a and x= K mod b. If x = 0 (unlikely) then we’ll need to go step 1.
3. Next step we’ll have to compute i− 1 mod b.
4. Then we’ll have to compute d= Hash(S).
5. Then we’ll have to compute y = i− 1(d + sx) mod b. If y = 0 (unlikely) then we’ll have to go step 1.
6. Finally it’ll return (x, y) [16].

DSA Signature Verification:

INPUT**:** Domain parameters (a, b, c); signer's public key E; signed-message, S, with message digest d= Hash(S); signature (x, y) [16]. OUTPUT**:** Either "Accept" or "Reject".

1. At first we’ll have to verify that x and y are in the range [1, b − 1]. If not then we’ll have to return "Reject" and stop.
2. Then we’ll have to compute p= y− 1 mod b.
3. Next step we’ll need to compute n= Hash(S).
4. In step 4 we’ll have to compute z1 = dp mod b and z2 = xn mod b.
5. Next step we’ll have to compute Y = cz1Sz2 mod a and v = Y mod b.
6. If v = x then we’ll have to return "Accept" otherwise we’ll have to return "Reject"[16].

In DSA If the digital signature isn't checked by the general public key, at that point the recipient should just stamp the message as invalid however he doesn't know whether the message was adulterated or the false private key was utilized [17]. Additionally, in a few states and nations, laws with respect to digital and innovation based issues are frail or even non-existent. In spite of the fact, digital signature gives validness yet it doesn't guarantee secrecy. Keeping in mind the end goal to give the mystery, some other method, for example, encryption and unscrambling should be utilized. DSA used in web application where user data and content transfer during email.

**3.3 ECC Algorithm:**

Elliptic curve cryptography was presented in the mid-1980s,by Koblitz and Miller as a promising option for cryptographic conventions in light of the discrete logarithm issue in the multiplicative gathering of a limited field [18].

ECC is same as RSA but different is that it has fast solving capacity and has different way of cryptographic algorithm. The ECC’s security key length is smaller than other asymmetric algorithms and its key length is only 163 bit. ECC takes full-exponential time and RSA takes sub-exponential time. For a case, RSA with key size of m, 1024 piece takes 4\*10m MIPS years with best known assault ECC with 160 piece key size takes 12.6\*10m MIPS .It uses elective curve equation in lieu of traditional prime numbers. Most of the execution time spends on scalar multiplication. ECC provides same security as other algorithms but in smaller key sizes.

The whole security of ECC rely upon the capacity to figure a direct increase and powerlessness toward process the multiplicand given the first and item point[18]. The ECC provides decent authentication in RFID system. For small key size it can use in wireless sensor networks like tablet, mobile phones.

Most significant privilege is that ECC provides good security with small key size which provides faster computational capabilities. On the other hand, it expands the extent of the encrypted message essentially more than RSA encryption. This algorithm is more confounded and hard to actualize than RSA, which improves the probability of usage blunders, subsequently lessening the security of the algorithm. ECC is utilized as a part of key trade for internet browser use additionally in a portable setting, including mobile phones and the Internet of Things.

1. **Results Analysis :**

The performance result analysis of different symmetric and asymmetric algorithms is done based on various performance metrics. These metrics decide which algorithm performs better than others. The following performance metrics are analyzed-

* **Key** **length:** Keylength is the number of bits in a key used by a cryptographic algorithm which determined the time complexity of transferring the data to the sender and receiver ends.
* **Block Size:** A block is an arrangement of bytes or bits, typically containing some entire number of records, having a greatest length, a block size. data in this way organized are considered to be blocked.
* **Round:** Roundis afunction, which measures how much time the operation needs to perform for retrieve data.
* **Vulnerabilities:** Weakness points of a system which can be exploited by attacker.
* **Efficiency:** Determines how fast or slow it behaves when implemented in hardware and software.
* **Applications:** Performance area of algorithm with specific function directly for the user or, in some cases, for another application program. Identify the best protocol for different applications in computer networking system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Performance Metrics | AES | BLOWFISH | DES | 3DES |
| Key-Length (bits) | 128,192,256 | 32-448 | 56 | 112,168 |
| Developed | 2000 | 1993 | 1975 | 1978 |
| Block Size | 128 | 64 | 64 | 64 |
| Security | Mostly Secure | Unpatented and royalty-free | Not Good Enough | Adequate security |
| Possible thread | Side channel attack | Brute force attack | Brute force attack, man in the middle attack | Some channel attacks |
| Rounds | 10,12,14 | 16 | 16 | 48 |
| Efficiency | Fast | Fast | Slow | Fast for hardware but Slow in software |
| Applications | Wireless communication | JFile, Foopchat | Image processing | Smart Card, e-payment |

TABLE 1: Performance Analysis of Symmetric Cryptography Algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| Performance Metrics | RSA | DSA | ECC |
| Key-Length (bits) | 1024-2048 | 2048-3072 | 160 |
| Developed | 1977 | 1991 | 1980 |
| Block Size | 192 | Variable | 80 |
| Security | Medium high level of security | Mostly Secure | Mostly Secure |
| Possible thread | Cycle Attacks, Sharing of common modules | Set of parameters can be generated for pre-chosen message | Curve generation attacks, zero-value point attack |
| Rounds | 1 | 16 | 1 |
| Efficiency | Slow in hardware specially when decryption | Slow for both software and hardware | Slow for both software and hardware |
| Applications | Internet Banking | Web application and email verification | Key exchange over web and mobile. |

TABLE 2: Performance Analysis of Asymmetric Cryptography Algorithms

1. **Discussion:**

From table 1 we can see that AES algorithm is better for wireless communication in terms of performance metrics like key lengths block size and rounds which increases time complexity. As a result it’s difficult to crack the system. JFile is a famous application that use blowfish algorithm. It is a flat-file database application for the PalmOS . Foopchat is a encrypted chat and advanced file sharing system using a client/server architecture .Blowfish is suitable for this two application because the key does not change frequently like a communication link or an automatic file encryptor. It is faster than most encryption algorithm when on 32-bit microprocessor with large data caches. For Image processing system DES is better, as it has small key and block size which will enable high transmission rate with moderate security during image transmission. For smart card (integrated circuit card) or e-payment purpose 3DES algorithm can be used although it’s performance is slow in terms of software because of triple phases of DES but it is very cheap for hardware implementation.

The result analysis for RSA in table 2 explains that this algorithm can be used for mobile banking system. RSA has higher key length , block size and slower efficiency which increases time complexity. Besides RSA provides a secure transmission over transmission channel which provides the system a good security. While DSA can be used in web application and email verification based on performance metrics. Since it has a larger number of key lengths and block size depends on variable along with measurement, higher security and efficiency which makes the system much secure. ECC works better in key exchange over web, mobile. ECC’s efficiency is lower terms of all performance metrics except numbers of round. Because of small key sizes it performs faster than remaining both.

1. **Conclusion:**

In this paper a comprehensive study is done based on the performance of different cryptographic algorithms to determine the possible applied field. The performance analysis is done based on different parameters, for example- Key-Length, Block Size, Security, Possible thread, Rounds, Efficiency. Although Symmetric and Asymmetric algorithms both are highly efficient for protecting the data in their own relevant field of data transferring but based on the result analysis and discussion we can conclude that symmetric cryptography algorithms such as – AES,BLOWFISH, DES, 3DES are more suitable for the applications like wireless communication, JFile ,image processing, smart card or e-commerce type of serveries respectively. On the other hand side, asymmetric cryptography algorithms such as – RSA, DSA, ECC are the best options for the applications like Internet banking, web application, email verification, key exchange over web, mobile. This work can be extended in the future by evaluating more cryptographic techniques and schemes to identify their possible field of application.

**Reference**:

[1] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Dr.(Prof.) Goutam Sanyal “A comparative survey of symmetric and asymmetric key cryptography”, IEEE 2nd International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014.

[2] RSA Laboratories- Chryptographic tools; section 2.1.5. unpublished;http://www.rsa.com/rsalabs/node.asp?id=2174.

[3] Ritu Tripathi, Sanjay Agrawal “Comparative Study of Symmetric and Asymmetric  
Cryptography Techniques” International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[4] Rachna Arora, Anshu Parashar, “Secure User Data in Cloud Computing Using EncryptionAlgorithms”, International Journal of Engineering Research andApplications **(**IJERA**)** , Vol**.** 3,Issue4**,** Jul**-**Aug2013**,** pp**.**1922**-**1926.

[5] Yogesh Kumar, Rajiv Munjal, Harsh Sharma,” Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[6] Yvo Desmedt, Jean-Jacques Quisquater, “Public-Key Systems Based on the Difficulty of Tampering (Is there a difference between DES and RSA)”.

[7] “3DES”, http://www.cryptosys.net/3des.html

[8]T. Sobh, K. Elleithy and A. Mahmood, “Novel Algorithms and Techniques In Telecommunications”, Automation and Industrial Electronics. Springer Science Business Media B. V., Bridgeport. (n.d.).

[9] http://codenamekidnextdoor.blogspot.com/2011/09/explaining-triple-data-encryption.html

[10] https://www.quora.com/Cryptography-What-are-the-advantages-and-disadvantages-of-AES-over-Triple-DES

[11] https://www.infoworld.com/article/3112324/security/new-collision-attacks-against-triple-des-blowfish-break-https-sessions.html

[12] Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ŢĂPUŞ ; “An Overview of the Attack Methods Directed Against the RSA Algorithm”; Revista Informatica Economica, nr. 2(30)/2004

[13] Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and  
AES) for Information Security”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[14] Dr. Prerna Mahajan & Abhishek Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.

[15] <https://www.techopedia.com/definition/27504/digital-signature-algorithm-dsa>.

[16] <https://www.di-mgt.com.au/public-key-crypto-discrete-logs-4-dsa.html>

[17] https://lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/

[18] Rahat Afreen and S.C. Mehrotra, “A Review on Elliptic Curve Cryptography  
for Embedded Systems”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

[19] Schneier, B.: "Description of a New Variable-Length Key, 64-BitBlock Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings(Dec. 1993), Lecture Notes in Computer Science(LNCS) Springler verlag Vol. 809, pp. 191-204,1993, ISBN 3- 540-58108-1.

[20] https://ieeexplore.ieee.org/abstract/document/5942029/

[21] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop proceedings December 1993, Springer-Verlag, 1994, pp. 191-204 .

[22] https://study.com/academy/lesson/blowfish-encryption-strength-example.html

[23] https://ieeexplore.ieee.org/abstract/document/5396115/

[24] https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35