**A Performance Analysis of Cryptographic Algorithms**

**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, the security issues of using these algorithms faces attacks like brute force attack, man in the middle attack and cycle attacks which are still remained as threads. For overcoming these threads, Cryptographic algorithms have been modified by various researchers many times. In this paper we will present the performance analysis of different techniques of symmetric and asymmetric algorithms.

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

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 the modern era cryptography provides a crucial role in network security purpose. It is useful for good communication under its security system.

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. Both the sender and the receiver must know the same key in order to use the technique. There are two common patterns in this method stream cipher and Block cipher. The stream ciphers generate 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 is usually done with the bitwise XOR operation. The key stream is not dependent on the plaintext and cipher text, in which case the stream cipher is synchronous, or it can depend of the data and its encryption, in which case the stream cipher is self-synchronizing. A block cipher converts a fixed-length block of plaintext into a block of cipher text which is of the 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].

Asymmetric uses two keys where one is public and another is private. It’s requires two types of keys: one to encrypt the plaintext and one to decrypt the cipher text, and it doesn’t work without one or another. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to whoever he wants, and the other one is the private key and it is known only by the owner [12].

This 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.

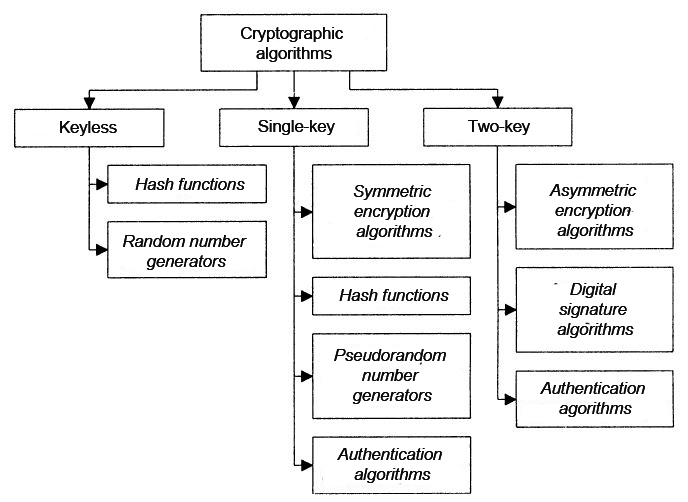


Figure 1: Classification of Cryptographic Algorithms

1. **Related Works:**

In this section, some selective research papers on cryptographic algorithm are provided. As this papers enlighten only a few algorithm types at a times but many researches is going on this topic to find out the best performing algorithm in their own field and improve the security data transferring.

On a paper [3] Ritu Tripathi & Sanjay Agrawal proposed some of selected algorithm such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen with high key length performance evaluation.

In another paper [4] Rachna Arora & Anshu Parashar proposed security and challenge issues of AES, DES, Blowfish and RSA algorithm in terms of using them in cloud computing.

In a paper [1] Sourabh Chandra et al proposed both symmetric and asymmetric key algorithms are highly efficient in secure in data transferring with providing data and comparable tables.

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

In this section various type of Symmetric algorithms are individually discussed in terms of their working procedure, uses in various data transferring techniques, advantages and limitations. We present these following Symmetric algorithms here,

* AES
* DES
* 3DES

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

Rijndael was selected as the AES in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in  
Belgium. AES is a symmetric block cipher that can Block size128bit, Cipher keys 128,192and 256 bits. Basically, encryption algorithms are divided into three major categories – transposition,  
substitution, and transposition – substitution technique. This algorithm uses a round function that  
is compared of four different byte-oriented transformations such as Sub byte, Shift row, Mix column, Add round key. Number of rounds to be used depends on 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 in the same way all the time.

* 1. **DES Algorithm:**

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

DES is a block cipher.in DES 64 bits of plain text goes as input, which produces 64 bits of cipher text. Even if 64 bit key is actual input, the key length is 56 for this algorithm. DES consists of a16-round series of substitution and permutation. Thus, data and key bits are shifted, permutated, XORed, and sent through 8 boxes, a set of lookup tables that are essential 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 .One of the important advantage is with having used DES, much faster public-key systems 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 is too small [5].

* 1. **3DES Algorithm:**

3DES or the Triple Data Encryption Algorithm was developed to address the obvious flaws in DES without de-signing a whole new cryptosystem [7]. With the idea that Double DES may not be strong enough to prevent a meet-in-the-middle attack has led to the development of 3DES, which was developed in 1999 by IBM by a team led by Walter Tuchman [8]. This type of attack is one of the main reasons why 2DES was replaced by 3DES. It is essential to avoid having the same key for the encryption steps since the output will only be a slower version of DES. 3DES has two forms, one requiring three completely different keys and the other only two completely different keys. Researchers used 56-bit key in data Encryption Standard (DES) and this was not sufficient to encrypt sensitive data. 3-DES was invented to simply extend the key size of DES by applying the algorithm three times in succession with three different keys and the combined key size is 168 bits (3 times 56).3DES involves using three 64-bit DEA keys (K1, K2, K3). In Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3[7].

3DES works in much the same way as DES, except that goes through three cycles during the encryption process, using three keys: encryption, decryption, and another encryption. It has a key length of 192 bits (64 bits x 3 keys), but its actual strength is 168 bits (56 bits x 3 keys). This method is three times as strong as DES, yet it also means that it is three times slower because of the triple processing [9]. One thing is very important that all three keys must be different. If any of the keys are found to be same, it will be easier for a hacker to discover the plaintext. For this reason, several modes of operation were designed by researchers for symmetric block ciphers such as 3DES.

Encryption using 3DES can be represented as:

A = B (C3, D (C2, E (C1, K))).

Similarly, decryption is the same process backwards:

X= K (C1, E (C2, D (C3, B))).

3DES is easy to implement and accelerate in both software and hardware. This is ubiquitous: most systems, libraries, and protocols include support for it [10]. Researchers believe that3DES is still being secure because it requires 2112 operations which are not achievable with foreseeable technology.

Researchers found that 3DES cipher suffers from a fundamental weakness linked to its small (64-bit) block size, i.e. the size of plaintext that it can encrypt. In the common mode of operation (CBC), each plaintext block is XORed with the previous cipher text before encryption. That means if we encrypt a lot of data and by chance get the same cipher text block twice, an attacker can learn the XOR of the two corresponding blocks of plaintext. Also there is now a practical, relatively fast attack on 64-bit block ciphers that lets attackers recover authentication cookies and other credentials from HTTPS-protected sessions, a pair of French researchers said. Legacy ciphers Triple-DES and Blowfish need to go the way of the broken RC4 cipher: Deprecated and disabled everywhere [11].

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

In this section various type of Asymmetric algorithms are individually discussed in terms of their working procedure, uses in various data transferring techniques, advantages and limitations. We present these following Asymmetric algorithms here,

* RSA
* DSA
* ECC
  1. **RSA Algorithm:**

In 1978 RSA was designed by Ron Rivest, Adi Shamir, and Leonard Adleman .It is the most common public key algorithm. It’s one of the best known public key cryptosystems [13].

RSA is an asymmetric cryptosystem. There are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key is private because its kept secret.it is based on number theory and is a block cipher system. RSA works in three steps:

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

Steps:

1. Choose two distinct large random prime numbers c & d such that c ≠d

2. Compute z= c × d.

3. Calculate: (z) = (c-1) (d-1).

4. Choose an integer e such that 1<e< (z)

5. Compute g to satisfy the congruence relation g × e = 1 mod phi (z); g is kept as private key exponent.

6. The public key is (z, e) and the private key is (z, g). Keeping all the values g, c, d and

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

Steps:

Plaintext: A< n

Cipher text: B= Ae mod n.

1. Decryption: Decryption is the process of converting the cipher text to the original plain text.

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]

* 1. **DSA Algorithm:**

A digital signature algorithm (DSA) refers to a standard for digital signatures [15]. It was introduced in 1991 by the National Institute of Standards and Technology (NIST) as a better method of creating digital signatures. Along with RSA, DSA is also considered one of the most preferred digital signature algorithms used today [15]. DSA does not encrypt message digests using private key or decrypt message digests using public key. Instead, it uses unique mathematical functions to create a digital signature consisting of two 160-bit numbers, which are originated from the message digests and the private key. DSA makes use of the public key for authenticating the signature, but the authentication process is more complicated when compared with RSA. DSAs are exclusively used for digital signatures and make no provisions for encrypting data; it is typically not subject to import or export restrictions, which are often enforced on RSA [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 is not verified by the public key, then the receiver will have to simply mark the message as invalid but he does not know whether the message was corrupted or the false private key was used.  For using the digital signature the user will have to obtain both private and public key, the receiver has to obtain the digital signature certificate also. In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities [17]. Also, in some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents [17]. Though digital signature provides authenticity but it does not ensure secrecy of the data. In order to provide the secrecy, some other technique such as encryption and decryption needs to be used.

* 1. **ECC Algorithm:**

Elliptic curve cryptography was introduced in the mid-1980s independently by Koblitz and Miller as a promising alternative for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite 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 an example, RSA with key size of m, 1024 bit takes 4\*10m MIPS years with best known attack ECC with 160 bit key size takes 12.6\*10m MIPS years. 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 entire security of ECC depend on the ability to compute a point multiplication and inability to compute the multiplicand given the original and product 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 in small key sizes which done the process within short time. On the other hand, it increases the size of the encrypted message significantly more than RSA encryption. This algorithm is more complicated and difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm.

1. **Results Analysis and Comparison :**

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

* **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 a sequence of bytes or bits, usually containing some whole number of records, having a maximum length, a blocksize. Data thus structured are said 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:** After implemented how fast or slow it behaves through hardware and software.

|  |  |  |  |
| --- | --- | --- | --- |
| Performance Metrics | AES | DES | 3DES |
| Key-Length (bits) | 128,192,256 | 56 | 112,168 |
| Developed | 2000 | 1975 | 1978 |
| Block Size | 128 | 64 | 64 |
| Security | Mostly Secure | Not Good Enough | Data Passing in some aspects |
| Vulnerabilities | Side channel attack | Brute force attack, man in the middle attack | Some channel attacks |
| Rounds | 10,12,14 | 16 | 48 |
| Efficiency | Both software and hardware | Slow | Slow in software |

TABLE 1: Comparison between 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 | Data Passing in some aspects | Mostly Secure | Mostly Secure |
| Vulnerabilities | 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 | Both in software and hardware | Slow |

TABLE 2: Comparison between Asymmetric Cryptography Algorithms

1. **Discussion:**

From table 1, it can be seen that AES is the better solution to perform data transferring. Firstly, AES can works with large numbers of key length and block size. Secondly, it performs different type of round operations based on key length. Finally, this algorithm works efficient after implemented both software and hardware. Although AES is vulnerable in side channel attack but its performance in every metrics presents better results than DES and 3DES.

The result in table 2 explains that, ECC’s efficiency is slower in terms of all performance expect numbers of round operation where RSA and DSA have problems in other performance metrics. But ECC’s key lengths are not as large as RSA and DSA and because of these small key sizes it performs faster than remaining both. Security of ECC and DSA are mostly secure. But in terms of key-length ECC gets more priority than RSA and DSA. However, ECC is vulnerable in curve generation attacks and zero-value point attack. With this information from table 2 ECC stands better security solution for asymmetric while RSA and DSA can be implemented in their own relative field.

1. **Conclusion**:

Symmetric or Asymmetric both are highly efficient to protecting the data in their own relevant field of data transferring. In this paper, we have highlighted the basic working process and which one is better for separately both in symmetric and asymmetric. In Symmetric Cryptography, AES comes with better results of data processing and transferring. While Asymmetric Cryptography, DSA and RSA both stand their way to perform secure data processing and transferring based on client and server based. But ECC gets more flexibility as it can work with small key sizes and perform faster. Moreover, these algorithm techniques still not perfect as the secure data transferring become challenging. With this paper we provide a collective study of both these techniques in their best way of data transferring.

**Reference**:

[1] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Dr.(Prof.) Goutam Sanyal “A comparative survey of symmetric and asymmetric key cryptography”, 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.