COMPARATIVE ANALYSIS OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC TECHNIQUES

Shikha Gupta, Nishi Gupta, Satbir Jain NSIT, NewDelhi-110078
shikha.gpt1@gmail.com, nishigupta99gmail.com, jain_satbir@yahoo.com

Abstract. In today's scenario security is becoming the most challenging aspect due to increase in online transmission media including computers and network applications. To protect the data from modern cyber security attacks there is no alternative tool other than cryptography. Cryptography is one such technique that plays an vital role in protecting data by implementing various parameters counting from confidentiality, authentication, integrity, availability, accuracy and identification to maintain the security and privacy of user's data. So, Cryptography is a tool used to achieve security to the applications by converting the data into an unreadable form by using various encryption techniques. Researchers have developed and implemented numerous encryption algorithms based on symmetric and asymmetric techniques. This paper provides a comparison between some of the symmetric encryption and asymmetric encryption techniques by analyzingthevarious parameters like key exchange, effectiveness, flexibility,
security etc. to determine the efficiency of cryptosystem.

1. INTRODUCTION

Security is today's world is one of the key challenge during transmission of data through internet which includes the data that contains personal information of users that may be intercepted by the attackers during the transmission. There are many applications on internet that carries various personal information such as credit card numbers details, telephone numbers etc. So, the users may need private and secure communications to protect their personal information from attackers to maintain the confidentiality and integrity of data against unauthorized access and use. Hence, in order to provide secure communication over the public network, different cryptographic schemes are used.

1.1 CRYPTOGRAPHY

Cryptography plays a vital role in protecting information from attackers and converting it into a form undistinguishableby its attackers though stored in databases and transmitted online.

The main purpose of cryptography is to keep data secure form unauthorized users. It ensures that the plaintext being sent remains private and should received only by the intended receiver. The main goals of cryptography to protect the information could be defined as follows:

1.1.1**DataConfidentiality:**Data confidentiality is important to store the valuable data of users either in databases or in cloud. It ensures that nobody can read the information except the intended recipient.

1.1.2 **Sender Authentication** : Recipient is used to verify the identity if sender and validate whether the information is coming from authorized user ornot.

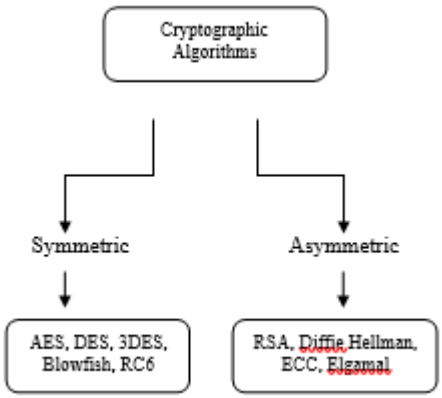
1.1.3 **Data integrity**: is one of the most critical elements in any information system. It ensures that the information received has not been deleted or modified by any unauthorizeduser.

1.1.4 **Sender Non-repudiation** : A process that proves that sender has really sent the message and should not be able to deny that the message was sent byhim.

1.1.5 **Access control :** In access control property only the authorized user can view the message that is sent. It can be done with the help of a key and decryption algorithm. Cryptography depends on two basic components: the first component is an algorithm also known as cipher and second component is a key. The algorithms are based on numerical procedure and key is an important component as whole security depends on it and it is used for data transformation. These algorithms provide security to data by using different encryption techniques to protect the data from unauthorized users. Encryption is a mathematical method used for promoting the security of data. It converts the input data into an unreadable form called cipher text and in decryption cipher text is converted back to its original input form called the plain text. Encryption techniques are further classified into symmetric encryption, asymmetric encryption also known as private key or public key algorithms and hash function. Symmetric encryption uses the same key both for encryption and decryption. It is also known by other names like single or

secret key encryption. The problem with symmetric algorithms is that user only shares a single or secret key in a secure way which causes difficulty in key exchanging [2]. AES, DES, 3DES, Blowfish, IDEA and RC6 are some commonly used symmetric encryption algorithms. Asymmetric algorithm is use to solve the problem of key distribution by usingapairofkeysi.e.publickeyanda

private key pair which are related to each other. Diffie-Hellman key exchange, RSA, ECC and Elgamal[5] are some of the asymmetric key based algorithms. Hash functions uses one way encryption and no key is used in these algorithms. It works on a plain text of fixed size to produce a hash value. Because of this content of theplaintext cannot be broughtback.



Classical Cryptographic Algorithms Fig-1

In Figure. 1 the basic classification of cryptographic algorithms is shown. Researchers have proposed and compared these algorithms on the basis of various parameters like time complexity and space complexity. This paper compares these algorithms on the basis of parameters like key length, flexibility, throughput, security, encryption speed andthe limitations of each algorithm. An algorithm is said to be effective if it provides a strong security level. This section analyzes symmetric and asymmetric encryption algorithms along with their security levels and also discusses the limitations of selected cryptographic algorithms. such as AES, DES, 3DES, Blowfish and RC6 are analyzed along with their merits and demerits.

2. BackgroundStudy

2.1 DES (Data Encryption Standard) DES stands for Data Encryption Standard. It is a symmetric key block cipher introduced by IBM in early 1970. It operates on 64 bit of blocks. DES has 16 rounds which means a total of 16 processing steps are being applied on the plaintext to produce desired ciphertext. It encrypts 64 bit size of input block by using a key of size 56 bits and results into an output block of 64-bit.. The structure of DES is based on Feistel cipher which divides the block into two halves and then applies 16 rounds of processing to encrypt the data [7]. The cipher works on 4 stages: Expansion, Key mixing, Substitution and Permutation. The major concern of DES is large amount of data availability and its short key length of 56 bit that makes DES an insecure block cipher. This drawback is not the end of the DES, an algorithm named 3DES is used as an enhancement of DES, it is the most trusted block cipherused today.

***2.2** Triple DES(3DES)*

3DES is an enhancement of DES that works on a 64-bit block cipher having a key size of 168 bits (56 * 3) and is much more complicated than DES in achieving high level of security. The encryption method used in it is similar to that of DES but applied 3 times using three different unrelated keys of 56 bit size to increase the encryption level and difficult to break by attackers. 3DES with three keys requires 2^168 possible combinations and for two keys it requires 2^112 possible combinations. The advantage of TDES is that it is a strongest encryption algorithm which gives its application in banking industry. On the other side this algorithm has a disadvantage that it is too time consuming and slower than other block cipher methods. It is vulnerable to certain variations of meet-in-the-middle attacks. It is also exposed to differential and related- key attacks[R4].

***2.3** AES (Advanced Encryption Standard)*

AES stands for Advanced Encryption Standard. It is a symmetric key block cipher introduced in 1997 by NIST. It is based on substitution and permutationmethod. It encrypts data block of 128-bit by using the key of size 128, 192, and 256 bits that makes it different from DES and 3DES [11]. It takes 10, 12 or 14 rounds to convert the plain text and its security is broken by chosen plain text attack. AES performs 9 rounds for 128 bit

block length and key length. For 192 bits, itperforms

11 processing rounds and for block and key of length 256 bits, it performs 13 processing rounds [6]. Each round performs four operation: Sub byte, Mix Column, Shift rows, Add round key. This algorithm is more secure, faster and flexible and implemented both in hardware and software [8]. Drawback of the algorithm is that it needs more processing and requires more rounds of communication when compared to DES[1].

2.4 *RC6*

RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits. RC6 is basedonFeistelStructurewhichuses128 bit block size and supports varying key size of 128, 192 or 256 bits with 20 rounds. RC6 is very much similar differs by the number of registers used (2 and 4 respectively) [2]. It is an evolutionary improvement of RC5 and is highly resistant to differential and cryptanalytic attack. It is a secure, compact simple block cipher whose code and data can readily fit in cache memory [2]. The brute-force attack appears to be infeasible if the key size large and the estimated round of 20 is recommended. RC6 is vulnerable to differential and brute force attack if the key size is small. Time consumption for process in RC6 ishigh.

2.5 *Blowfish*

Blowfish is a block cipher encryption based on Feistel function which uses a 64 bit block and key size ranges from 32-448 bits, variable length key is used. Variants of 14 or less processing rounds are available in blowfish [1] [7]. Substitution boxes are independent of the keys. Blowfish required more processing time because of varying key length. The time consuming sub-key generation process increases the complexity

for a brute-force attack. It provides long term data security without any known backdoor vulnerability. Reliability of Blowfish is damaged due to the use of large number of weak keys. The first 4 rounds of process are exposed to 2nd order of differentialattacks. Blowfish[4] is one of the fastest block ciphers developed to date. Blowfish suffers from weak keys problem, still no attack is known to besuccess.

In this manner the speed of the symmetric cipher is still a benefit, and the problem of distributing the symmetric key is removed. Such systems are known as hybrid cryptosystems. Another important use for public-key cryptography is to create digital signatures. Digital signatures are used much like real signatures to verify who sent a message. The private key is used to sign the message, and the public key is used to verify thesignature.

2.6 *RSA (Rivest, Shamir andAdleman):*

RSA stands for Rivest, Shamir and Adleman who introduced the RSA algorithm in 1977 [11]. RSA is an asymmetric cryptographic algorithm [2] which is also used for encryption and decryption of the message. RSA is widely used in transferring of keys over an insecure channel. Due to asymmetric nature, there are two keys used in the algorithm. One is public key and second is a private key. The public key is openly accessible to everyone in the cryptosystem and the private key is kept secret by authorized person. RSA provides confidentiality, integrity, authenticity, and non-repudiation of data [11] [13]. RSA is more commonly used in electronic industry for online money transfer [14]. In future, RSA can be used in Java cards [15].

2.7 *Diffie-hellman*

was found by whitfield diffie and martin hellman in the year 1976. This algorithm doesn't have specified key size because it uses key exchange management and has a block size of 64bits. It is a symmetric key cipher and uses common network to transfer messages. It takes nearly 14 round to convert a message and its security is broken by eaves dropping. Benefits of this algorithm is that security factors with respect to the fact that solving the discrete algorithm is very challenging, and that the shared key is never

itself transmitted over the channel. Drawback of it is the lack of authentication [1].

2.8 ElGamal

2.9

ElGamal algorithm was introduced in 1985 by Taher ElGamal [29]. ElGamal is an asymmetric key encryption algorithm that is based on the Diffie-Helman key exchange as an alternative to RSA for public key encryption. ElGamal is also used in digital signature generation algorithm called ElGamal signature scheme [11][12][13]. A homomorphic algorithm named paillier used for its semantic security[6].

ECC (Elliptic CurveCryptography)

ECC stands for Elliptic Curve Cryptography. ECC introduced in 1985 by Neal Koblitz and Victor S. Miller. ECC lies in the category of the asymmetric scheme that is based on elliptic curves. The applications of ECC are encryption, digital signatures and pseudo-random generators[10].

3. CONCLUSION

The paper defines a detailed analysis of symmetric and asymmetric encryption algorithms on the basis of different parameters. The main objective was to analyze the performance of the most popular symmetric as well as asymmetric key algorithms in terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. During the analysis it was observed that AES (Rijndael) was the best among all in terms of Security, Flexibility, Memory usage, and Encryption performance. Although the other algorithms were also competent but most of them have a tradeoff between memory usage and encryption performance with few algorithms been compromised.