A Comparative Study of Performance Analysis of Various Encryption Algorithms

Gaurav Yadav
M.E. Student,
Dept. of EXTC,
Shree L.R Tiwari College of Engineering,
Mumbai University,
gauravy167@gmail.com

Mrs. Aparna Majare
Assistant Professor,
Dept. of EXTC,
Shree L.R Tiwari College of Engineering,
Mumbai University,
aparna.majare1303@gmail.com

Abstract: In recent years, security related issues has become the major problem of informational data over the network system. To overcome these problems various encryption algorithms have been implemented. Encryption is done by using various enhanced hybrid algorithm for security of data against unauthorized attacks. This security of the data can also be done by using different secret sharing algorithm which enhance the security on confidential data over the network. In this paper, we have analyzed various encryption algorithms based on different parameter and compared them to choose the best data encryption algorithm, which overcome the problem of security related issues (integrity, authentication, confidentiality, identification of user data, privacy, availability), so that we can use it our future experimental work. Experimental results are given to analyses the effectiveness of each algorithm with the encryption and decryption time, encryption speed and throughput.

Index terms– *Encryption, AES, DES, Blowfish, Twofish, RSA, Diffi-Hellman.*

*****

1. INTRODUCTION

Cryptography is the process of converting original plain text to cipher text is known as encryption process and restoring the main text from cipher text is known as decryption process. The main aim of cryptography provides number of security goals to overcome the security related issues which on confidentiality, authentication, integrity, nonrepudiation and access control. Cryptography has symmetric-encryption algorithms(same key use for encryption and decryption) and asymmetric-encryption algorithms(different key use for encryption and decryption). Asymmetric encryption techniques(RSA, Diffi-hellman) are almost 1000 times slower than Symmetric techniques(DES, AES, Blowfish, TwoFish), because they require more computational processing power. Encryption is a very general method for promoting the information security. The development of encryption is moving towards a prospect of endless possibilities. Each day new methods of encryption techniques are discovered. This paper proposed some recent existing encryption techniques and their performance according to different parameters used in Algorithms. This comparison analysis shows which algorithm is best suited in which environment.

2. RELATED WORK

There are various research studies that compare between the performance of the common encryption algorithms. This section discusses the results of some of these studies:

For analyzing the performance comparison of the AES and DES algorithms which demonstrate the performance resultsuch as encryption speed ,time ,block size and complexity[1]. Similarly AES, Blowfish and Twofish are analyzed on the basis of their performance parameter such as encryption and decryption time, level of security, throughput performance and overall execution time of the algorithm[2]. Symmetric encryption algorithms AES and Blowfish are specified as better solution as compared with others algorithm such DES, 3DES andTwofish in the aspect of different parameter such power consumption, throughput, encryption / decryption ratio and level of security[3],[7]. Asymmetric encryption algorithm RSA is more secure since it uses the factoring of high prime number for key generation andcan be used for better application in wireless network system because of its high functional speed and to overcome security issues related[3],[7].Confidentiality and scalability provided by Triple DES over RSA and DES is much higher that makes it suitable even though DES consume less power memory and time to encrypt and decrypt the data but on security front DES can be easily broken by brute force technique as compared to Triple DES and RSA making it the least secure algorithm and performance of algorithms is different according to the inputs size[5].New Comparative Study between three encryption algorithm such as DES, 3DES and AES within Nine Factors achieving an effectiveness, give and security, which is at the challenge of researchers[4].

By analyzing and comparing the performance of symmetric and asymmetric encryption algorithms such as DES, triple DES, AES, Blowfish, RSA and Diffie-Hellman on various parameter such as tunability, key length, throughput, power consumption. we have concluded which algorithm is suitable for particular environment[6].

3.ENCRPTION ALGORITHMS

There are two types of encryption technique which are symmetric key encryption and asymmetric key encryption.

[A]Symmetric key encryption

In the symmetric key encryption, same key is used for both encryption and decryption process. The sender and receiver must share the algorithm and the key. The key must be kept secret.

1 Advanced Encryption Standard (AES)

AES is a symmetric block cipher that can Block size 128 bit, three different Cipher keys 128, 192 and 256 bits. Basically, AES is based on a design principle encryption algorithmsknown as – transposition, substitution, and transposition-substitution technique. Most AES calculation are uses a round function in special finite field that is compared of four different byte-oriented transformation such as Sub byte, Shift row, Mix column , Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. At present the most common key size likely to be used is the 128 bit key. Rijndael was selected as the AES in Oct-200 designed to have the following characteristics:

- Resistance to protect from all known attacks.
- Speed and code compactness depends on a wide range of platforms.
- Design simpler.

2 Data Encryption Standard (DES)

DES is a symmetric key algorithm which was developed by IBM inJan 1977. It is to be insecure for many applicationmainly due to used block size 64 bit being too small, key length usable 56 bits. The key is usually expressed as a 64-bit number, but every eight bit 64 bit is used for parity bit checking and otherwise ignored. These parity bits are the least-Significant bits(LSB) of the key bytes. DES always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES used 16 rounds of transposition and substitution to encrypt each group of 8(64 bit) plaintext letters and output from each round is one by one. The number of rounds is exponentially proportional to theamount of time and fined a key using a brute-force attack. Therefore, the security of the algorithm increases exponentially due to increasing the number of rounds.

3 Blowfish Algorithm

Blowfish is a symmetric fast cipher key, designed in 1993 for different length key from32 bits to 448 bits used in general. It uses 64-bit block size and slow key changes occurs. The algorithm existing into two parts: a key-expansion part for conversion of key and a data-encryption part for existing rounds. Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, 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.

4Twofish Algorithm

Twofish is also a symmetric key block cipher having fiestel structure and it uses different key sizes of 128, 192 and 256 bits with block size of 128 bits and there are 16 rounds of encryption algorithm. It is also developed and explained by bruceschneier in 1998. Twofish also uses block ciphering like Blowfish. It is efficient for software that runs in smaller processor (smart cards) and embedding in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Twofish has not been patented and the reference implementation due to that it is license-free and freely available for use.Twofish encryption algorithm also provides good level of security but it lacks in encryption speed as compared to blowfish.

[B]Asymmetric key encryption

Asymmetric key encryption is the technique, in which one algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. One key is public (published) and second is kept private. They are also called as the public key encryption. It must be impossible or at least impractical to decipher a message if no other information is available.

1 RSA Algorithm

Most widely accepted and implemented general purpose approach to public key encryption developed byRivest, Shamir and Adleman of MIT in 1977. It is block cipher in which the plaintext and cipher text are integers between 0 and n-1 for same n and typical size of n is 1024 bits or more for a high level of security. It can be able to be used for both encryption and digital signatures. The security of RSA is generally considered to factoring. RSA computation occurs with integers modulo n = a * b, for select two random secret primes a, b. To encrypt a message m, public key use a public key exponent e. so cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (a-1)*(b-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The problem for the attacker isthat computing the reverse d of e is assumed to benoeasier than factorizing n. Keys of size, say, 2048 bits that provides.

2Diffie-Hellman Algorithm

Discovered by Whitfield Diffie and Martin Hellman for key exchange management in public key encryption algorithm, the protocol enables 2 users to establish a secret key over an insecure medium requires no prior secrets using a public key process based on discrete logarithms.The protocol is secure only if the authenticity of the 2 participants can be established. Therefore, in many cryptographically protocols, two parties wish to start communicating. Diffie-Hellman protocols are exchange keys and allow the construction of common secret key over an unconfident contact channel. This problem is based on related to discrete logarithms; its name is Diffie-Hellman problem. This problem is hard, as compare to the discrete logarithm problem.

4 PERFORMANCE ANALYSIS

There are various performance factors which are used to analyzed the different encryption algorithms.

1. Throughput performance

It is the higher rate of production or maximum rate at which data can be processed which belong to may be delivered over a physical or logical link. It may be affected by various factors such as medium, available processing power of the system components and end-user behavior.

2. Key Length Size

In most cryptographic function, the key length is important security parameters andkey management is the important factor to shows the how the data is encrypted. The symmetric algorithm uses a different key length which is longer than asymmetric logarithm. So, the key management is a huge aspect in encryption processing for control operation of the cipher.

3. Encryption and Decryption Speed

In many real-time applications, the encryption and decryption algorithms are fast sufficient which depends on the register size of the CPU to meet real time requirements**.**

4. Encryption Ratio

The encryption ratio is the measurement of the total number of data that is to throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased the power consumption is decrease and gives more long life of the system component.

5. Encryption and Decryption Time

The time given by algorithms totally depends on the speed of the processor and algorithm complexity. Less time algorithm improves the entire operation of the processor. For better encryption and decryption, computation of time factor is essential by the algorithm.

6. Level of security Issues

Cryptographic security defines whether encryption process is secure against from all known attacks **s**uch astime attackand variable plaintext-cipher text attack. For highly important multimedia application to the encryption process should satisfy cryptography security.

Comparison of Encryption Algorithms:

Algorithms **Parameters**	**DES**	**AES**	**Blowfish**	**Twofish**	**RSA**	**Diffi-Hellman**
Key length(Bits)	64(56 usable bits)	128/192/256 bits	Variable key length i.e, 33-448 bits	128/192/256	>1024 bits	Key exchange management
Rounds	16	10/12/14	16	16	1	56
Block size (Bits)	64	18	64	128	Variable block size	56
Encryption speed	Very slow	Faster	Very fast	Fast	Fast	Slow
Power consumption	Higher than AES	Higher than Blowfish	Very low	Low	High	Lower than RSA
Level of security	Adequate security	Excellent	Highly secure	Secure	Good level of security	Secure
Through put	Lower than AES	Lower than Blow fish	Very high	High	High	Low
Complexity	More	Less	Less than AES	Moderate	More	Less
Security against	Brute force attack	Chosen plain, known plain text	Dictionary attacks	Differential attack, related key attack	Timing attacks	Eaves Dropping
Application	Smart card	Password Manager	IDS server	Sql server 2000	Online credit card security system	Protocols like SSL,SSH, IP sec.

CONCLUSION

Encryption algorithm plays a very important role in communication security to overcome security related issues. This paper presents a comparative study of different key algorithms like, AES, DES, Twofish, Blowfish, Diffi-hellman and RSA. Each algorithm has been comparatively analyzed on different set of parameters. From the results, it has been found that among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient algorithms. The speed and power consumption of these algorithms are more better compared to the others. In case of asymmetric encryption algorithm, RSA is more secure and can be used for application in wirelessnetworkbecauseof its good speed, less time and security. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and it is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques the blowfish and Twofish algorithm is specified as the better solution.

REFERENCES

[1] Shaza D. Rihan, Ahmed Khalid, SaifeEldin F. Osman "A performance Comparison of Encryption Algorithms AES and DES" International Journal of Engineering Research and Technology, Volume 4, december 2015.

[2] Neha, Mandeep Kaur "Enhanced Security Using Hybrid Encryption Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Volume .4, Issue 7, July 2016.

[3] AnkitaVerma, ParamitaGuha, Sunita Mishra "Comparative Study of Different Cryptographic Algorithms, International Journal of Emerging Trends and Technology in Computer Science, Volume 5, Issue 2, March -April 2016.

[4] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

[5] MohitMarwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[6] Ritutripathi, sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and research, Volume 1, Issue 6, June 2014, ISSN 2348-4853

[7] Ms. TheresBemila, Karan Kundar, Lokesh Jain, Shashikant Sharma, NayanMakasare "Comparative Study of Various Security Algorithms applicable in Multi-Cloud Environment", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2016.