AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS

AL.Jeeva[1]
Research Scholar
Dept of Computer Sci & Engg
Alagappa University
Karaikudi

Dr.V.Palanisamy[2]
Associate Professor
Dept of Computer Sci & Engg
Alagappa University
Karaikudi

K.Kanagaram[3]
Project Fellow (DST – PURSE)
Dept of Computer Sci & Engg
Alagappa University
Karaikudi

ABSTRACT

In wireless networks, the security of data is an important aspect and encryption algorithms play an important role to provide the security to the wireless networks. The main aim of the cryptography is to enhance the data confidentiality and privacy by making the information unintelligible. Hence the data cannot be interrupted by the intruders. The Encryption techniques and various algorithms are used to provide the needed security to the applications This paper provides a fair performance comparison between the various cryptography algorithms such as the AES, RSA, RC2, DES, 3DES, DSA where both types of symmetric and asymmetric techniques. We have compared these parameters for both the symmetric key encryption and for the asymmetric key encryption. The parameters such as the tunability, key length, computational speed, and the type of attacks on the security issues are provided. As a result, the better solution to the symmetric key encryption and for the asymmetric key encryption is provided.

Keywords: Cryptography, Encryption, AES, Symmetric key encryption, Asymmetric key encryption.

1. INTRODUCTION

The demand for the ubiquitous personal communications is driving the development of new networking techniques. In the wireless communication the security of the data plays the vital role. To improve the security of the data being transmitted various techniques are employed. The important method used to provide the confidentiality is the data encryption and decryption technique. Network security becomes more crucial when the volume of the data becomes larger and complex.

Cryptography is the art of transforming the information's on the applications into scrambled or in unintelligible format. It relates to the study of mathematical techniques related to the aspects of information security such as the confidentiality, data integrity, and authentication of the data. The technology used for this is called as the cryptology. When the user defined input may in any of the format such as the text, or an image is which is plain, is converted into a scrambled form called as the cipher text or cipher image. This process is referred to us as encryption. To convert the data the user should provide the specific algorithm. The reversible process in which the original data is recovered is called as the decryption process. In cryptography majorly three types of encryption techniques are taken place. The substitution technique, the transposition technique and the transposition- substitution technique.

The most important type of the encryption type is the symmetric key encryption. In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. It works with high speed. The symmetric key encryption takes place in two methodologies either as the block ciphers or as the stream ciphers. One of the main advantages of using the symmetric key encryption is that the computational power to this encryption technique is small. The keys for this are unique or there exists a simple transformation between the two keys.

Asymmetric key encryption is the technique in which the keys are different for the encryption and the decryption process. They are also known as the public key encryption. Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private, Algorithm. Asymmetric algorithms are generally slow and it is impractical to use them to

encrypt large amounts of data. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted.

The strength of the encryption algorithms is based on how it is vulnerable to the attacks made on it. The major attacks on the encryption techniques are such as the chosen-plain text attacks, known – plaintext attacks, brute force attacks, linear cryptanalysis etc. To avoid these attacks needed security measures should be enhanced with the encryption. The paper is organized as follows. In section 2 the related works on the paper is placed. In section 3 the classification of the, algorithm is taken place. In section 4 the various performance factors for the algorithms are given. In section 5 the results and the discussions area placed. With the section 6 the paper is concluded.

2. RELATED WORK

In this section the various methodologies and techniques for the encryption techniques used by various papers are provided. In the paper proposed by Jolly Shah and Dr. Vikas Saxena, the various performance factors such as the computational speed, tunability, format compliance, the visual degradation after the encryption and the security issues are proposed.

In the paper proposed by Pranay Meshram, Pratibha Bhaisare, and S.J.Karale the comparative study of selective encryption algorithm for wireless adhoc network the various techniques their algorithms, their results are evaluated. More over the paper refers the classification of the algorithms based on the techniques applied.

In the paper proposed by Nachiketh Potlapally, Srivaths Ravi, Anand Raghunathan and Ganesh Lakshminarayana, the security o the efficient public key encryption on the wireless networks is taken place. The paper discusses the various protocols used for the wireless transmission of the data after encryption.

Vidyasagar Potdar, Elizabeth Chang in their paper proposed the technique to encrypt the text and made it hidden and evaluated the various security issues that are araised.In the paper proposed byM. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki a Modified AES Based Algorithm for the encryption on text and the images is given.In the paper proposed by Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry the efficiency and the performance parameters of the algorithms when applied for the image encryption is taken place.

In the paper Cryptographic Algorithms for Secure Data Communication, by Zirra Peter Buba and Gregory Maksha Wajiga the asymmetric keys and its performance efficiency, key scheduling are discussed.In the paper, proposed by Gurjeevan Singh, Ashwani Kumar Singla, and K.S. Sandha the performance metrics for the symmetric key algorithms and their results are discussed.

3. PROPOSED WORK

In this section the overview of the classification of the types of the encryption techniques and the parameters that are verified for the algorithms and the security issues are briefly placed in the following sub sections.

3.1 Classification of the Encryption Algorithms

The encryption algorithms are basically classified into two types based on the keys used for the encryption. Symmetric key encryption and the Asymmetric key encryption.

3.1.1 Symmetric Key Encryption

The most important type of the encryption type is the symmetric key encryption. In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption. A block cipher is taken as the input, a key and input, and then the output block will be same in size in the symmetric key encryption.

The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. In the block cipher mode the whole data is divided into number of blocks and based on the block length the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized and then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. The performance evaluation is taken place for the following symmetric key encryption techniques. The AES Algorithm, the DES algorithm, Blowfish algorithm, Triple DES algorithm, and Rivest Cipher 4 algorithm.

3.1.1 a)The AES Algorithm

The encryption algorithm is an integral work of encryption and decryption process. They should preserve high security to the data being transmitted. Basically, encryption algorithms are divided into three major categories – transposition, substitution, and transposition – substitution technique. Internally the AES algorithm's operations are performed on a two dimensional array of bytes called the state. The state consists of four rows of each bytes, each contains Nb number of bytes, where Nb is the block length divided by 32.

3.1.1 b) The DES Algorithm

Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses using a 56-bit. DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm.

DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

3.1.1 c) Blowfish Algorithm

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general. It is a 16 round fiestel cipher that uses the large key size. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.

3.1.1 d) Triple DES Algorithm

The Triple Des Algorithm encrypts data three times and uses a different key for at least one of the three passes giving it a cumulative key size of 112-168 bits. That should produce an expected strength of something like 112 bits, which is more than enough to defeat brute force attacks. Triple DES is much stronger than (single) DES; however, it is rather slow compared to some new block ciphers.

3.1.1 e) Rivest Cipher 4 Algorithm

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext.The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted.

The RC4 (Rivest Cipher Version 4) is a symmetric key system, which process plain text in small blocks as small as a single bit. They sort some form of memory called stat for substitution. RC4 is a binary additive stream cipher. It uses variable sized key that can range between 8 and 2048 bits in multiples of 8 bits. Hence key length took an important task in RC4 Encryption

The algorithm is very fast. Its security is unknown, but breaking it does not seem trivial either. Because of its speed, it may have uses in certain applications. It accepts keys of arbitrary length. RC4 is essentially a pseudo random number generator, and the output of the generator is exclusive-ored with the data stream. For this reason, it is very important that the same RC4 key never be used to encrypt two data streams.

3.1.2 Asymmetric key Encryption

Asymmetric key encryption is the technique in which the keys are different for the encryption and the decryption process. They are also known as the public key encryption. One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's user. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key.

Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private Algorithm. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted. Asymmetric encryption algorithms need at least a 3,000-bit key to achieve the same level of security of a 128-bit symmetric algorithm. For the following algorithms the performance factors are evaluate.

3.1.2 a)RSA Algorithm

Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be used both for encryption and for digital signatures. The security of RSA is generally considered equivalent to factoring. RSA computation occurs with integers modulo n = p * q, for two large secret primes p, q. To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-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 is that computing the reverse d of e is assumed to be no easier than factorizing n. The key size should be greater than 1024 bits for a reasonable level of security. Keys of size, say, 2048 bits that provides security.

3.1.2 b) Diffie-Hellman Algorithm

It is the first public key encryption algorithm, using discrete logarithms in a finite field. Allows two users to exchange a secret key over an insecure medium without any prior secrets.Diffie-Hellman (DH) is a widely used key exchange algorithm. In many cryptographically protocols, two parties wish to begin communicating. The key exchange by Diffie-Hellman protocol, by allowing the construction of a common secret key over an insecure communication channel. It is based on a problem related to discrete logarithms, namely the Diffie-Hellman problem. This problem is considered hard, and it is in some instances as hard as the discrete logarithm problem. The Diffie-Hellman protocol is generally considered to be secure when an appropriate mathematical group is used.

4. PERFORMANCE FACTORS

In this paper, the following factors are used as the performance criteria, such as the tunability, computational speed, the key length management, the encryption ratio and the security of data against attacks.

4.1 Tunability

It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

4.2 Computational Speed

In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

4.3 Key Length Value

In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.

4.4 Encryption Ratio

The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation.

4.5 Security Issues

Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high.

5. RESULTS AND DISCUSSIONS

This section presents performance and comparison with respect to various parameters. The encryption ratio is measured in terms of either minimum, moderate or maximum. The speed is defined by the following term such as fast, slow, moderate. We specify tunability as either yes or no. The key value is measured in terms of bit value used. The experimental results are implemented using the visual studio. Net packages.

FACTORS ANALYSED	SYMMETRIC KEY ENCRYPTION					ASYMMETRIC KEY ENCRYPTION	
	AES	DES	TRIPLE DES	BLOWFISH	RC4	RSA	DIFFIE-HELLMAN
Encryption Ratio	High	High	Moderate	High	Low	High	High
Speed	Fast	Fast	Fast	Fast	Slow	Fast	Slow
Key Length	128-, 192-, or 256-bit	56-bit key	112-168 bits	32 bits to 448 bits.	256 bytes	> 1024 bits	Key Exchange Management
Tunability	No	No	No	Yes	No	Yes	Yes
Security Against Attacks	Chosen-Plain, Known-Plain text.	Brute force	Brute Force, Chosen – plain text, Known plain text	Dictionary Attacks	Bit Flipping attacks	Timing Attacks	Eavesdropping.

From the above evaluated table we can conclude that the encryption ratio is high in using the symmetric key encryption techniques. The Tunability is higher in the Asymmetric encryption technique. The key length is high at the asymmetric type of encryption; hence to break the code is complex in RSA. In the aspect of speed the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques the AES algorithm is specified as the better solution then follows the blowfish algorithm. In the Asymmetric encryption technique the RSA algorithm is more secure since it uses the factoring of high prime number for key generation. Hence, the RSA algorithm is found as the better solution in this method.

6. REFERENCES

[1] I.Branovic, R.Giorgi and E.martineli “Memory Performance of Public-Key Cryptography Methods in Mobile Environments”.

[2] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha , “Performance Evaluation of Symmetric Cryptography Algorithms “, in IJECT Vol. 2, Issue 3, Sept. 2011 ,ISSN : 2230-9543

[3] Gladman, "A Specification for Rijndael, the AES algorithm", May 2003, http://fp.gladman.plus.com/Cryptography_technology/rijndeal/aes.spec.311.pdf.

[4] Jolly Shah and Dr. Vikas Saxena," Performance Study on Image Encryption Schemes" In: IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4

[5] MarwaAbd El-Wahed and Mesbah and Amin shoukry, 2008, "Efficiency and Security of some Image Encryption Algorithms", Proceedings of the world Congress on Engineering 2008 Vol I.

[6] Nachiketh Potlapally Srivaths Ravi Anand Raghunathan and Ganesh Lakshminarayana_ "Algorithm Exploration for Efficient Public-Key Security Processing on Wireless Handsets", U. S. Department of Commerce, The Emerging Digital Economy II.

[6] Pranay Meshram,Pratibha Bhaisare, S.J.Karale,",comparative study of selective encryption algorithm for wireless adhoc network" ,IJREAS Volume 2, Issue 2 , in International Journal of Research in Engineering & Applied Sciences.

[7] W. Stallings. Cryptography and Network Security, Prentice Hall, 1995.

[8]I. VenkataSajManoj,"Cryptography and Steganography", International Journal of Computer Applications (0095 – 8887), Volume 1- No.12.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based Algorithm for Image Encryption" ,in World Academy of Science, Engineering and Technology.

[10] Zirra Peter Buba & Gregory Maksha Wajiga "Cryptographic Algorithms for Secure Data Communication International "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.

Authors Profile

Dr.PalanisamyVellaiyan obtained his B.Sc degree in Mathematics from Bharathidasan University in 1978.He also received the M.C.A., and ph.D Degree from Alagappa University in 1990 and 2005 respectively. After that working as Lecturer in AVVM Sri Pushpam College, Poondi from 1990 to 1995, He joined Alagappa University as Lecturer in 1995. He is currently working as Professor and Head of the department of Computer Science and Engineering. He also received the M.Tech. Degree from Bharathidasan University in 2009. He has published over 20 journals and conferences and his research interest includes Computer Networks & Security, Data Mining & Warehousing, Mobile Communication and Computer Algorithms.

JeevaAlagarsamy received his Diploma in EEE from Alagappa Polytechnic, Karaikudi. He also received B.C.A., and M.Sc., Degree from Alagapppa University, Karaikudi in 2008, 2011 respectively. He is doing M.Phil Degree in Computer Science, Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamil Nadu, India. His research interest includes ad hoc wireless Networks &Security Data mining and Computer Algorithms.

Kanagara Krishnan received his B.Sc., Degree in Electronics from Bharathiyar University in 2008. He also received the M.C.A., Degree from Anna University in 2011. He is currently working as Project Fellow (DST-PURSE) in Department of Computer Science and Engineering, Alagappa University, Karaikudi.His research interest includes Database Security and Computer Networks.