ISSN: 0974-2115

A comparative analysis of Symmetric and Asymmetric key cryptography

K. Uma*, G. Karthik, R. Vishnu Prasath
Department of IT, VIT University,vellore-632014, India
***Corresponding author: E-Mail: drumakphd@gmail.com**

ABSTRACT

Network safekeeping strategies initiation and execution is crucial for the purpose of secured data transmission and confidentiality. Cryptography is a technique which is developed solely for the purpose of data security and integrity in the process of communication. Though several theories and concepts exists, each varies with the amount of security it offers to the network channel. An important element which determines the type of cryptography is key distribution. Based on the type of key distribution, cryptography is broadly classified as symmetric and asymmetric. In this paper, the classical algorithms which are used for symmetric and asymmetric cryptography are analysed in terms of their pros and cons in various aspects.

KEY WORDS: Public Key, Private Key, Encryption, Decryption, Cipher Type, Key Dimension.

1. INTRODUCTION

Cryptography is the technique of scrambling plain text. This secures data and information from any internal or external attacks. Thus, it provides integrity, confidentiality, non-repudiation and authenticity to the secret data. The texts involved in cryptography are plain and cipher texts. Plain texts are human readable texts and the information which the sender intends to send. The plain text is encrypted to an illegible form called the cipher text. Based on the encryption methodology used, it is differentiated as symmetric and asymmetric cryptography. Modern cryptography concerns itself with the following four objectives:

- Concealment (unintended person cannot intercept the message)
- Uprightness (no alteration is permitted between the sender and receiver)
- Non-repudiation (the sender of the message cannot disagree at a later stage his intentions in the making of the information)
- Authentication (the confirmation of sender’s and receiver’s identity can be performed by each other)

Symmetric Key Cryptography: Symmetric key cryptography is also called secret-key or shared key cryptography. In this type of cryptography, the sender and receiver shares a common key for both encryption and decryption. The key used in this technique is certified by oneself. The key is shared through communication. If an intruder obtains the key, the whole process is compromised and the intruder can easily decrypt the message. This method is preferred because of its fast service and less resource requirement. The algorithms compared in this paper are DES, 3DES, AES, BLOWFISH, RC2, RC4, SKIPJACK.

Asymmetric Key Cryptography: The asymmetric key cryptography is also known as public key cryptography. Scrambling of text is carried out using public key of the sender and deciphering is carried out using the private key of the receiver. The concept of self-certification is lacking here because digital signatures are used to attest the keys. This method provides better authentication and security as the privacy remains intact. There are various algorithms to implement this cryptography mechanism. They are RSA, Diffie-Hellman, ECC and Digital Signature Algorithm, Rabin, EIGamal.

Comparative Analysis of Traditional Cryptography Algorithms: Traditional algorithms are the existing procedures used for achieving the process of cryptography. These algorithms are well tested before they are being implemented in an application. Every algorithm differs with the each other on various terms. Based on the test results, the following table (table 1) is derived based on the arrangement, key dimensions, number of rounds, and cipher type.

Table.1. Comparison of symmetric key algorithms

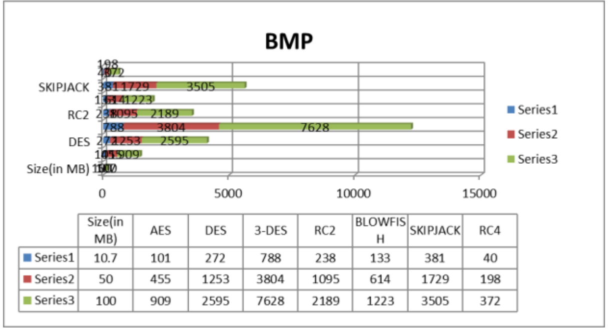
Method	Arrangement	No of rounds	Key dimensions	type
DES	Balanced Fiestel-Network	16	56	Chunk
3DES	Fiestel-Network	48	112,168	Chunk
RC2	Source-heavy Fiestel Network	18	40 to 1024	Chunk
RC4	Nil	256	40 to 2048	Stream
AES	Substitution Permutation Network	10,12,14	128,192,256	Chunk
Blowfish	Fiestel-Network	16	32 to 448	Chunk
Skipjack	Unbalanced Fiestel-Network	32	80	Chunk

Encryption time for flv and bmp file types (milliseconds): Each file takes its own time for encryption with respect to its type and size. The most common file types used are BMP and FLV. Every algorithm perform at a different pace since they differ with the number of rounds in encrypting the source message. The following table (table.2) is derived as the result of analysing the time taken for a particular file through a specific algorithm.

Table.2. Comparison of encryption time for BMP and FLV file types

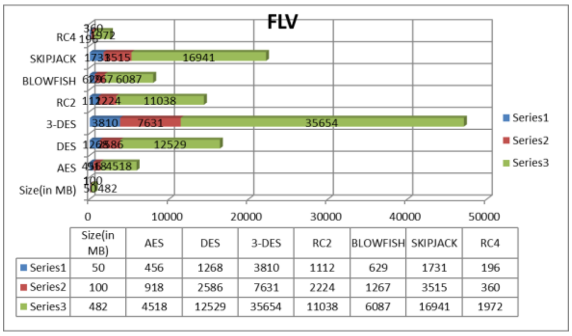
File type	Size(in MB)	Encryption Time In Millisecond						
		AES	DES	3-DES	RC2	BLOWFISH	SKIPJACK	RC4
		128	56	112	40	32	80	40
BMP	10.7	101	272	788	238	133	381	40
	50	455	1253	3804	1095	614	1729	198
	100	909	2595	7628	2189	1223	3505	372
FLV	50	456	1268	3810	1112	629	1731	196
	100	918	2586	7631	2224	1267	3515	360
	482	4518	12529	35654	11038	6087	16941	1972

Graphical Representation of Encryption Time Taken: The values provided in the table is represented as a graph for the easy interpretation of the inference. Two separate graphs are drawn for two file types. The x-axis represents the size of the image file while the y-axis represents the type of algorithm. The definitive aim is to know the speed of each method when performing the encryption. Fig.1, shows the time taken for encrypting BMP file and Fig.2, shows the time taken for encrypting FLV file.



	Size(in MB)	AES	DES	3-DES	RC2	BLOWFISH	SKIPJACK	RC4
Series1	10.7	101	272	788	238	133	381	40
Series2	50	455	1253	3804	1095	614	1729	198
Series3	100	909	2595	7628	2189	1223	3505	372

Figure.1. BMP file type



	Size(in MB)	AES	DES	3-DES	RC2	BLOWFISH	SKIPJACK	RC4
Series1	50	456	1268	3810	1112	629	1731	196
Series2	100	918	2586	7631	2224	1267	3515	360
Series3	482	4518	12529	35654	11038	6087	16941	1972

Figure.2. FLV file type

Comparative Study of Asymmetric Key Algorithms: This type of methodology requires pair of keys to satisfy the agenda of encryption and decryption. The key pair is usually mathematically related to each other. When one key scrambles, the other one can only be used to decipher the text. The different algorithms used for asymmetric-key cryptography are briefly explained below.

Rivest-Shamir-Adleman (RSA): General formula is (d, e) where d denotes the private key and e symbolises the public key. Both encryption and decryption uses the same function. It is highly secure because it is difficult to produce the private key from the public key and modulus. The attackers find it difficult to compute the reverse of e. Complexity of generating the key is high. The process of cryptography is quite slow. It has not been tested that it is equivalent to the factorization method and it is tedious to factorize large numbers. The key length should be larger than 1024 bits.

Rabin: It is used for Integer factorization problem, Square roots modulo composite. Rabin is secure against attacks by passive adversary and unbelievably fast due to single module squaring. Slower decryption method compared to RSA method. It is quite vulnerable to RSA attacks.

Elliptical Curve Cryptography (ECC): Elliptic curve equations is used to compute the keys. It can provide security using a 164 bit key and has more advantages than RSA and Diffie Hellman algorithms. The power exploitation is low and provides better benefits to batteries. Size of encrypted message is increased and the implementation is very difficult due to the high complexity compared to RSA. Elliptic Curve Digital Signature Algorithm (ECDSA) is introduced to serve this purpose. The Authenticated key agreement protocol, ECMQV secures the system against man in the middle attacks.

Digital Signature Algorithm (DSA): Data authentication is done using a pair of large numbers computed using some algorithms. Private keys are used to generate signatures and public keys are used to verify them. It is very fast and provides non-repudiation and legitimacy. It protects the data against different attacks like Man-in-the-Middle attacks and has more advantages than other traditional asymmetric key algorithms. Digital signatures have short life span. They complicate sharing because they are not compatible. Verification software is essential. Digital certificates should only be bought from trusted authorities.

Diffie-Hellman: It is based on the sharing of secret cryptographic key. This key is used for both encryption and decryption purposes. It depends on hardness of the discrete logarithms. The algorithm is quite fast since the symmetric key is of very short length (256 bits). The attacks escalates with the usage of symmetric keys. This algorithm is more vulnerable to Man in the Middle attacks. Frequent key changing is necessary. Development of Station-to-Station etiquette overthrows Man in the Middle attacks. The progress of digital signature is also a solution to the attacks.

EIGamal: It is based on discrete logarithm problem, Diffie- Hellman problem. It uses randomization encryption. Plain text is half the size of cipher text. Factor of two unconditionally flexible thus prone to chosen cipher text attack. There exists a possibility of bogus signatures. It can be cracked in case of weak decision of p and e. Encryption is slow as it involves two modular exponentiations.

2. CONCLUSION

Both Symmetric and Asymmetric Key algorithms are highly competent in securing the transferred data over any communication medium. In this paper, the traditional algorithms are discussed. Symmetric cryptography utilizes a single key to achieve encryption and decryption which could rise security issues. On the other hand, Asymmetric Key Cryptography uses two separate keys to prevent any unethical access to the data. One key remains private while the other is available in the public key repository. The latter provides more security than the former. Still symmetric cryptographic techniques are preferred for their simpler description and less requirement of resources. In future, for resourceful and protected data transmission, cryptography is an ultimate solution. Various applications can be built using symmetric and asymmetric algorithms for enhancing the protection. The higher the security of the system, lesser are the chances of breaking into it. The future of security system depends on such algorithms which makes the intrusion absolutely impossible.

REFERENCES

Adam J, Elbirt and Christof Paar, An Instruction-Level Distributed Processor for Symmetric-Key Cryptography, IEEE Transactions on Parallel and Distributed Systems, 16 (5), 2005, 468-480.

Ankita Baheti, Lokesh Singh, and Asif Ullah Khan,Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System and Authentication using Neural Network, Fourth International Conference on Communication Systems and Network Technologies, IEEE, 2014, 664-668,

Ankur Chaudhary, Khaleel Ahmad, and Rizvi M.A, E-commerce Security through Asymmetric Key Algorithm, Fourth International, 2014.

Bibhudendra Acharya, Sambit Kumar Shukla, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,H-S-X Cryptosystem and Its Application to Image Encryption, 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009, 720-724,

Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 18(4), 2010, 553-563, April 2010.

Debanjan Das, Megholova Mukherjee, Neha Choudhary, Asoke Nath, and Joyshree Nath,An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method, DJMNA symmetric key algorithm, 2011 World Congress on Information and Communication Technologies, IEEE, 2011, 1199-1204,

Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, and Asoke Nath, A new Symmetric key Cryptography Algorithm using extended MSA method, DJSA symmetric key algorithm, International Conference on Communication Systems and Network Technologies, 2011, 89-94.

Massimo Alioto, Massimo Poli, and Santina Rocchi, Differential Power Analysis Attacks to Precharged Buses, A General Analysis for Symmetric-Key Cryptographic Algorithms, IEEE Transactions on Dependable and Secure Computing, 7 (3), 2010, 226-239,

Miodrag J, Mihaljevic, Ryuji Kohno,Cryptanalysis of Fast Encryption Algorithm for Multimedia FEA-M, IEEE Communications Letters, 6(9), 2002, 382-384.

Nath A, Ghosh S, and Mallik M.A, Symmetric key cryptography using random key generator, Proceedings of International conference on SAM-2010 held at Las Vegas(USA), 2, 2010, 239- 244

Radu Terec, Mircea-Florin Vaida, Lenuta Alboaie, and Ligia Chiorean, DNA Security using Symmetric and Asymmetric Cryptography, The Society of Digital Information and Wireless Communications, 1(1), 2011, 34-51.

Robert M, Bevensee, Feigenbaum encryption of messages, IEEE Potentials, IEEE, 2001, 39-41,

Sean O'Melia and Adam Elbirt J, Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 18(11), 2010, 1505-1518.