A COMPARATIVE SURVEY ON DIFFERENT SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS

[1]Upendra Chaurasiya,[2]Manu Vardhan
[1] Faculty, [2]Assistant Professor
[12]CSE Department,
[12]National Institute of Technology, Raipur,India

*Abstract :*Cryptography is playing an important role to protect data and information on world wide web.In this paper we present a detailed study of most of the symmetric key encryption algorithms and asymmetric key encryption algorithms with their strengths and weaknesses over each other based on their Architecture, Scalability, Flexibility, Authenticity, Accuracy, Security and Restriction that are essential for secure communication, wireless or wired media .In this paper, we have provided a fair comparison between most common symmetric key cryptography algorithms: DES, 3DES, IDEA, BLOWFISH,TEA, CAST5,TWOFISH, RC4, RC5 and RC6.

***IndexTerms* - Symmentric Key Algorithm, Encryption, Decryption, Attacks, Security, Cryptography, Algorithm, Key, Cipher**

I. INTRODUCTION

Cryptography is playing very important role to protect information transmitted over a wireless or wire communication channel[1]. If user gave the password to online banking, client very sure that no one actually seen, what client is typing, so client safe and secure there. When a sender’s password has reached the server side.Server is also protected physically ,which means no one can get into the server machine and look at what client send, therefore on the sender side and server side data have been always secure, because they have got it physically. But the data has to go through many channels, so one is might be having some wireless channel or wired channels and routers on the way and finally they have reached the destination, the sender’s machine is secured, server machine sure that data is secure. But secure or protected path (channel) grantee that no one is looking at the wire into the channel. Anyone can set their frequency to client sending frequency in case about it is wireless, and easily trap client signals also trapped the wire, retrieve the data on the entire communication channel.The purpose of cryptography is to convert the message in the plain text into some unreadable forms, before sending it on the wires.

Now the entire purpose is sender takes the plain text and convert it into some forms which is unreadable by anyone which is called as the cipher text. Now this cipher text will be sent on wires. This cipher text will not be readable by anyone, nowonce this cipher text reached the server, it has to be converted back to the plain text, now the process of converting this plain text into cipher text is called encryption. The process of converting cipher text into plain text is called decryption. So we need encryption and decryption method in such a way that the only sender can do this and receiver can do this, so whenever a sender encrypts the data no one on the wire should be able to do the decryption. So this method is required, traditionally, we have two ways, there are two methods. One is symmetric and other one asymmetric key cryptography.

Symmetric key Cryptography deal with same key, if client have plain text then we have something called as encryption algorithm, and to this encryption algorithm ,we generally provide something called as key ,now this encryption algorithm is going to convert plain text into cipher text, and now this cipher text, we will be sent on the wire, to the otherside,now the other side is going to take this cipher text and this cipher text will be given to something called as decryption algorithm and to decrypt it again the same key, which ever sender used the same key will be use that is called as symmetric means same thing and shared key because the same is shared. This will be decrypted into plain text that is called symmetric key cryptography. The problem is before sender start everything communication, sender suppose to know what the keys value, so before client send actual data ,sender suppose to send the key to other side ,before client send plain text, do everything client have to the key, now the main problem is how can send the key to the other side, if any one on the way find the key, then it is game over, because anyone can decrypt what client is sending, So before client do this, the key has to be send, that is main problem.

In Asymmetric Key Cryptography,There are two parties one is Sender, the other is the recipient. If Sender wants to send information to Recipient securely. There is the main thing, before doing this both Sender & Recipient are supposed to generate a pair of keys known as public key and private key, So Sender is going to generate a pair of known as private key of Sender and public key of the sender, Recipient is going to generate one pair of key known as private key of Recipient & the public key of the recipient. Now these two key in such a way that once we encrypt anything using public key of Sender Then we can decrypted only using private key of Sender, if encrypt anything using private key of Sender, we can decrypt using only public key of the sender, and same thing true with this. If encrypt anything using the public key of the recipient then only decrypt using private key of Recipient, if we encrypt anything using the private key of Recipient, Then decrypt using only the public key of the recipient. The public key of sender & the public key of recipient are kept known globally, which means everyone should, what public key of Sender & Recipient. Before starting the communication, both Sender & Recipient suppose to generate pair of keys. This pair of keys should be such in a way that, if encryption is done with one of them, Then decryption should be done with another one. We can call one of them as private key, another one public key. The reason behind it is public key is going to be known globally and private key will be known only that party. The Private key of Sender will be known only to Sender and no one else will be known it, and more ever given this public key, no one able to find out what is a private key. So that is known private key, private means no one known about it,Public key means every one known about it. So public key of Sender, everyone known about it, private key of Recipient, only Recipient known about it, no one else about knowing it.

II. RELATED WORK

We have two types of cryptography one is called symmetric key cryptography or shared key or “secret key”, use the exact same key for both encryption and decryption [2][3] other is called asymmetric key cryptography or public key private key cryptography.

Some famous and well known symmetric algorithms includes Data Encryption Standard (DES)[4][5], Triple Data Encryption Standard TDES or 3DES [6], Blowfish [7][19], CAST5 [8][20], IDEA (International Data Encryption Algorithm) [9], Tiny Encryption Algorithm (TEA) [10], Advanced Encryption Standard (AES) [7, 8, 12, 13, 14, 15, 23], Twofish [11] [12], Rivest Cipher RC4,RC5,RC6, Serpent and MARS.

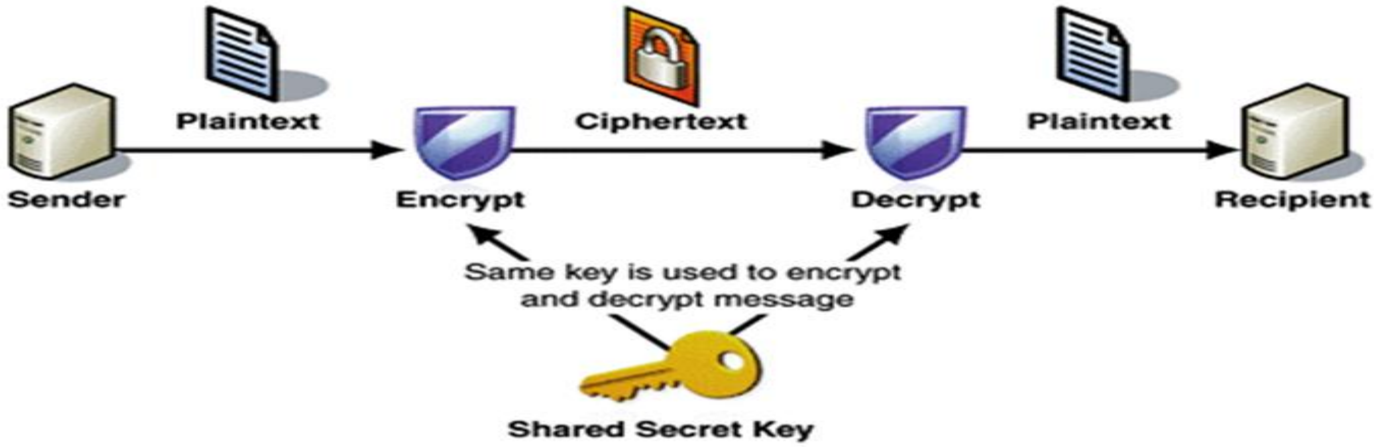

Figure1: Symmetric Key Cryptography

Table 1: Merits & Demerits of Symmetric Key Cryptography

Merits of Symmetric Encryption	Demerits of Symmetric Encryption
✓ Mathematical computation faster due to easy computational steps	->Security service provide only confidentiality,but do not provide another service like non-repudiation & authentication.
✓ Larger key size is considered very difficult to break; smaller key size is easy to break.	->each user needs a unique symmetric key,so number of individual key grows geometrically.
✓ Cipher Text and symmetric key value must be delivered to other parties separately.	->Key delivery must be in a secure environment.because sender and recipient use the same key.

Asymmetric key encryption algorithms also known as also known as “public key” cryptography is a form of modern cryptographic in which encryption process and decryption process depend on complex algebraic,algorithmic,numerical theory performed using two different keys, one key is private key and the other is referred to as public key. Some famous and well known asymmetric key encryption algorithms like PGP, with versions using RSA [16][17] and Diffie-Hellman [18], Secure Shell (SSH) provides strong encryption and integrity protection [6],Elliptic Curve Cryptosystem(ECC),Digital Signature Algoritm(DSA)[21], Merkle-Hellman Knapsack,ElGamal.Asymmetric key cryptography uses twopair of keys one is public which means everyone known and private key generated by asymmetricalgorithm for protecting encryption keys and key distribution, and a secret key is generatedby a symmetric algorithm and used for bulk encryption[22].

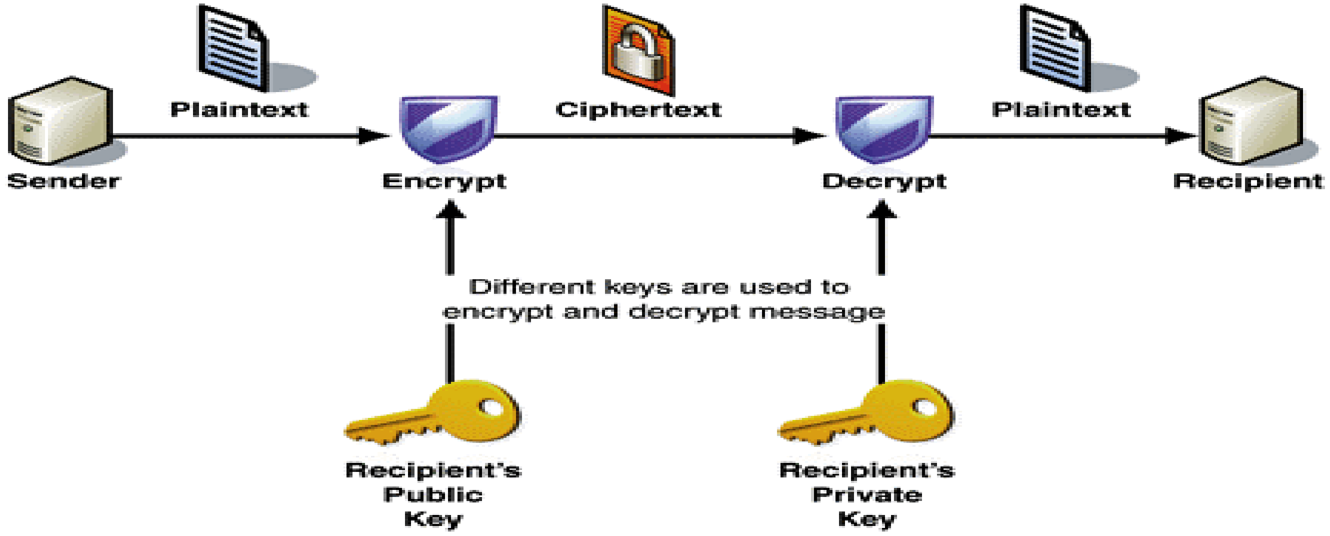

Figure 2: Asymmetric Key Cryptography

Table 2: Merits & Demerits of Asymmetric Key Cryptography

Merits of Asymmetric Encryption	**Demerits of Asymmetric Encryption**
✓ Asymmetric encryption provides Superior key delivery managementthan symmetric key encryption system.	-> Asymmetric encryption performance slower than symmetric key encryption.
✓ Asymmetric encryption provides Superior scalability then symmetric key encryption system.	->Asymmetric encryption performance complex and mathematical operation than symmetric
✓ Asymmetric encryption provides confidentiality, non-repudiation& authentication.	.

III. COMPARISON

Following table presents comparison of different encryption algorithm on the basis of standard parameter:

TABLE III. COMPARISON TABLE FOR DIFFERENT SYMMETRIC KEY ALGORITHMS

Algorithm	**Created by**	**Block Size(bits) or Plain/Cipher Text Length**	**Key Size or Length (bits)**	**Number of Rounds**	**No of S-Boxes**	**Structure**	**Possible Attacks**
DES	IBM and US Government in 1974	64	56	16	8	Feistel network	Brute force Attack,maninthe middle attack
Triple DES	IBM in 1978	64	168	48	8	Feistel network	Sometheoreti -calattacks
IDEA	Xuejia Lai and James Massey	64	128	8	N/A	Substitution-Permutation	Related key
Blowfish	Bruce Schneier in 1993	64	128-448	16	4	Feistel network	Notprone to attacks.
TEA	Roger Needham, Dav id Wheeler in 1994	64	128	64 (32 cycles)	N/A	Feistel network	Related key
CAST5	Carlisle Adams and Sta fford Tavares in 1996	64	40-128	12 – 16	4	Feistel network	-

Serpent	Ross Anderson, Eli Biham, Lars Knudsen	128	128 or 192 or 256	32	8	Feistel network	-
Twofish	Bruce Schneier in 1998	128	128 or 192 or 256	16	4	Feistel network	-
MARS	IBM in 1998	128	128-448	32	1	Feistel network	-
AES	Joan Daemen&Vincent Rijmen in 1998	128	128 or 192 or 256	10 or 12 or 14		Feistel network	Side channel attacks
RC4	Ron Rivest in 1987	Not a block cipher, State size: 2064 bits	40-2048	1	N/A	-	FluhrerMantin and Shamir attack
RC5	Ron Rivest In 1994	32 or 64 or 128	0 to 2040	1-255	N/A	Feistel network	Differential attack
RC6	Ron Rivest In 1998	128	128 or 192 or 256	20	N/A	Feistel network	Brute force Attack

IV. Conclusions

This paper performance analysis of different symmetric encryption algorithms.Survey of each symmetric key encryption.The Algorithm has been presented and comparison shows that some parameter like algorithm key size, block size,number of S-box (Substitution-box), number of rounds are playing important role in achieving the goal of security services provided by Symmetric Cryptography.BLOWFISH performs better and faster encryption speed in comparison with all symmetric key encryption algorithm.

References

[1] SumedhaKaushik&AnkurSinghal "Network Security Using Cryptographic Techniques," International Journal of Advanced Research and Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.18

[2] Dr. PrernaMahajan&AbhishekSachdeva "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

[3] Dr. Prerna Mahajan & AbhishekSachdeva "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

[4] O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "Peformance Analysis Of Data Encryption Algorithms",IEEE Delhi Technological University, India,2011.

[5] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC ,January 1977.

[6] Text Book: Cryptography and network security, Principles and practices by William Stalling, Retrieved on 8 December 2006

[7] Federal Register: September 12, 1997 ,Volume 62, Number 177.

[8] Federal Register: September 14, 1998 ,Volume 63, Number 177.

[9] X. Lai and J. Massey "A proposal for a new block encryption standard", In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.

[10] Wheeler, D.J., & Needham, R.J. (1994), "TEA, a tiny encryption algorithm" In Fast Software Encryption – Proceedings of The 2nd International Workshop,1008

[11] Schneier et al., Twofish: A 128 bit Block Cipher, AES algorithm submission, June 15, 1998

[12] AES home page may be found via http://www.nist.gov/ CryptoToolkit.

[13] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999,

[14] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Report on the Development of the Advanced Encryption Standard (AES), Volume 106 Number 3 May– June 2001

[15] Federal Register: January 2, 1997 ,Volume 62, Number 93

[16] Rivest, R.L., Shamir, A., Adleman, L. "A Method for Obtaining Digtal Signatures and Public Key Cryptosystems," Communications of the ACM, 21, No. 2, 120-126 (1978).

[17] RohitMinni, KaushalSultania, Saurabh Mishra, and Prof Durai Raj Vincent, "An Algorithm to Enhance Security in RSA", *4th ICCCNT 2013*, pp. 1-4, IEEE

[18] Diffie, W. and Hellman,M.E., "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22, No. 6, 644-654 (1976).

[19] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994.

[20] Heys, H.M.; Tavares, E. "On the Security of the CAST Encryption Algorithm", Electrical & Computer Engg.

[21] Rivest, R.L., Shamir, A., Adleman, L. "A Method for Obtaining Digtal Signatures and Public Key Cryptosystems," Communications of the ACM, 21, No. 2, 120-126 (1978).

[22] www.webopedia.com/TERM/S/symmetric_key_cryptography.html

[23] Schneier et al., Twofish: A 128 bit Block Cipher, AES al-gorithm submission, June 15, 1998.