A Survey on Secured Real Time Video Transmission with Significant Improvement in Privacy Preservation

[1] Ms Karishma Chaudhary,[2] Ms Gayatri Pandi(Jain)
[1]Student of Gujarat Technological University,[2] Head and PG Co-ordinator at L. J. Institute Of Engineering & Technology
[1]Department of Computer Engineering,
[1] L. J. Institute of Engineering and Technology, Gujarat Technological University, Ahmedabad, Gujarat, India

***Abstract* -In this era ,Internet and networks applications are growing very fast.With the rapid development of various multimedia technologies thousands of multimedia data are generated and transmitted in the Government Agencies(CID,FBI),research organisation,E-commerce and military fields,so the needs to protect such applications are increased.video encryption algorithms have become an important field of research these days.As an increasing rate of applying video is getting high,the security of video data become more important.Therefore, there is a great demand for secured data storage and transmission techniques.Over the last few years many encryption algorithms have applied to secure real time video transmission. While a large number of multimedia encryption techniques have been proposed and some have been used in real time.In this work, we present a new comparative study between DES,3DES ,AES ,Idea and Blowfish Symmetric encryption Algorithms.**

***Keywords* – Encryption Algorithm ,Decryption,Security,Video Transmission,DES,3DES,AES,Idea,Blowfish**

I. INTRODUCTION

The growing possibilities of modern communications require the special means of confidential and intellectual property protection against unauthorized access and use. Especially these problems are actual for computer networks,which make possible to exchange the large amount of Multimedia data. Multimedia technologies have popularized application like business data transfer, payment of online shopping, video etc. security is very important for multimedia commerce on the Internet.In this era, the communication through multimedia components is on peak. The data like text, images, video and audio is communicated through network.

In modern days cryptography is no longer limited to secure sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. The original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the disguised data so-called ciphertext, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem.

Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data [2] [3]. In the 19th century, a famous theory about the security principle of any encryption system has been proposed by Kerchhoff. This theory has become the most important principle in designing a cryptosystem for researchers and engineers. Kirchhoff observed that the encryption algorithms are supposed to be known to the opponents. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. For even though in the very beginning the opponent doesn't know the algorithm, the encryption system will not be able to protect the ciphertext once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space [3]. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. In encryption, the key is piece of information (value of comprise a large sequence of random bits) which specifies the particular transformation of plaintext to ciphertext, or vice versa during decryption.

Encryption key based on the keyspace, which is the range of the values that can be used to assemble a key. The larger keyspace the more possible keys can be constructed (e.g. today we commonly use key sizes of 128,192,or 256 bit , so the key size of 256 would provide a 2256 keyspace) [3][4]. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Depend on the algorithm, and length of the key, the strength of encryption can be considered. Assume that if the key can be broken in three hours using Pentium 4 processor the cipher consider is not strong at all, but if the key can broken with thousand of multiprocessing systems within a million years, then the cipher is pretty darn strong. There are two encryption/decryption key types: In some of encryptiontechnologies when two end points need to communicate with one another via encryption, they must use the same algorithm, and in the most of the time the same key, and in other encryption technologies, they must use different but related keys for encryption and decryption purposes. Cryptography

algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys)

II.CRYPTOGRAPHY

The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today.

(1)THE PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet [5]. Within the context of any application-to-application communication, there are some specific security requirements, including:

- **Authentication**: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are namebased or address-based, both of which are notoriously weak.)
- **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.
- **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation**: A mechanism to prove that the sender really sent this message.

(2)TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The two types of algorithms that will be discussed are :

A. Symmetric key Algorithms

In symmetric key encryption, the sender and receiver use the same key for encryption and decryption. As shown in figure 1. symmetric key encryption is also called secret key, because both sender and receiver have to keep the key secret and properly protected[11] Basically, the security level of the symmetric keys encryption method is totally depend on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted.

Figure 1: Symmetric key Algorithms

B. Asymmetric key Algorithms

Asymmetric key algorithm is also called public key algorithm. Public Key Cryptography was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. They described a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and address the problem of secret key distribution by using two keys instead of a single key [11]. In public key algorithm there are two keys are used. A public key, which can be known by everyone, and a privet key, which should be kept secret known only by the owner. As shown in figure 2.

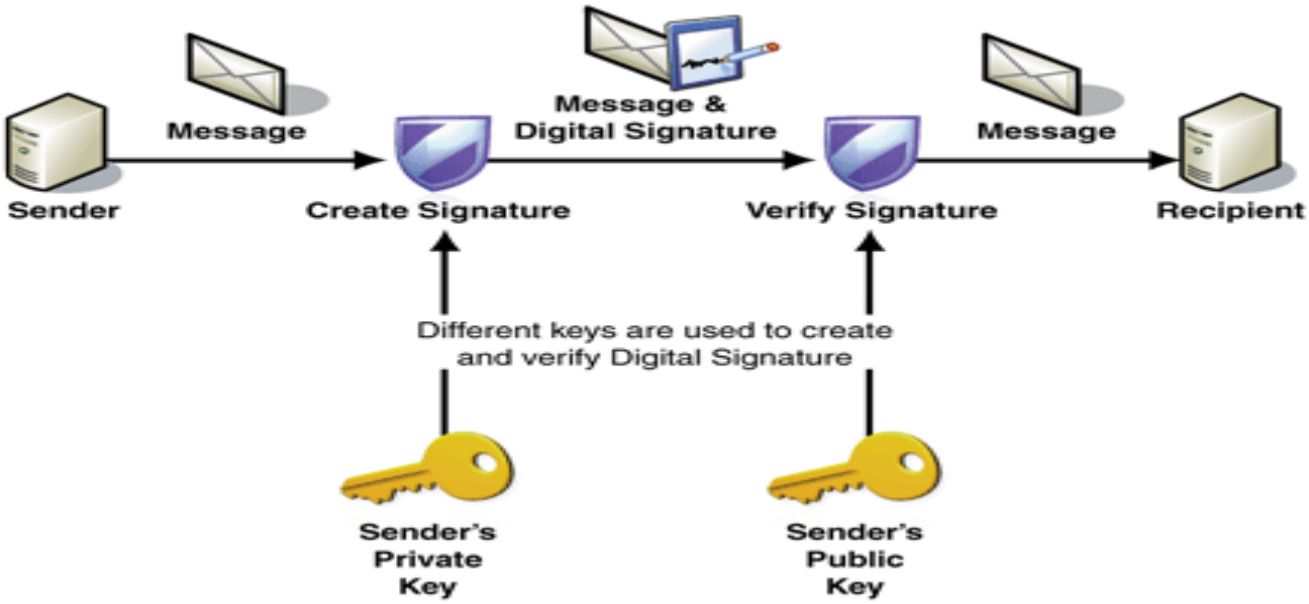

Figure 2: Asymmetric key Algorithms

III SYMMETRIC KEY ALGORITHMS VS. ASYMMETRIC KEY

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Key Exchange	Out-of-band	Symmetric key is encrypted and sent with message; thus, the key is distributed by in-bound means
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	Grows exponentially as users grow	Grows linearly as users grow
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

IV. LITERATURE REVIEW

Studied the impact of an encryption methods and representative video algorithms with respect not only to their encryption speed but also their security level and stream size and Introduces efficient and secure video encryption approach with use of distributed & parallel environment to make secure video encryption feasible for real-time applications without any extra dedicated hardware at receiver side.

Table 1: Comparative Analysis of Symmetric Encryption Algorithms

Features	DES	3DES	AES	IDEA	Blowfish	References
Created By	IBM in 1975	IBM in 1978	Joan Daeman, Vincet Rijmen in 1998	James Massey in 1991	Bruce Schneier in 1998	Stallings [1], Forouzan [16], Schneier [17]
Algorithm Structure	Feistel Network	Feistel Network	Substitution, Permutation Network	Substitution, Permutation Network	Feistel Network	Stallings[1], Schneier [17]
Block size	64 bit	64 bit	128 bit	128 bit	64 bit	Stallings [1],

						Forouzan [16]
Rounds	16	48	10,12,14	8	16	Stallings [1], Schneier [17]
Key length	56 bits	112, 168 bits	128, 192 or 256 bits	64 bits	32 bits to 448 bits	Stallings [1], Forouzan [16], Agrawal et al. [18], technet [25]
Computational Speed	Fast	Moderate	Fast	Fast	Very fast	Jeeva et al. [19] Agrawal et al. [18]
Tunability	No	No	No	No	Yes	Jeeva et al. [19]
Encryption Throughput	Medium	Low	High	High	Very High	Seth et al. [20] Alam et al. [21]
Decryption Throughput	Medium	Low	High	High	Very High	Seth et al. [20] Alam et al. [21]
Power Consumption	Low	High	Medium	Medium	Low	Marwaha et al. [22] Alam et al. [21]
Memory Usage	High	Very High	Medium	Medium	Very low	Seth et al. [20] Mandal et al. [23]
Security against attacks	Brute force	Brute force, Chosen plain text, known plain text	Chosen plain text, known plain text	Linear and differential attack	Dictionary Attack	Jeeva et al. [19] Agrawal et al. [18] Cornwell[24]
Confidentiality	Low	High	High	Very High	Very High	Marwaha et al. [22] Cornwell [24]

V. VIDEO CRYPTOGRAPHY

Video cryptography is consider as like first video convert into the number of frame after that insert some data into each frame and encrypt those frame for the security purpose. Each and every frame transmit over a network. receiver side first decrypt all frame than integrate all frame to generate original video. There are many techniques available for video Encryption for example MPEG video encryption algorithm to generate original video. There are many techniques available for video Encryption for example MPEG video encryption algorithm.

Image and video are the two most basic forms of transmitting information. With the help of Image and video encryption methods any particular set of images or videos can be transmitted without worrying about security.encryption is becoming popular for communication any type of sensitive data. With the increase in the development of multimedia technologies, the multimedia data are transmitted in the various fields like commercial, medical and military fields, which generally include some sensitive data. There are lots of encryption algorithms proposed for the video transmission.

Video encryption techniques can be classified as Naive algorithm, selective algorithm, Zig- Zag algorithm, Video Encryption Algorithm (VEA), and pure permutation [8], [9]. we will review each one briefly in this section.

1 Naive Algorithm

The idea of naive encryption is to deal with the video streams as text data. The sim- plest way to encrypt video streams is to encrypt every byte. So, Naive algorithm encrypts every byte in the whole video stream. Native algorithms guarantee the most security level. However, it is not an applicable solution if the size of the data is big enough. Because of encryption operations, the delay increases and the overhead will not be satisfactory for the real time video encryptions.

2 Selective Algorithm

Tang in [9] suggested encrypting different levels of selective parts of video streams. As video nature is different in its components, he suggested four levels of selective algorithms.

These Four levels are encrypting all headers, encrypting all headers and I frames, encrypting all I frames and all I blocks in P and B frames, and finally encrypting all frames as in Naive algorithm to guarantee the highest security.

3 Zig-ZagAlgorithm

The idea of ZIG-ZAG algorithm is basically encrypting the video streams before compress- ing them. Explicitly, when mapping the 8x8 block to a 1x64 vector each time in the same order. We can use a random permutation to map this transformation of the 8x8 block to the 1x64 vector. Therefore, the concept of the encryption key does not exist in the ZIG- ZAG permutation algorithms. Once the permutation list is known, the algorithm will not be secure any longer [7].

4 Video Encryption Algorithm

Klara and Quia in [10] suggested a new video encryption algorithm called VEA that depends on dividing the video streams into chunks. These chunks are separated into two different lists (odd and even lists). Afterward, applying an encryption algorithm like DES to the even list and the final ciphertext is a concatenation of output of encryption algorithm XOR with the odd list streams.

5 Pure Permutation

The idea of Pure Permutation is simply to apply a permutation technique for the I frames. Both the sender and the receiver have only the correct permutation to encrypt and decrypt the video streams respectively. Later work by Klara [8] proved that it is not secure to use pure permutations.

6 Suggested Technique

In our proposed technique,First of All the video file is converted into a series of frames of equal size. After that each frame should be Encrypted by IDEA Algorithm. The Encrypted frame will be transmit over the network and then Frame Integrating.The frames are then arranged into a sequential manner and the video is constructed from it. Now this video contains the information which gets transmitted along with the transmission of the video file.To get the original videoby using decryption technique.

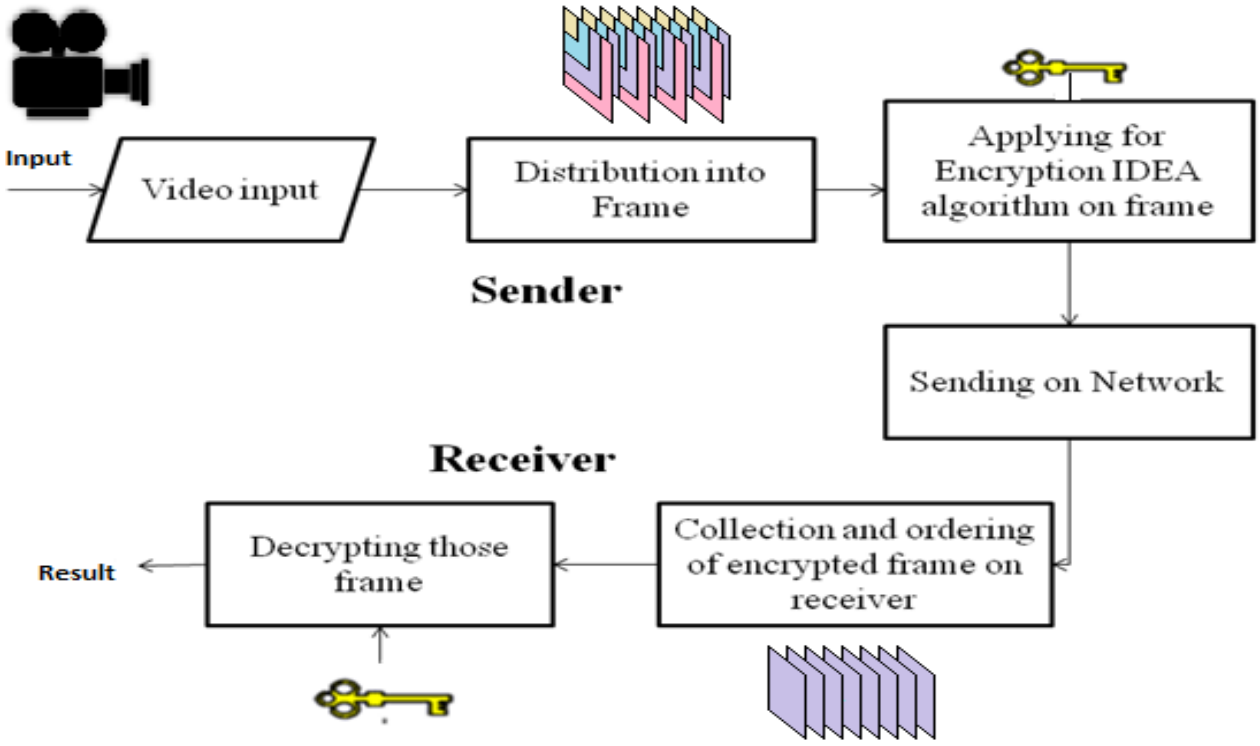

Figure 3. Flow diagram of proposed work

VI.CONCLUSION AND FUTURE ENHANCEMENT

Encryption algorithm plays very important role in communication security. Our research work surveyed the performance of existing Video encryption algorithms. In this paper a new comparative study between DES,3DES ,AES ,Idea and Blowfish were presented into Twelve factors which are Algorithm Structure, Block size, Rounds, Key length, Computational Speed, Tunability, Encryption Throughput , Decryption Throughput, Power Consumption, Memory Usage , Security against attacks, Confidentiality.However, Video Encryption in cryptography many challenges with regard to the characteristics of image. There are several methods by which image can be encrypted, but there are some drawbacks of the existing methods. According to the theoretical analysis, Existing method are not applicable for the real time application.So the proposed work performs better than the existing methods. Different Algorithms are studied and compare both symmetric and asymmetric keys then should be implementing IDEA algorithm in such a way that try to get more secure and fast video transmission.

VII .ACKNOWLEDGMENT

I would like to thank the honorable teachers, fellow students, supportive friends and specially my family. I would also like to say thank to that person who guides me through the way, she continually and persuasively conveys a spirit of adventure in regard to my work Ms. Gayatri Pandi(Jain) mam.

REFERENCES

[1] STALLINGS, WILLIAM, (2007). NETWORK SECURITY ESSENTIALS, APPLICATIONS AND STANDARDS,PEARSON EDUCATION, INCH

[2] Kessler,GaryC.,(1998).AnOverviewofCryptography,availablefrom:http://www.garykessler.net/library/crypto.html#intro. (Accessed july 28, 2015).

[3] B. White, Gregory, (2003). Cisco Security+ Certification: Exam Guide, McGraw-Hill.

[4] shon harris, (2007). SICCP Exam Guide, fourth edition, McGraw-Hall

[5] Heena A. Pandya Haresh A. Suthar, "A Survey On Cryptographically Secured Video Transmission", IJSRD - International Journal for Scientific Research & Development, Vol. 1, Issue 11, 2014 , ISSN (online): 2321-0613,pp. 2508- 2512.

[6] International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013 "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study" By Ajay Kulkarni ,SaurabhKulkarni, KetkiHaridasAniket More Vidyalankar Inst. Of Tech. Mumbai, India.

[7] L. Qiao, Multimedia Security and Copyright Protection, Ph.D. Thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, October, 1998.

[8] L. Qiao, K. Nahrstedt, Comparison of MPEG Encryption Algorithms, International Journal on Computers and Graphics, Special Issue on Data Security in Image Commu- nication and Network, vol. 22, num. 3, Permagon Publisher, 1998.

[9] L. Tang, Methods for Encrypting and Decrypting MPEG Vedio Data Efficiently, pro-ceeding of fouth ACM international multimedia conference 96, page 219-230, Boston, MA, Nov. 1996

[10] L. Qiao, K. Nahrstedt, A New Algorithm for MPEG Video Encryption, in Proc. of International Conference on Imaging Science, Systems, and Technology (CISST'97), pp. 21-29, Las Vegas, NV, June, 1997.

[11] M. Abomhara, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques",IACSIT, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201,PP.103-110.

[12] Narender Tyagi Anita Ganpati , "Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Science and Software Engineering, Volume 4, Issue 8, August 2014, ISSN: 2277 128X,pp.348-354.

[13] Metaliya Viral G, Deepak Kumar Jain, Sardhara Ravin, "A Real Time Approach for Secure Text Transmission Using Video Cryptography", 2014 Fourth International Conference on Communication Systems and Network Technologies,IEEE,Conference Location :Bhopal, DOI:10.1109/CSNT.2014.133, Print ISBN:978-1-4799-3069-2, INSPEC Accession Number:14348660, pp.635 – 638

[14] Yansong Jennifer Ren, Lawrence O'Gorman, Fangzhe Chang, Thomas L. Wood, and John R. Zhang"Authenticating Lossy Surveillance Video", Information Forensics and Security, IEEE Transactions , Date of Publication :23 August 2013, Date of Current Version :10 September 2013, Issue Date :Oct. 2013, Sponsored by :IEEE Signal Processing Society, ISSN:1556-6013, INSPEC Accession Number:13747543, DOI:10.1109/TIFS.2013.2279542, pp.1678-1687

[15] Xiaochun Cao, Na Liu, Ling Du, Chao Li, "PRESERVING PRIVACY FOR VIDEO SURVEILLANCE VIA VISUAL CRYPTOGRAPHY" , Signal and Information Processing (ChinaSIP), 2014 IEEE China Summit & International Conference, Conference Location :Xi'an, DOI:10.1109/ChinaSIP.2014.6889315, Print ISBN:978-1-4799-5401-8, INSPEC Accession Number:14563468, Date of Conference:9-13 July 2014, pp.607 - 610

[16] Forouzan Behrouz A., "Data Communications & Networking", Fourth Edition, 2008, New York: Tata McGraw- Hill.

[17] Schneier B., "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

[18] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[19] Jeeva AL, Palanisamy, Dr. V., Kanagaram K. "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms ", International Journal of Engineering Research and Applications(IJERA), Volume 2, Issue 3, May-June 2012, pp. 3033-3037.

[20] Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[21] Alam Md Imran, Khan Mohammad Rafeek. "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[22] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.

[23] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[24] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State university, Columbus, GA, 2010.

WEB REFERENCES

[25] technet.microsoft.com/en-us/library/cc961628.aspx 18-10-2015 10.12AM
[26] https://www.google.co.in/search?q=symmetric+key+figure&biw=1366&bih=643&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMIx-C2z6bEyAIVCx6OCh1QOQKA#imgrc=oVOIxSlnkeqQGM%3A 12-10-2015 11AM
[27] https://www.google.co.in/search?q=symmetric+key+figure&biw=1366&bih=643&source=lnms&tbm=isch&sa=X&ved=0%20CAYQ_AUoAWoVChMIxC2z6bEyAIVCx6OCh1QOQKA#imgdii=6WP4n5Yy7wZpyM%3A%3B6WP4n5Yy7WzpyM%3A%3Bg3IOx59sh3OUqM%3A&imgrc=6WP4n5Yy7wZpyM%3A 15-10-2015 13 PM
[28] https://www.google.co.in/search?q=symmetric+key+figure&biw=1366&bih=643&tbm=isch&source=lnms&sa=X&ved=0CAcQ_AUoAWoVChMIzfvEs5vLyAIVSAOOCh23TgXV&dpr=1#tbm=isch&q=symmetric+vs+asymmetric+difference&imgrc=eJfFkLzENT01_M%3A 18-10-2015 10.18AM