OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A Comparative Study of Hybrid Cryptographic Algorithms

Bhavik Rana[1], Sunil Wankhade[2]
P. G. Student, Dept. Of Computer Engineering, Rajiv Gandhi Institute Of Technology, Mumbai, India[1]
Professor, Dept. Of Computer Engineering, Rajiv Gandhi Institute Of Technology, Mumbai, India[2]

ABSTRACT: *Internet is a public-interacted system; the amount of information exchanged over the internet is not safe. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. Cryptographic algorithms are needed to secure the information over the internet. These algorithms are used to provide information Security. In the proposed system three major cryptographic algorithms like Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advance Encryption Standard (AES) are combined together to provide Security to the message. The algorithms mentioned here use the concept of symmetric-key cryptography.*
Keywords: *AES,Cryptography, DES, IDEA, Symmetric-key*

I. INTRODUCTION

Transmission of data over the internet is very risky these days as there are many attackers present on the internet. The confidential data that is passed on network is will not be secret if attacker can see this data and hence it is available for all those who are present on network. This means data sent on internet is not at all secure. This means data doesn't remain confidential, it violates integrity and is available to all. This means the main security goals are not achieved. For achieving this goals we secure the message using the term cryptography. The word "crypto" means "hidden" and "graphy" means "to write". Cryptography is used to achieve all the security goals as the plaintext is not available to anyone until he/she knows the key. This means data is confidential, it is integrated and only available for those who knows the key.

There are many cryptographic algorithms present over the internet to secure the message. Algorithms can be Symmetric-key (Secret key) algorithm or Asymmetric-key Algorithm. Symmetric-key algorithm uses single key for encryption and decryption of the data. Symmetric-key cryptography is also called Private-key cryptography as the key used for encryption and decryption is kept private. Asymmetric-key algorithm used two different keys i.e. private key and public key for encrypting and decrypting data. Asymmetric-key cryptography is also called as Public-key cryptography as the key used for encrypting the data is kept public while the key used for decrypting data is private.

To accomplish encryption, most secret key algorithms use two main techniques knownas substitution and permutation. Substitution is simply a mapping of one value toanother whereas permutation is a reordering of the bit positions for each of the inputs.These techniques are used a number of times in iterations called rounds. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is alsointroduced into the encryption so that decryption will be computationally infeasiblewithout the secret key. This is achieved with the use of S-boxes which are basicallynon-linear substitution tables where either the output is smaller than the input or viceversa.The main standard for encrypting data was a symmetric algorithm known as the DES [1].DES is a 64-bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted. The key size DES algorithm is 64-bits out of which 56-bits are used as key while other 8-bits are used for parity checking purpose.

The other symmetric-key cryptography algorithm is IDEA. IDEA is considered as one of the strongest cryptographic algorithm [2]. Although it is quite stronger, IDEA is not as popular as DES for two primary reasons: a) ItispatentedunlikeDESandthereforemustbelicensedbeforeitcanbeusedincommercial applications, b) DES has a longhistoryascompared toIDEA.IDEAisblockcipher.LikeDES,italsoworkson64-bit plaintextblock.Thekey islongerandconsistsof128bits.IDEAisreversiblelikeDES,thatis,samealgorithmisusedfor encryptionand decryption.IDEA uses both diffusion andconfusionfor encryption. The most powerful symmetric-key cryptography algorithm is AES. Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need

not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is nota Feistel structure. Recall that in a Feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128-bit key. This description of the AES algorithm therefore describes this particular implementation. Rijndael was designed to have the following characteristics: a) Resistance against all known attacks, b) Speed and code compactness on a wide range of platforms, c) Design Simplicity.

There are also some of the hybrid algorithms that combine two Symmetric-key Algorithms like DES and IDEA, DES and AES or combination of one Symmetric-key Algorithm and one Asymmetric-key Algorithm like simple Symmetric-key algorithm and Rivest-Shamir-Adleman (RSA) algorithm. These hybrid algorithms can be used for encryption and decryption of string, a normal file or an image file. The main objective of this paper is to understand various hybrid algorithm combinations used for encryption and decryption. Some hybrid algorithms were used for security of digital motion image [4], while some were used for data security [5].

In this paper, we describe the different hybrid cryptographic algorithms. We also provide an analysis of these algorithms. The rest of the paper is organized into 4 sections. Section 2 gives summary of algorithms used by different researchers for their research. Section 3 discusses the analysisof algorithm based on previous work that the researcher can choose for his research. Finally, conclusion will be presented in section 4.

II. LITERATUREREVIEW

There are many different combinations possible to create a hybrid cryptographic algorithms. The combination can be of either two symmetric-key cryptographic algorithms or else one symmetric-key and other asymmetric-key cryptographic algorithms is possible. Different combination of algorithms is shown in table 1 that are implemented by different researchers.

Table 1: Different Hybrid Cryptographic Algorithms

Contributed by	Research Paper Title	Algorithms Used	Mathematical Representation of Hybrid Algorithm Concept	Characteristics
M.B. Vishnu et. al. [4]	Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm	AES, DES	Ln = Rn-1 Rn = AES (Ln-1 XOR f(Rn-l, Kn))	a. It takes input as 256-bits for plaintext. b. It gives output as 256-bits ciphertext.
Jigar Chauhan et. al. [5]	Enhancing Data Security by using Hybrid Cryptographic Algorithm	AES, DES	L1 =f (R0) R1 =AES (f (L0) XOR f (R0))	a. It takes input as 256-bits for plaintext. b. It gives output as 1088-bits ciphertext.
P.G. Gopika et. al. [6]	Hybrid AES Algorithm Using 16 Feistel Based Network with Distinct Keys	AES, DES	Ln = Rn-1 Rn = AES (Ln-1 XOR Rn-1 XOR Kn)	a. It takes input as 256-bits for plaintext. b. It gives output as 256-bits ciphertext.
Anurhea Dutta et. al. [7]	Hybrid AES-DES Block Cipher: Implementation using Xilinx ISE 9.1i	AES, DES	Ln = Rn-1 Rn = AES (Ln-1 XOR Rn-1 XOR Kn)	a. It takes input as 256-bits for plaintext. b. It gives output as 256-bits ciphertext.
Wang Tianfu, K. Ramesh Babu [8]	Design of a Hybrid Cryptographic Algorithm	AES, DES	-	a. The input size is not mentioned as the bits are passed alternately to different algorithms. b. The ciphertext size is similar to

				that of input size of plaintext.
Jignesh R Patel et. al. [9]	Hybrid Security Algorithms for Data Transmission using AES-DES	AES, DES	-	a. It takes input as 128-bits for plaintext. b. It gives output as 128-bits ciphertext.
Mr. Mahavir Jain, Mr. Arpit Agrawal [10]	Implementation of Hybrid Cryptography Algorithm	DES, IDEA	-	a. It takes input as 64-bits for plaintext. b. It gives output as 64-bits ciphertext.

Cryptographic algorithms are used to provide the security to the message. But using the single cryptographic algorithm has its own drawback. Combining this cryptographic algorithm gives more security. We now discuss how different researchers used this combination to provide the security over internet.

M.B. Vishnu et. al. [4] suggested the combination of the two symmetric-key cryptographic algorithms i.e. Combining DES and AES for securing digital motion image. They presented the design and implementation of symmetrical hybrid based 128-bit key AE-DES algorithm.The idea of a hybrid based AES-DES can be construed with reference to basic DES Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the Feistel network, which in the case of DES was standardized at 16.The main idea about the algorithm is shown in Fig. 1.

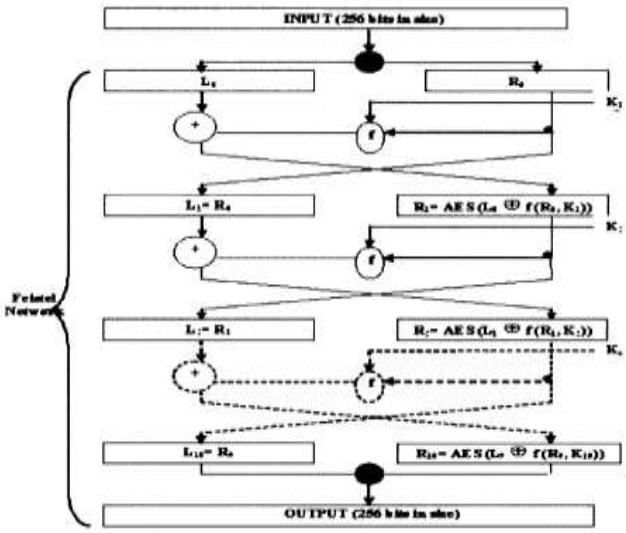

Figure 1: Hybrid AES-DES [4].

Jigar Chauhan et. al. [5] suggested the same combination of algorithms for providing data security. They presented the design and implementation of symmetrical hybrid based 128-bit key AES-DES algorithm for security enhancement. The idea of a hybrid based AES-DES can be construed with reference to basic DES Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the Feistel network, which in the case of DES was standardized at 16.

P.G. Gopika et. al. [6] suggested the hybrid AES algorithm which make use of AES with Feistel network and distinct keys. They proposed 16 rounds for AES-128. Their algorithm used AES key generation method for standard AES 128 and a predefined key for Feistel network. The basic idea of the hybrid AES using Feistel based network with distinct key is to integrate AES into each iteration of the Feistel network of DES.

Anurhea Dutta et. al. [7]suggested a system the combines AES-DES which is implemented in in VHDL using Xilinx ISE 9.1i platform and targeted on a XILINX XC3S400 based FPGA technology. They used the AES-128 for a block of 256-bit plaintext. The basic idea of the proposed hybrid model is to integrate AES into each iteration of the fiestal network of DES.

Wang Tianfu, and K. Ramesh Babu [8] hasused the combination of AES-DES algorithm but in different way. The alternatebits of plaintext were passed to alternate AES or DES block for example, if the size of plaintext is 87-bits, the first bit goes to AESblock while the next bit goes to DES block. This hybrid algorithm is designed for better security by combinations of AES and DES. The highlight of algorithm is shown in Fig. 2.

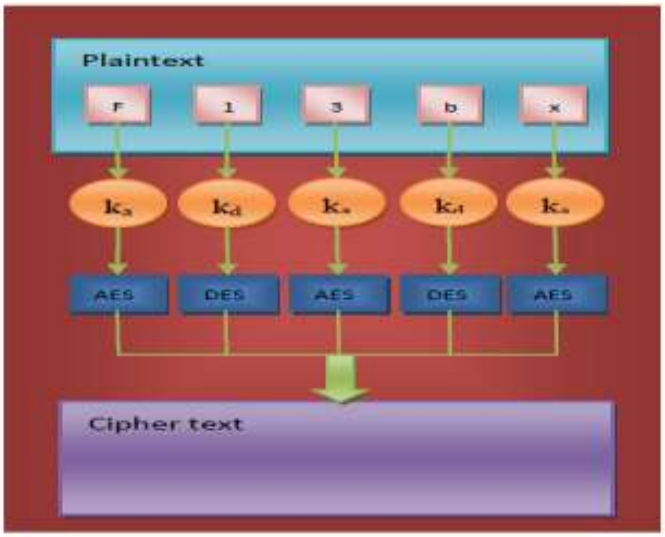

Figure 2: Hybrid algorithm overall structure [8]

Jignesh R Patel et. al. [9]also used the combination of AES-DES algorithms but slightly in different manner. They took 128-bit plaintext, divided plaintext into two halves 64-bit each, then passed both the 64-bit plaintext to two different DES block and after getting the two ciphertext block, they combined it to get128-bit block which was then passed to AES.

Mr. Mahavir Jain,andMr. Arpit Agrawal [10] Suggested something different than the above algorithms. They Combined DES-IDEA to create hybrid algorithm.It is a design for transfer data with better security. The algorithm workflow is shown in Fig. 3.

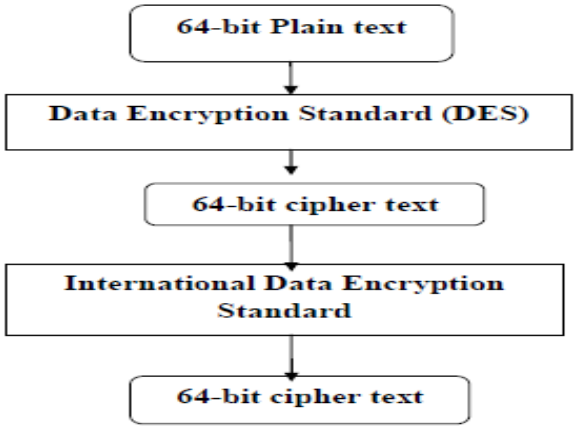

Figure 3: various stages of Hybrid cryptography algorithm [10].

III. ANALYSIS OFDIFFERENTHYBRID ALGORITHMS

The algorithms used for creating hybrid algorithms are symmetric-key algorithms. This means that all the algorithms use a single key for encryption and decryption process. That means if hybrid algorithm is combination of AES-DES than one key will be used for DES and one key will be used for AES and the same key is kept secret between sender and receiver for encryption and decryption process. These hybrid algorithms are designed for providing better security of data over internet. The main advantage of hybrid algorithm is it overcomes the drawback of single working algorithm. This paper concentrates on how different researchers used different techniques to create their hybrid algorithm which than helps to provide more security to the data.

The hybrid algorithms described above by different researchers are convenient in their own ways. All the algorithms provide a better way for securing data over the network. Most the AES-DES hybrid algorithm are almost similar in way and working with only difference that some of them are used for securing digital motion image while others are used for securing data, string or file. All the hybrid algorithms are time convenient and are very much secure. As AES is considered the most secure algorithm over the network in cryptography, combining this algorithm with DES makes it more secure. Also, IDEA is also considered the strongest securing algorithm, combining it with DES also gives a higher level of security. This is because the time taken for attacking this algorithm is addition of time taken to attack key of 1st algorithm and time taken to attack key of 2nd algorithm. Considering this all hybrid algorithms, combination of DES, IDEA and AES is also possible which will offer more security than combining the two algorithms at a single time.

IV. CONCLUSION

This paper is mostly concerned about how different researchers used the same algorithms but in different way to create their own hybrid cryptographic system. Making a hybrid cryptographic system is efficient as the drawback of one algorithm is overcome by the other algorithm, thus providing better security. The paper compares the different combination of algorithms done by different researchers and show how powerful and efficient are they in their own manner. At present, there are many more different algorithms present and can be used in different ways for providing security. But using the hybrid algorithm over an independent algorithm is more beneficial as it gives stronger results. The researchers can try more different combinations of algorithm which can have either both symmetric-key algorithm or one symmetric-key and one asymmetric-key algorithm. The paper concentrates on how the data can be more secured using more new hybrid algorithms over the internet.

REFERENCES

[1]. DES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdfIDEA.pdf [online]. Available FTP:

[2]. ftp://180.211.120.110/04%20IT%20Department/RNK/SE/International%20Data%20Encryption%20Algorithm.pdf

[3]. AES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[4]. M.B. Vishnu, S.K. Tiong, Member IEEE, M. Zaini, Member IEEE, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", in Proceedings of APCC2008 copyright © 2008 IEICE 08 SB 0083

[5]. Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, "Enhancing Data Security by using Hybrid Cryptographic Algorithm", in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[6]. P.G. Gopika, N. Hariharan and S. Perumal Sankar, "Hybrid AES Algorithm Using 16 Fiestel Based Network with Distinct Keys", in Middle-East Journal of Scientific Research 24 (4): 1325-1329, 2016, ISSN 1990-9233 © IDOSI Publications, 2016. DOI: 10.5829/idosi.mejsr.2016.24.04.23301

[7]. Anurhea Dutta, Prerna Bharti, Swati Agrawal, Surekha K S, "Hybrid AES-DES Block Cipher:Implementation using Xilinx ISE 9.1i", in UACEE International Journal of Advancements in Electronics and Electrical Engineering Volume 1: Issue 2[ISSN: 2319 – 7498]

[8]. Wang Tianfu, K. Ramesh Babu, "Design of a Hybrid Cryptographic Algorithm", in International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283 277 ISSN:2249-5789

[9]. Jignesh R Patel, Rajesh S. Bansode, Vikas Kaul, "Hybrid Security Algorithms for Data Transmission using AES-DES", in International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.2, February 2012

[10]. Mr. Mahavir Jain,Mr. Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", in International Journal of Core Engineering & Management(IJCEM) Volume 1, Issue 3, June 2014