IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Novel Technique for Secure Communication in Cryptography

Pooja Bhadauriya[1], Foram Suthar[2], Sumit Chaudhary[3]

Student, Computer engineering, IIST, Ahmedabad, India [1]

Assistant Professor, Computer engineering, IIST, Ahmedabad, India [2]

HOD, Computer engineering, IIST, Ahmedabad, India [3]

Abstract: Securing the information from attackers is very important key aspect in today's life. Many cryptographies algorithms are used in data transmission security. Many encryption algorithm like AES, DES, and RSA etc. have been proposed by researchers. Nowadays so many cryptography attacks are there so, we need to improve security level of algorithm which will also make algorithm complex .key is a very important factor in security algorithm. Two types of keys are available in cryptography 1. Symmetric key 2. Asymmetric key. In this paper we have proposed a new key algorithm of 128 bits which enhance the security level. It is combination of AES, DES and IDEA algorithm.

Keywords: AES, DES, IDEA, Encryption.

1. INTRODUCTION

There are many types of research are currently done over the encryption and description algorithm for security purpose. There are a large number of clients who regularly create, what's more, trade extensive volumes of data in different fields. Every one of these applications requires an uncommon treatment from the security perspective. So here comes the need of usage of cryptography systems which are pertinent. For secure information transmission cryptography dependably plays the vital part. The requirement for ensuring information correspondence prompted to an improvement of a few cryptographic calculations.In this research paper, I am combining three different types of algorithm to provide the best security during the transition. These algorithms are AES, DES, and idea respectively. As all know AES work on the 128 bits, Idea and DES both are work on 64 bits. So how the overall procedure to convert a message into corresponding bit section I determined using new architecture despite in this research paper. The research paper mainly includes the new algorithm that provides more security during the transition which can be represented as the combination of the all above maintained algorithms and provide the new architecture for how actually overall work or process carried out during the transition. For more security first, we take k1 and k2 64-bit using random key generation. We apply DES algorithm on k1 and IDEA algorithm on k2. After applying algorithm we adding both the bit generate 128-bit as k3. Then apply AES algorithm on k3 for applying more security.

2. LITERATURE REVIEW

In "Comparative Study of AES, Blowfish, CAST-128 And DES Encryption Algorithm"[4] Author have proposed reasonable comparison between four most basic symmetric key cryptography calculations: AES, DES, CAST 128 and Blowfish. The comparison takes over the conduct and the execution of the algorithm when distinctive information load is utilized as the fundamental worry here is to concentrate the execution of the calculations under various settings. The comparison is made on the basis of these parameters: speed, piece size, and key size. This paper expects to analyse the Avalanche Effect and integrity checking utilizing ECB and CBC method of the diverse calculations: Blowfish, Cast-128, DES and AES for one-bit change in key and one bit changed in the cipher text. Crypto tool will be utilized for implementing the performance analysis for all calculations said above. After the analysis has been led we found that AES gives the best security. The analysis demonstrated that in both modes DES gives strong avalanche affect and AES and Cast 128 gives solid change in term of integrity checking compared and others calculations utilizing ECB and CBC mode.

DES is an execution of a Feistel Cipher. It utilizes 16 round Feistel structure. The block size is 64-bit. However, key length is 64-bit, DES has a successful key length of 56 bits since 8 of the 64 bits of the key are not utilized by the encryption algorithm. One bit in every 8-bit byte of the KEY might be used for mistake location in a key era, conveyance, and capacity. Bits 8, 16, 64 are for use in guaranteeing that every byte is odd equality.

Advanced Encryption Standard, otherwise called the Rijndael calculation is supporting worldwide. AES Algorithm is utilized to monitor Electronic information. The quantity of rounds in AES is variable and relies on upon the length of the key. AES utilizes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds utilizes an alternate 128-bit round key, which is figured from the first AES

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

key. AES is a symmetric piece figure that can encode information squares of 128 bits utilizing symmetric keys.

1. SubBytes Transformation: - It utilizes substitution table which incorporates nonlinear substitution which works on every byte of the state.
2. ShiftRows Transformation: - In Shift Rows step, bytes in each column of the state are moved consistently to one side. The quantity of spots every byte is moved varies for each column. The main column doesn't change.
3. Mix Columns Transformation: - Blend Columns step works on the section level. It is comparable to the duplication of a network at segment level. Every segment of the state I duplicated with the settled polynomial.
4. Add Round Key Transformation: -In Round Key step, the state is combined with round key using XOR operation.
5. Expansion Key: - In AES calculation, the sender and beneficiary are thought about the key. The AES calculation secure, the key can't be resolved any trespasser regardless of the possibility that he knows the plaintext and the figure content. The AES calculation is developing to utilize one of three key sizes. The keys can be 128 bits, .128 bits implies. These are the key sizes which are maintained by AES Encryption. The bigger key secures the encryption. The keys are then extended along a key development routine for use in the AES figure calculation.

In “Introducing an Encryption Algorithm based on IDEA” [7] author have proposed that International Data Encryption Algorithm (IDEA) is one of the encryption calculations that is broadly utilized for security reason. IDEA block cipher operates with 64-bit plain text block and 64-bit cipher text block, and a 128-bit key controls it. The major outline of the calculation is utilizing three diverse algebraic operations: bit-wise Exclusive OR, multiplication modulo, and addition modulo. Having the biggest number of weak keys is one of the drawbacks of IDEA. In addition, a new attack during round six of IDEA’s operations has been detected. In this paper, we propose and depict the new outline and preparatory execution of a more secure encryption calculation in view of IDEA, and it is named DS-IDEA. Expanding the extent of the key from 128 bits to 512 bits will build the unpredictability of the calculation. The calculation's multifaceted nature is expanded by expanding the measure of dissemination (multiplicative added substance obstruct) in a solitary round. It is actualized to give better security to the client's secret key inside the Online Password Management System (OPMS) keeping in mind the end goal to ensure the client's information inside the database from programmers and different types of unauthorized access.

The International Data Encryption Algorithm (IDEA), initially called Improved Proposed Encryption Standard (IPES).IDEA utilizes 52 subkeys, every 16 bits in length. Two are utilized amid each round legitimate, and four are utilized before each round and after the last round. It has eight rounds. Notwithstanding one mainstream email protection innovation known as Pretty Good Privacy (PGP) depends on IDEA. The working of IDEA can be imagined at an expansive level. The 64-bit input plain content block is divided into four bits of plain content, say p1 to p4. Consequently, p1 to p4 are the input the round of the calculation. There are eight rounds. In each round, six–keys are produced from initially key. Each of the sub-key comprises of 16-bits. These six sub-keys are connected to the four information square p1 to p4. In this manner for the first round will have the six keys k1 to k6. For second round will have keys k7 to k12. At last, for the eight rounds will have k43 to k48. The last stride comprises of an Output Transformation, which utilizes only four sub-keys (k49 to k52). The last yield delivers by the Output Transformation step, which is four block of cipher text named c1 to c4. There are combined to form the last 64-bit ciphertext block.

3. PROPOSEDWORK

3.1 flowchart

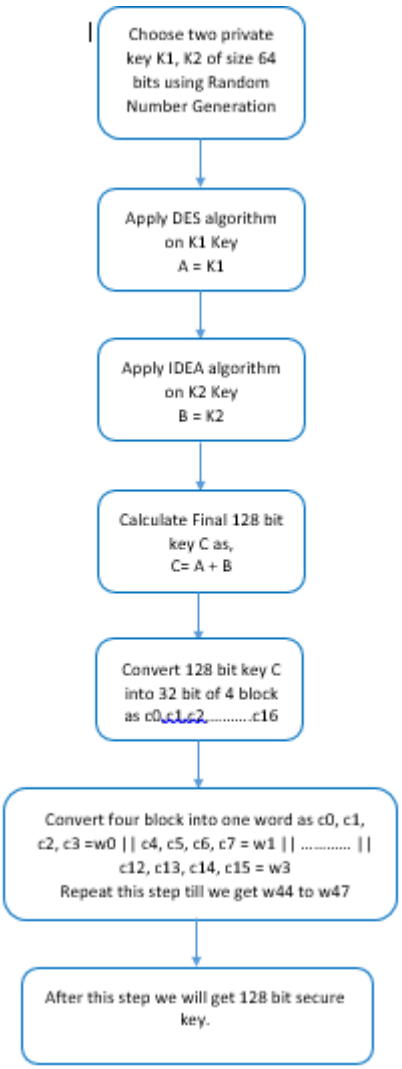

Figure 1Flowchart of Hybrid key algorithm using AES, DES and IDEA

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

3.2 Algorithm

1) Choose two private key K1, K2 of size 64 bits using Random Number Generation Function.
2) Apply DES algorithm on K1 Key A = K1
3) Apply IDEA algorithm on K2 Key B = K2
4) Calculate final 128 bit key Key: A + B
5) Calculate Key Expansion() function

Key expansion function
Key Expansion (byte c[16], word[44])
{
Word temp
For (i=0; i<4; i++)
W[i] =(c [4*i], c [4*i+1], c [4*i+2], c [4*i+3]);
For (i=4; i<44; i++)
{
Temp = w [i-1];
If (I mod 4 = 0)
Temp = Sub Word (Rot Word (temp)) □ Rcon [i/8];
W[i] = w [i-4] □ temp;

g function process

1. Rot Word performs one-byte circular left shifts on a word .ex input word [A0, A1, A2, A3] is transformed into [A1, A2, A3, A0].
2. Sub Word performs a byte substitution on each byte of its input word, using S-box
3. The result of step 1 and step 2 is XORed with a round constant, Rcon[j]

4. CONCLUSION

In this paper, we have proposed a hybrid secure key algorithm which is a combination of DES, AES, IDEA having key size 128 bits. This key algorithm increases security but it will also increase the complexity of an algorithm. Through a combination of algorithms can be applied in a parallel manner or sequential manner to provide more security in the message. We can use this key in any algorithm have key size 128 bits.

REFERENCES

[1] Selent, Douglas. "Advanced encryption standard." Rivier Academic Journal 6.2 (2010): 1-14. Cazier, Joseph A., and B. Dawn Medlin. "Password security: An empirical investigation into e-commerce passwords and their crack times." Information Systems Security 15.6 (2006): 45-55.
[2] Patel, Jignesh R., Rajesh S. Bansode, and Feb Vikas Kaul. "Hybrid Security Algorithms for Data Transmission using AES-DES." International Journal of Applied Information Systems (IJAIS) (2012): 2249-0868.Ye, Peisong, and Guangxue Yue. "Security Research on WEP of WLAN." Proceedings of the Second International Symposium on Networking and Network Security (ISNNS'10) Jinggangshan, PR China. 2010.
[3] Dutta, Anurhea, et al. "Hybrid AES-DES Block Cipher: Implementation using Xilinx ISE 9.1 i."Casey, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.
[4] Nkiama, Maheyzah MD Siraj Herve. "Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm." Structure 4.8: 4. [8] Garber, Lee. "Denial-of-service attacks rip the Internet." IEEE Computer 33.4 (2000): 12-17.
[5] FPGA Implementation of AES Using Splitting Method Barber, Richard. "Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated." Computer Fraud & Security 2001.3 (2001): 9-12.
[6] Karthil, S., and A. Muruganandam. "Data Encryption and Decryption by using Triple DES and performance analysis of crypto system." International Journal of Scientific Engineering and Research (2014): 24-31.
[7] Almasri, Osama, and Hajar Mat Jani. "Introducing an Encryption Algorithm based on IDEA." International Journal of Science and Research (IJSR), India 2.9 (2013).
[8] Singh, Sombir, Sunil K. Maakar, and Dr Sudesh Kumar. "Enhancing the security of DES algorithm using transposition cryptography techniques." International Journal of Advanced Research in Computer Science and Software Engineering 3.6 (2013): 464-471. APA.
[9] Mahajan, Prerna, and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology 13.15 (2013).
[10] Dadhich, Shraddha. "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java."
[11] Patil, S., and B. Varunda. "An Enhancement in International Data Encryption Algorithm for Increasing Security." International Journal of Application or Innovation in Engineering and Management 3.8 (2014): 64-70.

BIOGRAPHIES

Pooja Bhadauriya is pursuing BE in Computer Engineering from IIST, Rajpur, kadi, Gujarat, India. She is currently doing her 8th-semester project in .Net language. Her area of interest is Information and Network Security.

Foram Suthar is working as Assistant Professor in CSE at Indrashil Institute of Science & Technology, Cadila Group, Rajpur, Ahmedabad (Gujarat).She has more than 1 year experience in teaching. She obtained her M-Tech in Computer Science & Engineering (Specialization in Network Technology) with Hons from Nirma University and B-Tech in Computer Engineering from SVBIT (Gujarat Technical University). During this short period of time, She has been worked as Teaching Assistant in Nirma University. She has attended several seminars, workshops at various levels. Her many papers are published in various national journals. Her area of research includes Wireless Sensor Network (WSN), Network Security,Software Testing.

Sumit Chaudhary is working as Head of Department in CSE at Indrashil Institute of Science & Technology, Cadila Group, Rajpur, Ahmedabad (Gujarat). He is pursuing Ph.D. from Uttaranchal University, Dehradun (Uttarakhand). He worked with various institutes like Uttaranchal Institute of Technology (UIT), Dehradun, Shri Ram Group of colleges, Muzaffarnagar (U.P.), IIMT Institute of Engineering & Technology, Meerut (U.P.), INDIA including all that he has more than 7 year experience in

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

teaching. He obtained his M-Tech (Computer Science & Engineering) with Hons from Shobhit University and B-Tech (Computer Science & Engineering) from SCRIET, Meerut (U.P.). During this short period of time, he has been supervised several dissertation of M.Tech students. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes Cloud Computing, Wireless Sensor Network (WSN), Network Security, Neural Network, Artificial Intelligence and MANET (Mobile Ad-Hoc network)..

DOI10.17148/IJARCCE.2017.6374