RESEARCH REVIEW JOURNALS
Volume-03
Issue-11
November -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Multilevel Data Encryption with Compressive Approach Using Asymmetric Key Technique-Survey

[1]Urvi G. Patel & [2]Prof. Pradish Dadhania

[1]Research Scholar, Information Technology Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat (India)
[2]Professor Information Technology Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat (India)

ARTICLE DETAILS

Article History
Published Online: 10 November 2018

Keywords
RSA, AES, Random generators, Multilevel Security

***Corresponding Author**
Email: urvipatel6[at]gmail.com

ABSTRACT

Now a days transferring of texts, documents over the internet are the tasks in common. The transferred text must be cryptographically protected so that cannot be accessed by the invaders. In the communication medium, protected data uses cryptographic techniques and random bit generators. Once the key is generated by the random generators, how well we can secure and transmit fast in the network plays a vital role by applying appropriate algorithm. To fulfill the needs for secure and lightweight data transmission approach, we propose a new Data transmission Technique, which uses compressed bit stream of information as a mean of communications. This technique reduces information loss, and bandwidth requirement. It maximizes the data security as it nullifies information notching, and prevents the attempt of modification by unauthorized third party using multilevel Asymmetric key approach.

1. Introduction

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. Data security is also known as information security (IS) or computer security. Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers. One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical record (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities. Encrypting data prevents unauthorized access to the data. If encrypted data can only be encrypted with a matching key, this can be used to prove sender's identity (i.e. prevents masquerading).Likewise, it can be used to ensure that only intended recipients can use the data.

Plain Text- The original message that is easily readable by humans. It is a term used in cryptography that refers to a message before encryption or after decryption.

Cipher Text- In cryptography, cipher text is data that has been encrypted. This text is unreadable until it has been converted into plain text with a key.

Key- A key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption work on the plain text and at the time of decryption work on the cipher text. The selection of key plays vital rolein cryptography process as the security of encryption algorithm fully depends on it.

2. Related Work

In paper [1] Rakshitha and Prof.Radhakrishna Dodmane proposed a day's transferring the messages over a communication channel needs very much security and on time faster delivery of information. After surveying different methods to secure the data by using algorithm, this technique deals with the hybrid cryptography multilevel encryption and decryption methods by using AES and Fiestel which makes the information to transfer safer and process faster. This system also tried with the different random generator methods during the cryptographic process to have better security and analyzed the results for the different methods. In future, this method is used not only to transfer messages over a communication channel can also adopted to transfer video, audio and confidential images in the medical field in faster and secured way.

In paper [2] Shiladitya Bhattacharjee, Lukman Bin Ab. Rahim, and Izzatdin B A Aziz proposed technique, which is independent of the bit stream. Hence, if some of the bits are modified or lost during the travelling time, it does not significantly impact the original data. This is the main advantage of this approach. As the compression technique reduces the output file in very small size, so the channel overhead will be significantly low. The proposed algorithm is

also time efficient for both data incorporation and retrieval. But due to the high compression there must be lots of statistical similarities exist, which liquefy our proposed security scheme. Our proposed scheme is also not capable to protect complete information loss. So there are some scope to modify our proposed scheme to make it more efficient in terms of security and robustness.

In paper [3] Deepali Bhat , Krithi V , Manjunath KN , Srikanth Prabhu ,and Renuka A. proposed methodology is quite simple to use and efficient in terms of both time as well bandwidth requirement. The stego file which is transmitted is created dynamically and thwarts any frequency based analysis and attacks. The size of the stego file is considerably small and also looks like an ordinary question paper. The use of DES encryption adds to the security as any attack would require the decryption of hidden data using shared key between sender and receiver. Thus, in order to break the security it is required that both the shared symmetric key as well as the steganography algorithm are compromised. This methodology may thus prove to be of good use in applications such as password management systems. One of the possible limitations of the proposed method could be that the increase in the size of the input data will increase the size of the position array used. In addition to this, in order to maintain the simplicity of the proposed methodology, the position array used at the end of each question is embedded as it is work may involve an improvisation where this data can be hidden further without overly increasing the complexity of the embedding process.

In paper [4] Keerthi K and Dr.B.Surendiran proposed method, the characters in the plaintext are converted into ASCII values and the next step is to convert it into HEXADECIMAL. The entire HEXADECIMAL values are grouped based on the input size. The encryption is done in the reverse order of the HEXADECIMAL result in-order to provide security. ECC implementation is more effective compared to RSA for key size and also security. It provide more security with lesser key size. So this can be utilized in electronic devices with lesser memory and lower power consumption. The security in the mapping technique will provide double security for the text encryption. Here we have implemented a secure mapping technique along with less overhead in mapping.ie, is implementation will help to reduce the common look-up table between the sender and the receiver and hence reduce the overhead. So the encryption procedure works faster. One of the major advantage of this method is that we don't have to pad extra bit when the grouped hexadecimal is odd in number. Because the length zero group is taken as NULL.

In paper [5] Er. ManpreetKaur and s Er. Jasjeet Kaur Cryptography plays important role in increasing growth of digital data storage and communication. It is used to achieve the mains of security goals like confidentiality, integrity, authentication, non-repudiation. It is analyzed that in Diffie-Hellman key exchange cryptography algorithm, secret keys are exchanged between two users. Whereas a digital signature is used by receiver in digital signature algorithm to verify that the signal received is not altered. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Many new encryption techniques developing therefore fast and secure standard encryption techniques will always work out with high rate of security.

In paper [6] Cheng Tan, and Qingbing Ji information security system, cryptography has showed its powerful function in data transmission. Consequently, cryptanalysis has been a popular research topic these years. In order to prepare for deciphering work, the identification of cryptographic algorithm is urgent and necessary. In this paper, we present a novel identification system of cryptographic algorithm based on pure ciphertext. Through comparing the experiment results caused by same and different keys for training and testing ciphertexts, we find that the identification of cryptographic algorithm is easy to operate by our identification system when keys keep the same for training and testing ciphertexts. If training and testing ciphertexts are encrypted by different keys, it will be a hard job to identify these cryptographic algorithms. At the same time, we can still obtain a high identification rate for one to one identification associated with AES.

In paper [7] Shangwei Shi, Yining Qi, and Yongfeng Huang proposed model is that such a webpage exists and can be found. We proved that the probability of such a webpage existing is proportional to the size of webpage set under some assumptions and if the secret message is restricted, such a webpage can be found by searching on the Internet. Experimental results show that the proposed method can achieve a capacity of 10.32% at least and 80.98% as typical value. At the same time, the stage message looks like a common URL, so the proposed method has good concealment. As future work, we should develop a high efficient position codec to further improve hiding capacity. And we should study how position information can be added to URL flexibly according to individuality of the webpage behind each URL.

In paper [8] Anup Ashok Patil and Shital Mali In this paper, hybrid cryptographic method is proposed in order to reduce the network overhead in EAACK scheme. Extensive simulation results show the effectiveness of proposed system in terms of network overhead. From obtained result, we can conclude that by adaption of hybrid cryptography there is a significant reduction in the network overhead which is the main aim of this paper. To increase the reliability of this research, testing the performance of EAACK with hybrid cryptography in real time environment is one of the main concerns in future scope.

3. Methodology

a. AES[1]

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

Features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES

- Provide full specification and design details
- Software implementable in C and Java

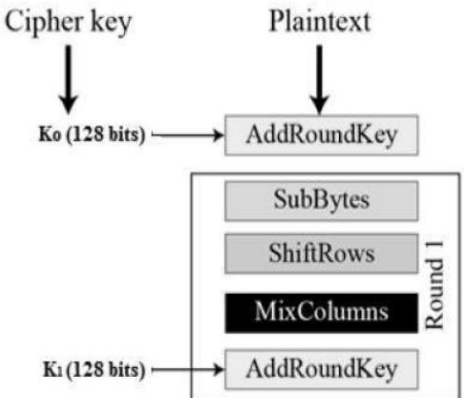

Figure 1: AES Encryption algorithm

i. *Byte Substitution (SubBytes)*

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

ii. *Shiftrows*

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.
-

iii. *MixColumns*

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

iv. *Addroundkey*

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order.

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

b. DES [1]

Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and Final Permutation: The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other.

Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output

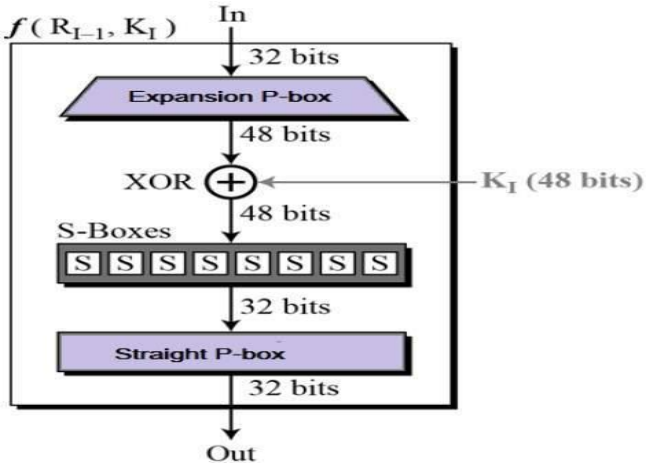

Figure 2: DES Encryption algorithm

Expansion Permutation Box − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits.

Substitution Boxes. − The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

c. RAS[1]

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1) Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2) Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3) To decrypt ciphertext message C, raise it to another power *d* modulo *n*. The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user

4. Comparative Study

Table I. Comparison between Feature Extraction Method

Encryption	Advantages	Disadvantages
DES[1]	For encryption, DES uses the 56-bit key. Besides, there are 256 possible keys, which means a brute force attack will never have any impact.	The 56-bit key size is the biggest defect of DES. Chips to perform one million of DES encrypt or decrypt operations a second are available. DES cracking machine can search the entire key space in about 7 hours.
AES[1]	It uses higher length key sizes such as 128, 192 and 256 bits for encryption. -more robust against hacking. -common security protocol.	It uses too simple algebraic structure. Every block is always encrypted in the same way.
RSA[1]	As computing power increases and more efficient factoring algorithms are discovered, the ability to factor larger and larger numbers also increases. Encryption strength is directly tied to key size.	The user should not worry if public key leak, but need to consider someone takes another's place by counterfeiting published false public key. Complexity of the key creation.

5. Proposed Work

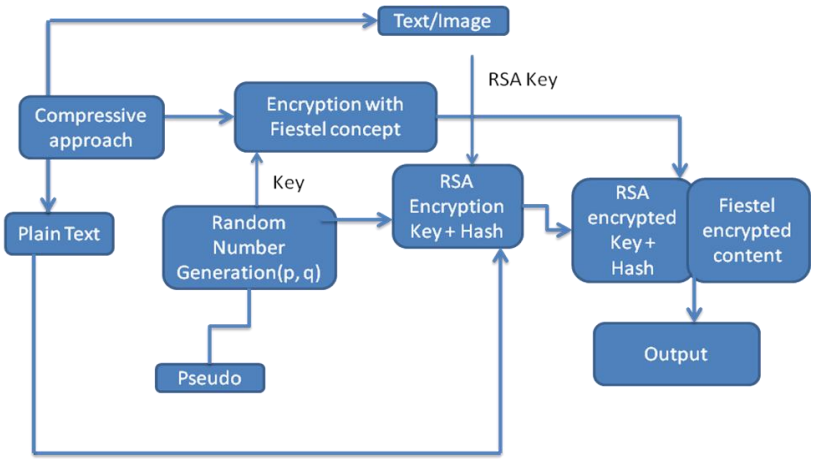

Figure 3: Proposed block

We going to proposed this work.

The basic process in encrypting a 64 bit data with a 56 bit key consist of three main stages An initial Permutation; 16 rounds of a complex key dependent computations; A final permutation, being the inverse of the initial permutation. DES algorithm takes an input of 64-bit long plaintext (or a multiple of 64 bits) data block and 56-bit key (8 bits of parity) and generates output of 64-bit block of cipher text. If the input data was less than or greater than 64 bits, it pad the last block of such input data with some regular pattern of zeros, ones, or alternating ones and zeros, to make it a complete block (64 bit block or a multiple of 64 bits).

The plaintext block was then subjected to an Initial Permutation (IP) to shift the bits around. The 8 parity bits were removed from the key by subjecting the key to its Key Permutation thereby reducing the 64 bit key to 56 bits. After initial permutation, the plaintext and key are processed in 16 rounds of operations giving below; The key was split into two 28-bit halves. Each half of the key was shifted (rotated) by one or two bits, depending on the round.

The halves were recombined and subjected to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key was used to encrypt this round's plaintext block. The rotated key halves from (ii) were used in next round. The data block was splitted into two halves; the left half (LH) and the right half (RH), with both halves having a 32 bit data block. One half (RH) was subjected to an expansion permutation to increase its size to from 32 bits to 48 bits.

The output of step (vi) was XOR with the 48-bit compressed key from (iii) The output of step (vii) was now compressed to reduce the 48-bit block down to 32-bits. The output of step (viii) was XOR with other half (LH) of the data block. The two data halves were swapped and become the next round's input.behind it, as well as for its potential real world applications.

6. Conclusion

This method is used for transfer message over communication to transfer video, audio and confidential information and confidential imaged in the medical field in faster and secure way. In this paper we have compare different methods of encryption with its advantages/disadvantages and finding outs its problems. We have also prepared encryption system with RSA algorithm for future research.

References

1. Anup Ashok Patil, Shital Mali, Hybrid Cryptography Mechanism for securing self-Organized Wireless Networks, IEEE, 2016.
2. Raghav Mathur, Shruti Agarwal, Vishnu Sharma, Solving Security Issues in Mobile Computing using Cryptography Techniques-A Survey, IEEE, 2015.
3. W. Jinwei; L. Guangjie; L. Shiguo, "Security Analysis of Content-Based Watermarking Authentication Framework," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on, vol.1, no., pp.483-487, 18-20 Nov. 2009
4. C. Ning; Z. Jie, "A multipurpose audio watermarking scheme for copyright protection and content authentication," Multimedia and Expo, 2008 IEEE International Conference on, vol., no., pp.221-224,June 23 2008-April 26 2008.
5. P.Bh,D.Chandeavathi , and P .P. Roja,"Encoding and Decoding of a message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method", International Journal on computer science ,vol.02,no.05,pp-1904-1907,2010.
6. F.Amounas and E. H. E. Kinani,"Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography", vol. 1, no. 2, pp. 54-59,2012.
7. S. Mahato, D. K. Yadav and D. A. Khan, "A Novel Approach to Text Steganography Using Font Size of Invisible Space Characters in Microsoft Word Document," in Intelligent Computing, Networking, and Informatics, 2014.
8. S. Roy and M. Manasmita, "A Novel Approach to Format Based Text Steganography," in International Conference on Communication, Computing & Security (ICCCS '11), 2011.
9. Church KW, Hanks P. Word association norms, mutual information, and lexicography. Comput Linguist 1990;16:22–9. Department for a Healthy New York. New York State Confidentiality Law;2013.

