



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.512

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

Design of Encryption Algorithms for Security

Ninad Mate, Rusha Waghmare, Shubham Salunke, Vivek Beluse, Prof. Chanchal Kedia

Department of Computer Engineering, Trinity Academy of Engineering, Pune, India

ABSTRACT: In recent years network security has become an important issue. Encryption has come up as a solution and plays an important role in the information security system. Many techniques are needed to protect the shared data. The present work focuses on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography, user selects via which technique he wants to encrypt/decrypt data. Secondly, by using the decryption technique (as per the user's choice), the receiver can view the original data. Key is sent via Email using steganography.

KEYWORDS: AES, cryptography, steganography, RSA, DES

I. INTRODUCTION

Cryptography is an effective way for protecting sensitive information .it is a method for storing and transmitting data in form that only those it is intended for read and process. The evolution of encryption is moving towards a future of endless possibilities. Stenography is the art of passing information through original files. It is arrived from Greek word meaning "covered writing" [7]. Stenography refers to information or file that has been concealed inside a picture, video or audio file.

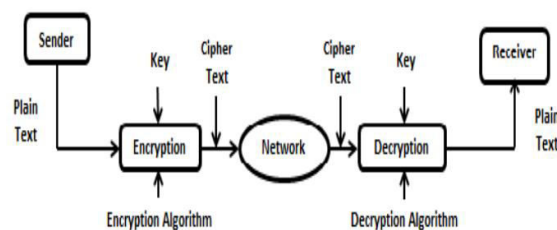


Fig.1. General concept of Cryptography [1]

Some techniques are required for the application of security goals. The two most dominant techniques used today are cryptography and steganography [1]. Two Greek words 'Kryptos' meaning 'secret' and 'Graphein' meaning 'writing' derive the word 'Cryptography'. So Cryptography means 'secret writing', a science of transforming a message into an unintelligible form [3]. The unencrypted message is called 'plain text' and after encryption, it is converted into an unintelligible form which is called 'cipher text' [4]. The cipher text is then sent over an insecure channel with the presence of a third party called adversary or intruder and at the receiving end after decrypting the cipher text again the plain text is found. Fig.1. illustrates the general concept of cryptography using a block diagram.

Cryptography introduces three different types of streams:

- 1) Symmetric-key (Shared secret key) Cryptography
- 2) Asymmetric-key (Public-key) Cryptography
- 3) Hashing

Concepts used in Cryptography [7]

- Plain Text: The original message that the person want to communicate is defined as plain text. For an example, Alice is a person wishes to send "Hai, How are you" message to person Bob, "Hi friend how are u "is referred as plain text.

- Cipher Text: The message which cannot be understood by anyone is defined as cipher text for an example “ib%ipvbufzpv@ “ is a cipher text produced for plain text “Hi, How are you “.
- Encryption: Converting plain text to cipher text is referred as encryption . It requires two processes. Encryption algorithm and a key.
- Decryption: Converting cipher text to plain text is referred as decryption . This may also need two requirements Decryption algorithm and key.
- Key: Combination of numeric or alpha numeric text or special symbol is referred as key .it may use at time of encryption or decryption .key plays a vital role in cryptography because encryption algorithm directly depends on it.

Sometimes to protect data/information, cryptography is not sufficient; it is also required to conceal the existence of the data/information. This process of hiding the existence of data/information is called steganography.

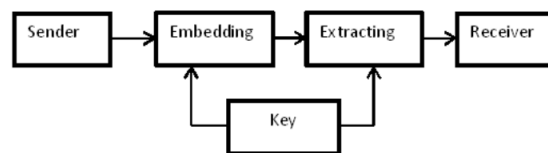


Fig.2. General Concept of Steganography [1]

Steganography is formed from the two Greek words ‘Steganos’ meaning ‘Covered’ and ‘Graphein’ meaning ‘writing’, which refers to ‘Covered Writing’. It is the science of hiding the existence of information into another information [6]. The information is embedded into a cover or carrier object so that no one can understand the presence of information. A key is used for embedding procedure without which the adversary cannot be able to detect the embedded message [1]. The altered new object is called stego object. Image, audio, video etc. can be the cover objects. Fig. 2 shows the general concept of steganography.

II. LITERATURE SURVEY

In [1], hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of message. At the receiving side this digital signature is used for integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method, LSB. Here hybrid cryptography provides a better security, steganography strengthens the security. Message integrity checking is a special feature of this algorithm. Successful simulations have been shown to support the feasibility of this algorithm.

A new hybrid cryptosystems was implemented in [2]. Main objectives of this paper are to emphasize on better performance, maximum speed of an algorithm, checking effectiveness and comparison with other algorithms. In the paper is proposed two new hybrid algorithms using combination of both symmetric and asymmetric cryptographic algorithm such as Twofish, AES, RSA and ElGamal. To analyze results was used JAVA program implementation. The results shows that the proposed hybrid algorithm AES+RSA is significantly secure. However, Twofish + RSA hybrid has other advantages like better computation time, the size of cipher text, and the memory consumption.

A nascent picture mapping method for doing thing was presented in [3] for encoding the message into relative concentration by scramble plain content believer into HEXADECIMAL. The changed over Hex qualities are assembled together to type of framework. Pseudo Random Number Engenderer (PRNG) circuits are basic central of cryptographic structure. These days, the aim of information security has wound up more prevalent than the back, due to the particularly that especially in open system frameworks, there's a potential risk of making fragile information, for

example, military requests, wellbeing records and individual data to interceptor. The enhancement of overwhelming cryptographic plans to arrangement of information security. In the correspondence medium, secured information utilizes identified with ways and working or delivering something of we tried our method for getting things done with various info content sizes. The substance Cover to use to stow away the fragile information was vigorously effectively and did not reveal the closeness of any puzzle code data. It tends to be combination these two cryptographic systems gives a viable answer for information concealing and data transmission through unbound channels. The outcome demonstrates that the proposed sizably voluminous arrangement/format/duplicitous arrangement is inducing a ton with next to no waste and equipped for accomplishing something great/great when contrasted with famous subsisting methods for getting things done.

In [4], comparison of existing RDH, and LSB (with encryption) algorithm is carried out with improved RDH algorithm from two aspects including the security and the peak signal-to-noise ratio (PSNR).

In [5], a 3-layered architecture for securing message sharing mechanism was proposed by using QR code image in one layer. This architecture utilizes the empirical and strategic use of cryptography and steganography techniques. The proposed system provides the higher level of security on the basis of quantitative and qualitative results. Also, we evaluate our system against the performance evaluation criteria discussed in the paper.

In recent era, providing security is more difficult using traditional encryption techniques. To avoid this vulnerability, it is advisable to combine two traditional encryption algorithms. Next, use a Differential Expansion technique to instill an enciphered confidential key into the concealed image. One possible case can be the malicious person is ignorant about the cipher text and the enciphered key. The probability of attack is negligible. On the other hand, if the hacker knows the cipher key then with the help of private key he can get the plaintext image. The algorithm proposed in [6] is robust and provides a better security when compared with other existing algorithms. It will be implemented in MATLAB.

Research work [7] surveyed the existing encryption techniques like AES, DES and RSA algorithms along with LSB substitution technique. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. but RSA consume more encryption time and buffer usage is also very high . we also observed that decryption of AES algorithm is better than other algorithms.

Paper [8] is interested in securing transmission of Meteosat images on the Internet, in public or local networks. To enhance the security of Meteosat transmission in network communication, a hybrid encryption algorithm based on Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms is proposed. AES algorithm is used for data transmission because of its higher efficiency in block encryption and RSA algorithm is used for the encryption of the key of the AES because of its management advantages in key cipher. Our encryption system generates a unique password every new session of encryption. Cryptanalysis and various experiments have been carried out and the results were reported in this paper, which demonstrate the feasibility and flexibility of the proposed scheme.

In the research paper [10] proposed that the different performance factors are discussed such as key value , computational speed and tunability They concluded that AES algorithm is better among Symmetric algorithm and RSA algorithm is found as better solution in asymmetric encryption technique.

III. PROPOSED SYSTEM

In our day by day life day's style we moving starting with one spot then onto the next spot with writings, records over the web are the undertakings in like manner identified with puzzle PC key arrangement of PC guidelines assumes an a major job in a cryptosystem, which secures those touchy and private information. With the extended cryptanalysis,



verifying intuitive media data sight and sound information against variations of assaults against different sorts of ambushes might be a testing work. A security system using cryptographic and steganography technique is proposed in Fig 3. A website is developed using the Django framework allows users to register themselves. After registration, the user login into the portal via user ID and password. The user has been given the option to choose any of the two algorithms for encrypting documents that they uploaded earlier. Cloud (firebase server) saves encrypted files, from where the receiver fetches file. To decrypt the document user needs a key which will be sent to the authorized person via E-mail. Steganography is used to encode keys. In steganography, the secret messages can be hidden in various multimedia files such as text, audio, images, animations, video, etc, in this system we are going to hide our key in an image.

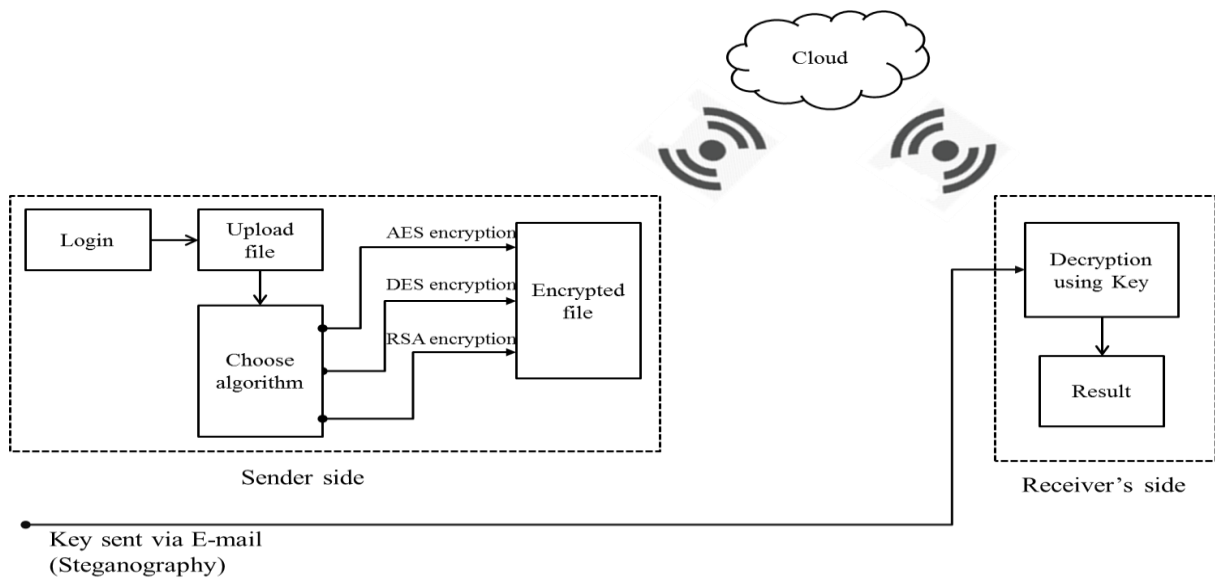


Fig 3 proposed system

AES algorithm

AES (acronym of Advanced Encryption Standard) is a Symmetric encrypt algorithm. AES bits for encrypt/decrypt the data and fortifies lengths are 128,192 and 256 bits.

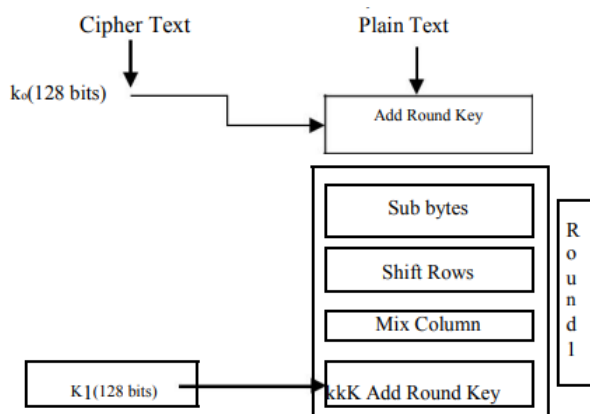


Fig AES Encrypt [3]



- 1) Byte Supersede (Sub Bytes) The 16bit of info information is fine-turned layouts and result in network shapes lines and section.
- 2) Circular byte Shift rows Every four lines of matrix network are moved to left positions for each round other.
- 3) Mix Columns The yield of another framework is store of 16 nascent bytes and in last round this progression in not rehashed.
- 4) 4)Add round key The 16bytes of input matrix and round key and output will stored in cipher text 128 bits and 16 bytes homogenous round of interpreted the data
- 5) Decryption The tasks of decode of an AES cipher text activity in the inconsistency request. All round comprises of the four stage directed in the logical inconsistency request.

RSA

The Rivest-Shamir-Adleman (RSA) algorithm is one of the prominent and reliable public-key encrypt pattern. Cryptographic assessment that are utilized for security accommodations which empowers open key encryption and is broadly utilized to secure touchy information data, concretely over an unreliable network such as the cyber world.

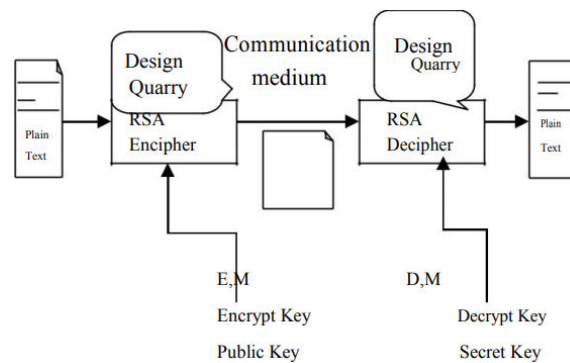


Fig. 6 RSA Encryption [3]

- Step 1: Choice 2 prime number P and Q and P is not equivalent Q.
- Step 2: Intentional N, by accumulate P and Q; $N=P*Q$.
- Step 3: Now, intentional $\phi(n)=(p-1)*(q-1)$.
- Step 4: choice a public key e such that e is not equivalent factor of $\phi(n)$.
- Step 5: choose secret key d such that $(d*e) \text{ mod } \phi(n)=1$.
- Step 6: Intentional C.T(C): $C=M \text{ mod } N$.
- Step 7: Intentional P.T (M): $M=C \text{ dmod } N$.

DES [1] Information Encryption Standard (DES) may be a symmetric-key. DES is a utilization of a Fiestel Idea having a cleared out half that's a culminate reflect image to right half of the correct half. It utilizes 16 circular Fiestel structure. The 64 bit information and key length is 56 bit for scramble information 8 and 64 bit are not utilized. DES is anticipate a head on the Fiestel Cipher, code all that must outline DES is

- Round function
- Key schedule
- Any ads citations processing – Inceptive and eventual organization combination of ordering

Introductory and Last Stage: In to begin with and objective p-boxes are inverses orchestrate of each Circular function. The heart of this cipher is the DES work, f. The DES work petition a 48- bit key to the farthest right 32 bits to cause a

32-bit yield. In cryptography strongly produced the sequenced of cipher. While Fiestel multilevel round divide into cipher for Fiestel network.

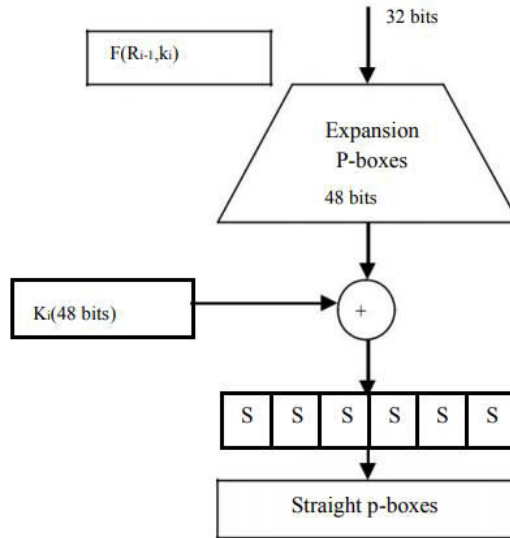


Fig. 7 DES Encrypt [3]

Expansion Permutation Box :Extension Change right input 32bit and circular key is 48 bit fair investigate to right side of input esteem as it were.

Table 1: Comparison between AES, DES and RSA [9]

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm



Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient

IV. CONCLUSION

In this paper both the hybrid cryptography and steganography have been applied, and a stego image has been generated. Here, the message is encrypted using AES, DES or RSA (user’s choice). All these encrypted files, i.e. the encrypted message, encrypted key and the encrypted digest have been combined together to form a complete message. We have used cryptographic algorithm like DES, AES and RSA along with the steganography technique for hiding the document in an image file. Our future work will focus on SLSB which replace LSB technique (steganography technique).

REFERENCES

[1] Biswas, Chitra; Gupta, Udayan Das; Haque, Md. Mokammel (2019). [IEEE 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) - Cox'sBazar, Bangladesh (2019.2.7-2019.2.9)] 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) - An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. , (), 1–5. doi:10.1109/ECACE.2019.8679136

[2] Jintcharadze, Elza; Iavich, Maksim (2020). [IEEE 2020 IEEE East-West Design & Test Symposium (EWDTS) - Varna, Bulgaria (2020.9.4-2020.9.7)] 2020 IEEE East-West Design & Test Symposium (EWDTS) - Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. , (), 1–5. doi:10.1109/ewdts50664.2020.9224901

[3] Patel, Urvi; Dadhania, Pradish (2019). [IEEE 2019 Innovations in Power and Advanced Computing Technologies (i-PACT) - Vellore, India (2019.3.22-2019.3.23)] 2019 Innovations in Power and Advanced Computing Technologies (i-PACT) - Multilevel Data Encryption Using AES and RSA For Image and Textual information Data. , (), 1–5. doi:10.1109/i-PACT44901.2019.8960227

[4] Rashmi, N.; Jyothi, K. (2018). [IEEE 2018 2nd International Conference on Inventive Systems and Control (ICISC) - Coimbatore, India (2018.1.19-2018.1.20)] 2018 2nd International Conference on Inventive Systems and Control (ICISC) - An improved method for reversible data hiding steganography combined with cryptography. , (), 81–84. doi:10.1109/ICISC.2018.8398946



- [5] Mendhe, Abhijeet; Gupta, Deepak Kumar; Sharma, Krishna Pal (2018). [IEEE 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) - Jalandhar, India (2018.12.15-2018.12.17)] 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) - Secure QR-Code Based Message Sharing System Using Cryptography and Steganography. , (), 188–191. doi:10.1109/ICSCCC.2018.8703311
- [6] Mahalakshmi, B.; Deshmukh, Ganesh; Murthy, V.N.L.N (2019). [IEEE 2019 Fifth International Conference on Image Information Processing (ICIIP) - Shimla, India (2019.11.15-2019.11.17)] 2019 Fifth International Conference on Image Information Processing (ICIIP) - Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm. , (), 363–366. doi:10.1109/ICIIP47207.2019.8985665
- [7] B. Padmavathi , S. RanjithaKumari, “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique”, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 4, April 2013
- [8] IBoukhatem Mohammed Tizi-Ouzou, Cherifi Mehdi, “Meteosat Images Encryption based on AES and RSA Algorithms Meteosat Image Encryption”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 6, 2015
- [9] Dr.PrunaMahajan&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 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350
- [10] [1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037
- [11] ShashiMehrotra Seth, Rajan Mishra “Comparative Analysis Of Encryption Algorithms For Data Communication” IJCST Vol. 2, Issue 2, June 2011 I S N : 2 9 - 4 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (O n l i n e) www. i j c s t . c o m
- [12] E.Thamiraja ,G.Ramesh,R.Uma rani “A Survey on Various Most Common Encryption Techniques” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X
- [13] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani “New Comparative Study Between DES, 3DES and AES within Nine Factors” Journal Of Computing, Volume 2, Issue 3, March2010,Issn2151-9617
- [14] Aman Kumar , Dr.SudeshJakhar , Mr. Sunil Makkar “comparative analysis between DES and RSA algorithm” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X



INNO  **SPACE**
SJIF Scientific Journal Impact Factor

**Impact Factor:
7.512**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details