IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

ADVANCED DATA SECURITY USING HYBRIDCRYPTOGRAPHY AND STEGANOGRAPH

[1]MRS. K.SRILATHA
ASSISTANT PROFESSOR
DEPT.OF CSE
TEEGALA KRISHNAREDDYENGINEERING COLLEGE, MEERPET

[2]S.SUJITH KUMAR, [3]AYUSH JOSHIYA, [4]R.SHIVANANDINI
DEPT. OF CSE
TEEGALA KRISHNA REDDY ENGINEERING COLLEGE, MEERPET

ABSTRACT

Maintaining data security is crucial to any successful online presence. With the development of new and advanced technologies, traditional data security methods are becoming less effective in protecting data. Consequently, there is an increasing need for a robust Hybrid Cryptosystem. The efficiency and performance of a hybrid data encryption scheme are investigated in this research. The hybrid crypto-system utilizes a mix of Blowfish, RSA, and AES layers to encrypt data. The system additionally encrypts the keys used and embeds them in an image using LSB Steganography. This study investigates a prospective hybrid-crypto system that may be able to alleviate the disadvantages of present conventional systems.

Keywords: multi-layered Hybrid Cryptosystem, Blowfish, RSA,AES layers to encrypt data, LSB Steganography

1.INTRODUCTION

Apps and services utilize a wide variety of Encryption Algorithms to keep user information safe. But the development of more complex technology is rendering these older methods useless. As hardware has improved, the time needed to crack a cryptosystem has decreased. The suggested system combines three of the most powerful and widely used algorithms for data encryption. Combination of the symmetric AES and Blowfish algorithms with the asymmetric RSA algorithm. RSA is a popular asymmetric encryption method [1] used for more than only data security because to its ability to employ two different keys for encryption and decryption. In contrast, Blowfish and AES are what are known as Symmetric Ciphers since they only need a single key for both encryption and decryption. While Blowfish is the fastest encryption method [2], Advanced Encryption Standard (AES) is the most safe and efficient. When used together, they may overcome the shortcomings of each individual component.

Compared to its individual components, studies found that the AES-Blowfish Hybrid Cryptosystem was more successful at encrypting data [4]. The use of LSB Steganography to store data in image in the system showed that the system was resistant to attacks because the histograms of both the cover and stegoimage were similar [5]. A similar cryptosystem consisting of RSA and AES combination implemented in Java was also studied and found to provide a high level of security and enhanced integrity.

To guarantee key security, the keys are encrypted and stored in an image using steganography, and the method suggested in this research makes use of a layered encryption architecture that encrypts data three times utilizing the three separate algorithms. Password hashes are used to encrypt the keys, with the AES,SHA-1 key being used to produce the hash from the user's entered password. Experimental findings show that the suggested Python-based system is an effective cryptosystem for protecting sensitive information.

2.LITERATURE REVIEW

Knowing and being ready is the first line of defense against cyber dangers and cybercrimes, e.g. with information security training. Two types of training exist, the first of which is designed to help security personnel become more knowledgeable about and adept at countering modern threats. The purpose of this article is to explore the notion of a cyber range, and to include a full examination of literature addressing unclassified cyber ranges and safety test beds [1]. In this study, we construct taxonomy for cyber range systems and assess current research that focuses on design and scenarios, but also capabilities, functions, resources etc. In this study the IoT-based smart grid's dangers and future methods are studied and concentrate on types of cyber threats and include an in-depth of the smart grid's cyber-security environment. We focus on network vulnerabilities, analysis of such vulnerabilities, testing of protective measures, and the need of such measures. We want to shed light on the issues surrounding cyber security in smart grid applications, as well as provide a road map for future cyber security research. This research constructs a model of a V&V process for cyber security controls utilizing adaptive focused testing as the foundation for the solution. Additionally a quantitative technique is established to design and priorities fault-prone information security policies. It has been proven that the model constructed may give an extra and more trustworthy framework for expert subjective assessment [3]. This essay emphasizes on the relevance of distinct cyber defense standards, and cyber security framework design. We address security risks, attacks and cyber security remedies. Then we explore the many difficulties of standardization of cyber security. We also discuss different government techniques in defending cyber security, and the national information security strategy to secure cyberspace. Finally, we have some key rules for information security and information safety [4]. This document addresses the standards necessary for the Federal Government's examination of cyber security policies for the United States Department of Health and Human Services. Compliance with established Federal regulations and standards enables cyber security policies and procedures, whose overarching goal is to protect the operational resources and goals of the United States Department of Health and Human Resources and to encourage best practices of security in the defense of information systems against unauthorized actors and cyber threats [5]. There will be less opportunity for human mistake in the order processing and more efficiency in the delivery of orders thanks to this automation. However, assaults from cyberspace, especially from the Internet, may disrupt that. In this research, we present a new attacker-defender model against an adversary of the quantum response (QR) to secure vital assets by considering the defensive budget and the dependence on characteristics. Each asset's degree of security in the solution represents how much that item should be guarded [6]. In this work, we provide a comprehensive overview of deep learning techniques, along with a detailed comparison of existing methods, current state-of-the-art datasets, and potential future directions in the field of cyber security threat detection. In specifically, we present an overview of intrusion detection systems centered on deep learning methodologies. We identify 35 popular cyber datasets and classify them into seven broad groups based on their function in intrusion detection: network traffic, electric network, internet traffic, virtual private network, android device, internet of things (IoT) traffic, and internet connection [7]. To automatically identify and categorize cyber intrusions at network and host rates in real time, an intrusion detection system (IDS) is often built using machine learning algorithms. There are, however, a number of challenges that arise when dealing with malicious assaults that are both constantly changing and occurring in huge numbers, and so necessitating a scalable response. For researchers in the field of information security, there are a plethora of malware databases available online [8]. The ultimate purpose of this research is to develop automated and efficient methods for learning relevant feature

representations from massive amounts of unlabeled raw network traffic data using deep learning techniques. By layering dilated convolution auto encoders, we present a novel network intrusion model and evaluate it on two new intrusion detection datasets. Multiple studies have shown that our approach is effective [9]. In this study, we investigate the potential of off-line deep learning based NIDSes by building the detection engine with many advanced deep learning models and conducting a quantitative and comparative assessment of these models. We begin by discussing the theoretical implications of deep learning as a generic method for the problem of network intrusion detection. Finally, we evaluate multiple machine learning approaches for two network intrusion detection tasks [10].

3.IMPLEMENTATION OF ALGORITHM

3.1.Blowfish Algorithm

Blowfish is a Symmetric Block Cipher designed in 1993 by B. Schneider. Blowfish algorithm has ablock size of 64 Bits and key lengths varying from 32 to 448 Bits. It is particularly known for its features like complicated key schedules and key-dependents-boxes. Being a

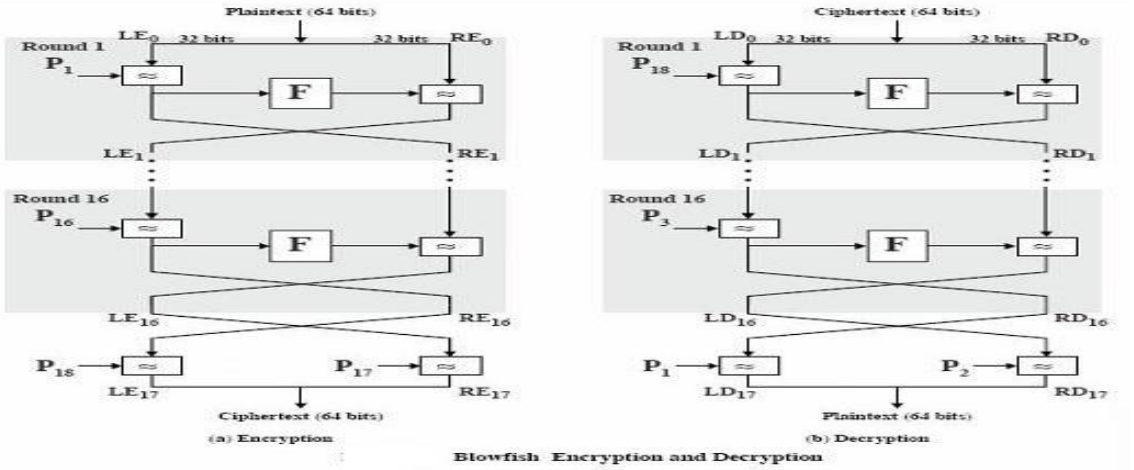


Fig 1.BlowfishAlgorithmEncryptionandDecryption

Feiste lcipher it has16 rounds. Each round of the Blowfish algorithm has four steps.
In the nth round, the left part of the block is XORed with the nth element in the sub key-array followed by passing it to the round function F. The output of function F is XORed with the right half of the initial block and then swapped. The round function F divides the 32-bit input into four 8-bit blocks that are then fed to 4different S-Boxes. The output of the 1st and 2nd s-box is added and the result is XORed with the output from the 3rd s-box and again added to the output of the 4th s-box. It is one of the fastest algorithms for encryption [2].

3.2. AES-AdvancedEncryptionStandard

Rijndael is a Block Cipher developed by Belgian cryptographers, Vincent Rijmen and Joan Daemen that has been established as the Advanced Encryption Standard by the U.S. National Institute of Standards and Technology(NIST)in2001[7].The AES has key lengths of 128,192,256 bits,and10,12,14 rounds respectively. The 128 Bit key is expanded using AES Key Schedule into several sub keys depending on the number of rounds. In the beginning, an Initial Round Key is XORed to the inputblock. Then, for the first N-1 rounds, where N is the number of rounds, 4 Round Functions are applied one ach block. The first-round function is Substitute Bytes where each byte is replaced with another according to a lookup table. Followed by Shift Rows, where the last three rows of the state are shifted cyclic all ya certain number of steps .Mix Columns, a linear mixing operation that operate son the columns of the state, combining the four bytes in each column is applied to the block after Shift Rows. Lastly, Add Round Key where each byte of the state is combined with a byte of the round key using bitwise xor is applied on the block. For the Nth round, i.e the last round all the abovefunctions are applied except the Mixed Columns step [7]. It is one of the most widely used andsecure

encryption algorithms for data security. Even though it is slower than blowfish, it provides a higher level of data security [2]

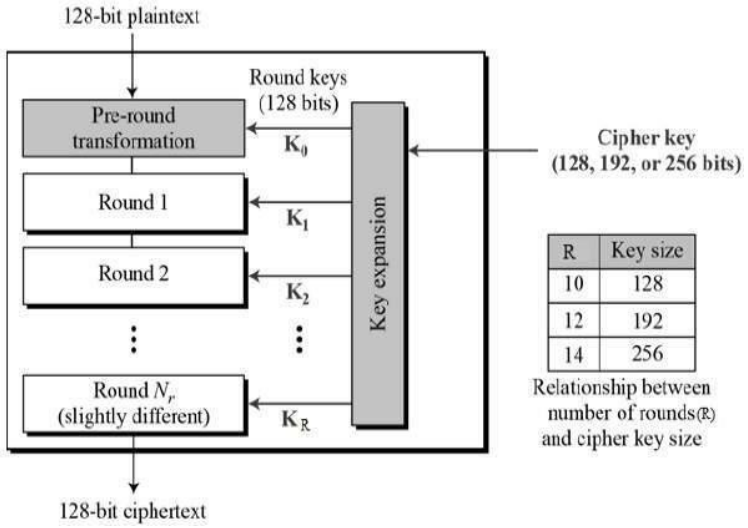


Fig2.AESAlgorithmEncryptionandDecryption

3.3. RSA Algorithm

Rivest–Shamir–Adleman (RSA) Algorithm is an asymmetric cryptographic algorithm that uses a Public Key, available to everyone on the network, to encrypt data and a Private Key, available to only the Sender and Receiver, for decryption. The keys are large prime numbers of lengths 1024/2048/3072/4096 Bits.

Two large prime numbers p and q are selected. The modulus n is calculated as, n=p x q

Euler'sTotient Function of n,φ(n)is such that (n)=(p-1)x(q-1)
The Public key is selected such that e and φ(n) are co-primes. e gcd (e,φ(n))=1
ThePrivateKey,discalculatedsuchthat(dxe)modφ(n)=1
Hence the Public Key pair is (e,n)and the Private Key Pair is(d,n).
Using RSA, encryption of the plain text, Mis done using the Public Key ,e as:

$$\text{Ciphertext, } C = M^e \bmod n$$

The Cipher text,C Is decrypted using the Private Key, as:

$$\text{Plaintext, } M = C^d \bmod n$$

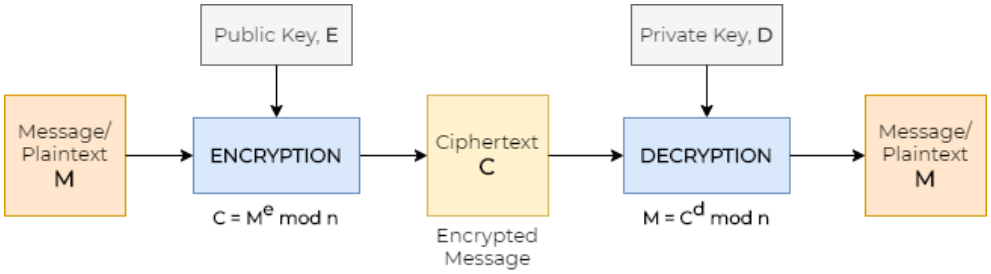


Fig3.RSA Algorithm Encryption and Decryption

3.4.LSB Image Steganography

Least Significant Bit Steganography or LSB Steganography is the method of hiding secret datainside any form of digital media, here, Image. Images are made up of pixels, and the value of each pixel usually refers to the color of that particular pixel. In a gray scale image, these pixel values range from 0-255,0being black and 255 being white. In LSB Image Steganography, changing the last bit value of a pixel won't have much of a visible change in the color. A cover image is used to embedthe data in the Cover Image is converted to greyscale. The message is converted into binary. Each pixel of the image is traversed through, and for each

pixel, initiate temporary variable, temp.If the LSB of the Pixel Value and the message bit is the same, set temp as 0 and set temp as 1 other wise. Update the output image pixel as image pixel value added with the temporary variable value, temp. This is done until the message is completely embedded.

3.5. SHA-1HashingFunction

Secure Hashing Algorithm is a one-way hash function that produces a condensed hash of the message, called the message digest. Any changes made to the message get reflected on to the message digest that is if the message changes the message digest will change. This feature of SHA-1 is useful in the generation and verification of digital signatures, message authentication codes, generation of r and om numbers and bits.[8]

4. DESIGNOF PROPOSED SYSTEM

4.1. Data Encryption using Blowfish, RSA &AES Encryption Algorithms in cascading manner.

The System consists of three Encryption Layers, a Key Generator, and a List of Keys. The KeyGenerator generates the random n-bits Key depending on the Encryption Algorithm, while the List of Keys stores the Key Generated in each layer.

The plaintext P is first Encrypted using the Blowfish Algorithm with a 32 Bit / 64 Bit / 128 Bit Key,$K_{Blowfish}$. The Key $K_{Blowfish}$ is generated by the Key Generator and is used for Blowfish Encryption. It isthenappendedtotheListofKeys,L.ThePlaintext,PisencryptedtogenerateCiphertextC_1.

$$C1 = Blowfish\ (\ Plaintext = P\ ,\ Key = K_{Blowfish}\ )$$

$$L = [\,] \oplus K_{Blowfish}$$

The Ciphertext, C1 is then encrypted using RSA Encryption with the 1024/2048 Bit Public Key, KRSA-Public generated by the Key Generator. A Private Key, $K_{RSA\text{-}Private}$, is also generated for Decryption.While the Public Key is used in Encryption, it is not stored in the List of Keys, L. The Private Keygenerated is appended to the List of Keys. C1 is encrypted to generate Ciphertext C2 .

$$C2 = RSA(\ Plaintext = C1\ ,\ Key = K_{RSA\text{-}Public}\ )$$

$$L = [K_{Blowfish}] \oplus K_{RSA\text{-}Private}$$

The Ciphertext, C2 is then encrypted using AES-128 Encryption with the 128 Bit, KAES generated bythe Key Generator. The Key, KAES generated is appended tothe List of Keys, L. This Step gives the final encrypted cipher text C.

$$Ciphertext,\ C = AES(\ Plaintext = C2\ ,\ Key = K_{AES}\ )$$

$$L = [K_{Blowfish}\ ,\ K_{RSA\text{-}Private}\ ] \oplus K_{AES}$$

The output of the system is the Ciphertext, C, and the list of keys L with all the keys.

$$Ciphertext,\ C$$

$$List\ of\ Keys,\ L = [K_{Blowfish},\ K_{RSA\text{-}Private}\ ,\ K_{AES}\ ]$$

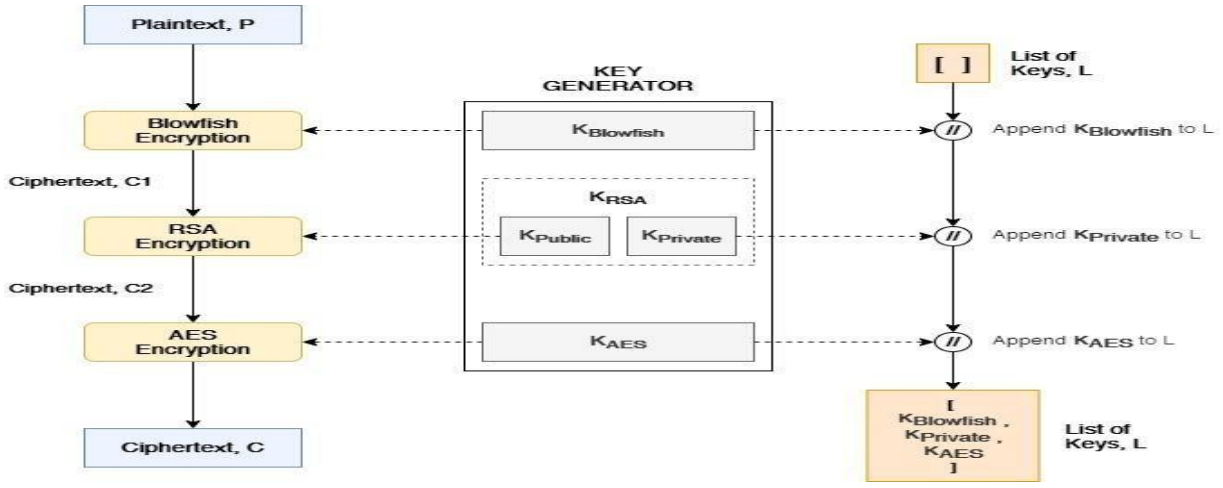


Fig4.DataEncryptionusingCascadingCryptographicSystems

4.2.Secure Keys to rage using encryption of Keys and LSB Steganography Image Embedding.

Using the proposed system, the Keys used for encryption at the various layers can be securely stored. The List of keys, stores all the keys generated throughout the Data Encryption Process. Whenever the key for a particular Encryption Layer is generated, it is appended to the List of Keys, L. In the system, the encryption layers are Blowfish, RSA,and AES, respectively, so the Keys used, are stored in the same or dears:

$$L=[K_{Blowfish},K_{RSA\text{-}Private},K_{AES}]$$

This List, then passed into a function that converts the list into a single string of keys separated by separators(x,*,/).

$$L_S=Stringify(L,separator='x')=K_{Blowfish}xK_{RSA\text{-}Private}xK_{AES}$$

The String, L_S is then encrypted using the AES Encryption Algorithm with a Key generated from user-input password. The user inputs a password, PW which is has hed using SHA-1,and the first 16 Bits of the Hash is used as the key $K_{Password}$. The Key, $K_{Password}$ is used for the Encryption, generating the encrypted string$L_{S\text{-}Encrypted}$.

$$HashedPassword,H_P=SHA(P_W)$$

$$Key,K_{Password}=H_P[0:16]$$

$$L_{S\text{-}Encrypted}=AES(L_S,K_{Password})$$

ThisEncryptedstringisthenEmbeddedintoaCoverImageusingLSBSteganography,givingtheembeddedStegoImage.

$$StegoImage=LSB_Steganography(L_{S\text{-}Encrypted},CoverImage)$$

The StegoImage is transferred to the Receiver along with the Encrypted Data.

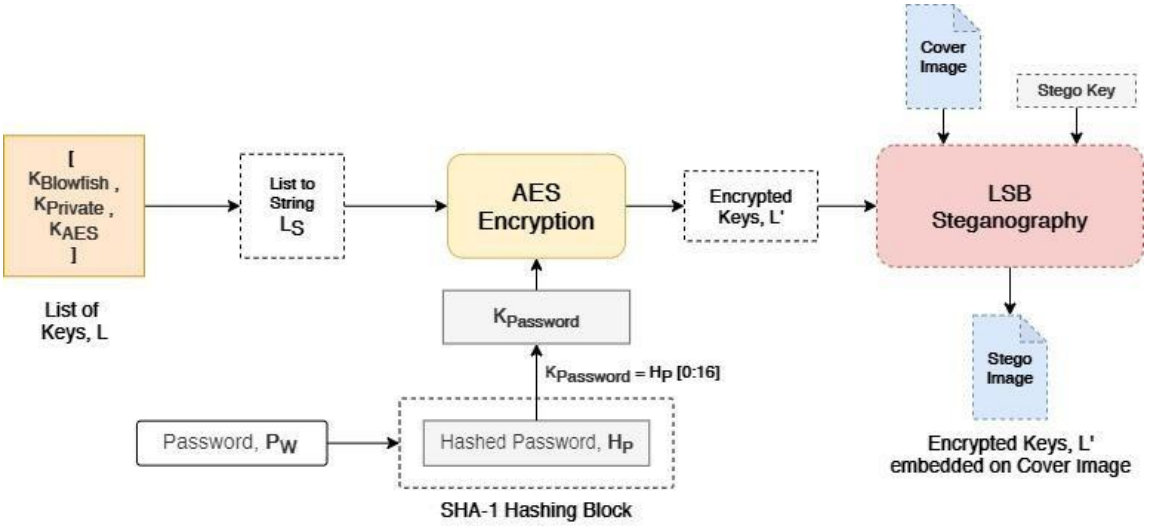


Fig5.Secured Key Encryption and Storage in image using Steganography

5. OUTCOMES AND RESULTS

The Proposed Hybrid Crypto-system was implemented using Python and tested on a Windows PC with an Intel i3 processor and 4GB of RAM. For demon starting the Encryption of data, the following plaintext was encrypted. To encrypt the keys, 'enc2021'was used as the password.

Plaintext:
Hello,World!Thisis2021!

```
Enter Plaintext: Hello, World! This is 2021!
Enter Password: enc2021
Ciphertext:
8afd0bbae83aff941a6c850d49a49bad5082f02bb6d9985c07efbab14c90dba02bc41f644553fa3b83e01b08f3b000d36ff82a32f9cc110bd2d30e710e20cd0
aafa18f562a3cd58b6e8c39e14a88ec00c90949d43b07918f2d6519bad3894ca3c68adf8a79384922b353f8ebd1653cfa7eb894136a7066562f49624929fcea
6cc65c809e7547a9cbe2f9c15444b9c4276798ace196932e73ade9abfc5ffa9e68646238de55d703d0694135353907c4e2beed80c9fdc0094a03ca0934db298
44ea90c6f65006ed053a0d612c9b921c6f3c2a06fca7ad261e7e89fe6f3bb0f42519e6397f8c025284d6ad79c21351768b3f44c1792ca8848a8c67695d126d3
5aea2a142cc7d73ec7e2297e96fe17fdec9d
Encryption Complete!
Encryption Metrics:
Length of Plaintext   :  54
Length of Ciphertext  :  544
Length of Password    :  7
Encryption Time (sec) :  0:00:00.959421
```

Ciphertext:
8afd0bbae83aff941a6c850d49a49bad5082f02bb6d9985c07efbab14c90dba02bc41f644553fa3b83e01b08f3b00
0d36ff82a32f9cc110bd2d30e710e20cd0aafa18f562a3cd58b6e8c39e14a88ec00c909d43b07918f2d6519bad3894ca
3c68adf8a79384922b353f8ebd1653cfa7eb894136a7066562f4962929fcea6cc65c809e7547a9cbe2f9c15444b9c427
6798ace196932e73ade9abfc5ffa9e68646238d5d703d0694135353907c4e2beed80c9fdc0094a03ca0934db29844e
a90c6f65006ed053a0d612c9b921c6f3c2a06fca7ad261e7e9fe6f3bb0f42519e6397f8c025284d6ad79c21351768b3
f44c1792ca887695d126d35aea2a142cc7d73ec7e2297e96fe17fdec9d

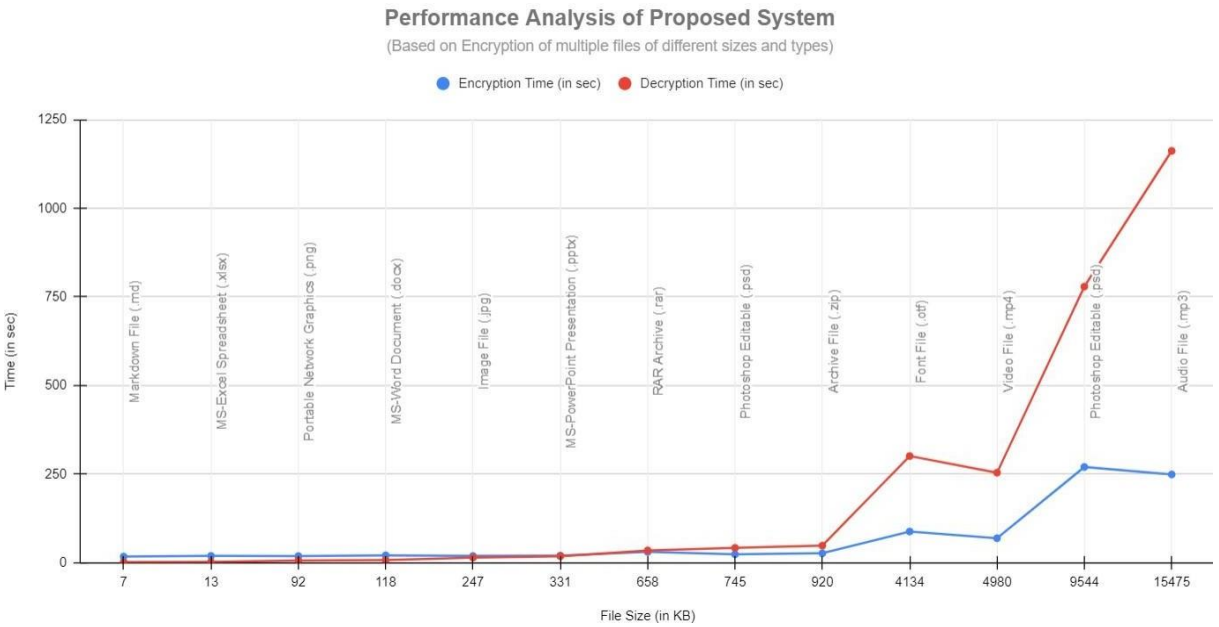
Results show that the ciphertext is 10 times that of plaintext in length. It can be seen that the plain text and cipher text differ by a huge margin and are random, hence we can infer that the system can successfully encrypt the data to a form very different from the original plain text.

5.1. Performance Analysis of the Proposed System

For performance analysis Files of different sizes and types were encrypted using the proposedsystemwiththesamepassword,foreveryfile.Thepasswordusedwas“enc2021”.
The results obtained showed that the crypto-system, when encrypting large-sized files, has adecryption time, significantly higher than encryption time. But when encrypting smaller-sized files the encryption time is slightly higher than the decryption time.

File Type	Size (in KB)	Encryption Time (in sec)	Decryption Time (in sec)	Encryption Rate (in KB/sec)	Decryption Rate (in KB/sec)
Markdown File (.md)	7	17.24	1.81	0.4060324826	3.867403315
MS-Excel Spreadsheet (.xlsx)	13	19.19	2.14	0.6774361647	6.074766355
Portable Network Graphics (.png)	92	18.69	6.28	4.922418406	14.64968153
MS-Word Document (.docx)	118	20.75	7.31	5.686746988	16.14227086
Image File (.jpg)	247	19.06	14.26	12.9590766	17.32117812
MS-PowerPoint Presentation (.pptx)	331	20.09	18.25	16.47585864	18.1369863
RAR Archive (.rar)	658	30.37	34.73	21.66611788	18.94615606
Photoshop Editable (.psd)	745	23.96	41.92	31.09348915	17.77194656
Archive File (.zip)	920	26.65	48.1	34.52157598	19.12681913
Font File (.otf)	4134	88	301	46.97727273	13.73421927
Video File (.mp4)	4980	69	254	72.17391304	19.60629921
Photoshop Editable (.psd)	9544	270	779	35.34814815	12.25160462
Audio File (.mp3)	15475	249	1162	62.14859438	13.31755594

Table1.PerformanceAnalysisofproposedsystem



Graph1.PerformanceAnalysisofproposedsystem

Total Size of Files Encrypted: (in KB)	Average Encryption Time (in sec):	Average Decryption Time (in sec):	Average Encryption Rate (in KB/sec):	Average Decryption Rate (in KB/sec):
37264	67.08	205.45	26.54	14.69

On average, we observe that the Rate of Encryption is higher than the Rate of Decryption. Studieshave shown that crypto-systems with higher decryption time take more time to break and henceare less susceptible to attacks and more secured [6]. Hence we can conclude that the proposed crypto system with high decryption time and rate, is highly secure and efficient in encrypting data.

6. SCOPE OF FURTHER RESEARCH AND IMPROVEMENTS

The proposed system is very secure and robust. It has proven to encrypt data and ensure keysecurity. While it is efficient and secure, it was also seen that the encrypted files are generally 2-3 times the size of the original file; hence the encrypted file takes up a significant amount of space to store. This drawback can be addressed by studying it further and making changes to the proposedsystem. Another improvement that can be made is by making the encryption and decryption timelesser. Further research on the proposed system can also be done by analyzing different order ofcombinations of the three algorithms used. A slightly different combination can also be studied by replacing one of the algorithms for improved performance.

7. CONCLUSION

The proposed cryptosystem uses a combination of symmetric and asymmetric cryptography tosecure data. The system also introduces a sub-process to encrypt the keys used for encryptionbeforeembedding them in an image. The combination of Blowfish-RSA-AES has significantly improved the security and also ensured that the drawbacks of the standalone systems are addressed. The system also helps in improving security without the use of key so flagger lengths. We have also seen from the test results that the system is less us citable to brute force attacks as the decryption time is significantly high [6]. The manyfold expansion of plaintext into cipher text also helps in ensuring a high level of security. While the system successfully does its intended work, it still required minor improvements for larger adoption.

REFERENCES

[1].Sandeshi ,Sachithi & Priyanjana, W & Sajindra, Hirushan & Bandara, Hansi.(2020). "RSA in Communication."

[2].Ghosh, Archisman. (2020). "Comparison of Encryption Algorithms :AES, Blowfish and T wofish for Security of Wireless Networks."10.13140/RG.2.2.31024.38401.

[3].V.kaulA.PShaikh,"EnhancedSecurityAlgorithmusingHybridEncryptionandECC,"IOSRJ.Comput.Eng.,vol.16,no.3,pp.80–85,2014.

[4].Muin, Muhammad &Setyanto ,Arief & Sudar mawan ,& Santoso, Kartika.(2018). "Performance Comparison Between AES 256 -Blowfish and Blowfish-AES256 Combinations." 137-141.10.1109/ICITACEE.2018.8576929.

[5].Chitra Biswas Udayan Das Gupta Md. Mokammel Haque . "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography."2019 International Conference on Electrical, Computer and Communication Engineering(ECCE)

[6.]In ayatullah, Analis is Penerapan Algoritma MD5 Untuk Pengamanan Password ,vol.3,no.3. 2007.

[7]Deepfake Video of Mark Zuckerberg Goes Viral on Eve of House A.I. Hearing : https://fortune.com/2019/06/12/deepfake-mark-zuckerberg/ Accessed on 26 March, 2020

[8]10 deepfake examples that terrified and amused the internet : https://www.creativebloq.com/features/deepfake-examples Accessed on 26 March,2020

[9]TensorFlow:https://www.tensorflow.org/(Accessedon26March,2020)

[10]Keras:https://keras.io/(Accessedon26March,2020)

[11]PyTorch:https://pytorch.org/(Accessedon26March,2020)

[12]G. Antipov, M. Baccouche, and J.-L. Dugelay. Face aging with conditional generative adversarial networks. arXiv:1702.01983, Feb. 2017

[13]J. Thies et al.Face2Face: Real-time face capture and reenactment of rgb videos. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 2387–2395, June 2016. Las Vegas, NV.