Advanced-Data Security using multiple Cryptographic Algorithms over multiple layers and secured Key storing

Project ID:21J606593

Review - III

Group Members

RA1711003030606 Tanmoy Sen Gupta

RA1711003030593 Ritik Srivastava

Supervised By:

Dr. K. Marimuthu

Professor

Department of Computer Science & Engineering

Faculty of Engineering & Technology

SRM Institute of Science & Technology

May 18, 2021

Table of Contents I

Abstract

Security of Data is one of the most important aspects of one's digital presence. With the advent of new and sophisticated technologies, existing data security systems are becoming less efficient in protecting data. Advanced data security protocols used in various applications like WhatsApp and Telegram are becoming inadequate to protect the privacy of an individual. With advancements in Hardware, the time required to break a cryptographic system is becoming even lesser than earlier.

Thus the requirement of a multi-layered encryption protocol that utilizes multiple advanced cryptographic algorithms implemented in a cascading manner is ever more necessary. In this project, data will be encrypted using multiple algorithms like AES, RSA, and Blowfish.The keys that will be used for encryption will also be secured similarly. Multi-layered encryption protocols are not widely used in current systems, hence this project will address the problems faced by standalone systems used for data security.

Objective

- The main objective of this project is to build a Hybrid Crypto-system that secures data on multiple layers and also ensures security of keys.
- The Hybrid crypto-system also securely stores the keys so that they don't lead to any vulnerabilities.
- To create a crypto-system that provides excellent security without compromising on performance and speed.
- To overcome the performance-security tradeoffs of cryptographic algorithms when used separately.

Literature Survey

TITLE AND AUTHOR	SUMMARY
Application of AES and RSA Hybrid Algorithm in Email - *Ye Liu, Wei Gong, Wenqing Fan - ICIS, 2018* [6]	Combining asymmetric encryption with symmetric encryption algorithms makes the system significantly secured and faster. The experimental system also shows that Hybrid Crypto-systems are a great alternative to traditional crypto-systems that rely on higher keys sizes and rounds.
Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations - *Muhammad Abdul Muin, Muhammad Abdul Muin, Arief Setyanto, Sudarmawan, Kartika Imam Santoso - ICITACEE, 2018* [7]	Result shows that a composite cryptosystem on AES256-Blowfish required longer decryption time compared to the composite cryptosystem in reverse order (Blowfish-AES256) therefore, is considered the most secure algorithm compare to Blowfish-AES256, Blowfish or AES256.
Enhancement the Security of Cloud Computing using Hybrid Cryptography Algorithms - *Ali Abdulridha Taha, Dr. Diaa Salama AbdElminaam, Prof. Khalid M Hosny - IJACT, 2017* [10]	The proposed system demonstrates that the use of hybrid algorithms increases the level of encryption of encrypted mobile data and also reduces the time required for encryption and decryption.
An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography - *Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque - ICECCE, 2019* [2]	The resistivity of the proposed system, consisting of AES-RSA Data and Key security and LSB Steganography for storing encrypted key, against attack has been ensured. Thus this algorithm provides confidentiality, integrity and authentication together.
A Research Paper on New Hybrid Cryptography Algorithm - *Prof. Swapnil Chaudhari, Mangesh Pahade, Sahil Bhat, Chetan Jadhav, Tejaswini Sawant - IJRDT, 2019*[3]	The paper studies the implementation of a hybrid Crypto-system of symmetric encryption and asymmetric algorithms. It explores the flows in both standalone systems and uses a hybrid approach to enhance security and address the drawbacks of the standalone systems.

Literature Survey

TITLE AND AUTHOR	SUMMARY
Performance evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text and images - *Pooja Patil, Dr. Rajesh Bansode - IJRET, 2020* [8]	A combination of AES-ECC and SHA-256 is implemented and targeted towards securing medical sector data. It proves efficient in securing text and image based data.
Secure File Storage using Hybrid Cryptography - *S.Gokulraj , P.Ananthi , R.Baby , E.Janani - SSRN, 2021* [9]	A robust and highly secure cryptosystem is implemented using a combination of AES, DES, RC2 to secure data and LSB Steganography is used to ensure Key Security.
Efficient Hybrid Cryptography Algorithm - *Mayes M. Hoobi - Journal of Southwest Jiaotong University, 2020* [4]	Hybrid crypto-system with a combination of DES and ECC, based on test results, proved to increase complexity of block cipher, in addition to increasing the search space of DES Key.
Design And Implementation Of A Hybrid Cryptography Textual System - *Dr. Mahmood Zaki Abdullah, Zinah Jamal Khaleefah - Transactions on Image Processing (Journal), 2018* [1]	The experimental results for the proposed algorithm based on Lorenzo Chaotic and image steganography show that it is secure because it has a large key space, high sensitivity to plain text and secret key.
Novel Hybrid Cryptography for Confidentiality, Integrity, Authentication - *Avinash Jain, V. Kapoor - IJCA, 2017* [5]	A combination of AES and RSA cryptosystem proves to provide high data security and administer key distribution providing secure transmission of data and key

Design of Proposed System

Data Encryption

Data is encrypted using 3 layered hybrid crypto-system consisting of a combination of Blowfish, RSA and AES algorithms. The Plaintext is encrypted using Blowfish using a secret key, then the ciphertext from Blowfish is encrypted by RSA Algorithm using the RSA Public Key. The encrypted ciphertext from RSA is then finally encrypted using the AES Algorithm. The encrypted ciphertext from the AES Algorithm is the final required ciphertext.

Design of Proposed System

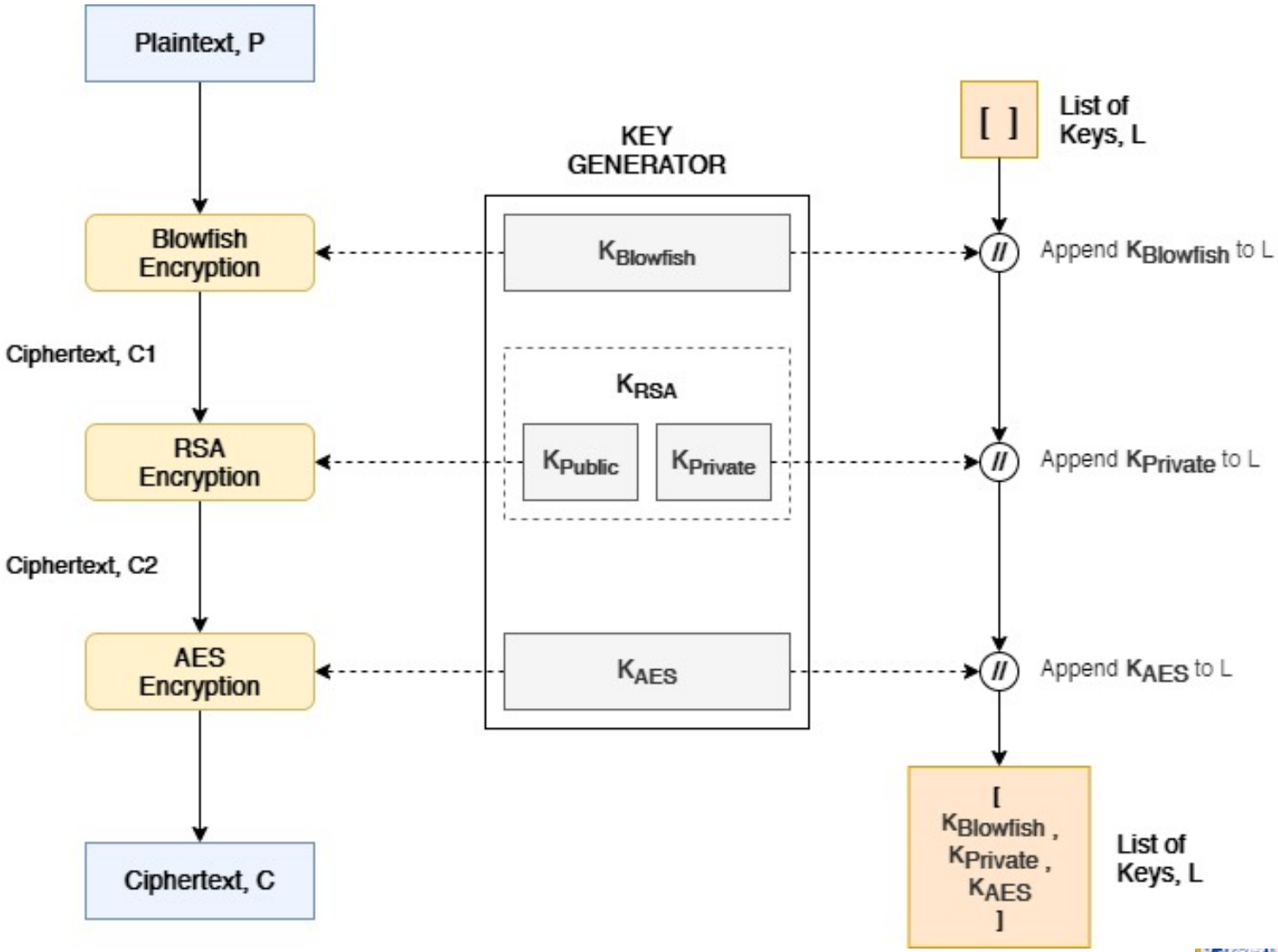


Figure: Data Encryption using Cascading Cryptographic Systems

Design of Proposed System

Secure Key storage using Keys encryption and LSB Steganography

Security of the Keys used is ensured by Encrypting the keys and embedding them in an image. The Keys used are appended to a list of keys after each usage. Then the list is encrypted using AES Algorithm, using the hash of the password set by the user as the key.

The encrypted keys are embedded in an image using LSB Steganography.

Design of Proposed System

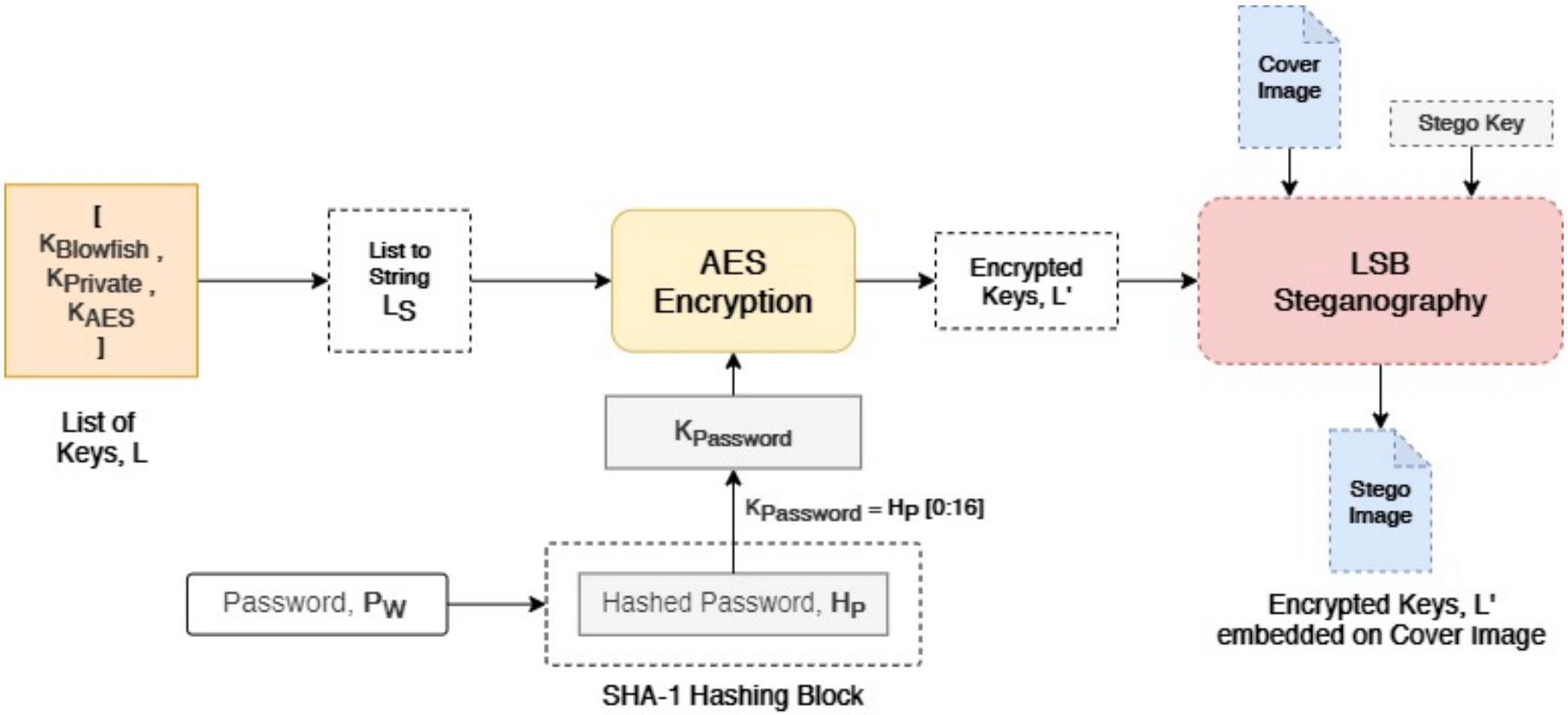


Figure: Secured Key Storage

Experimental Results

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

```
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
```

Results show that the ciphertext is 10 times that of plaintext in length. It can be seen that the plaintext and ciphertext 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 plaintext.

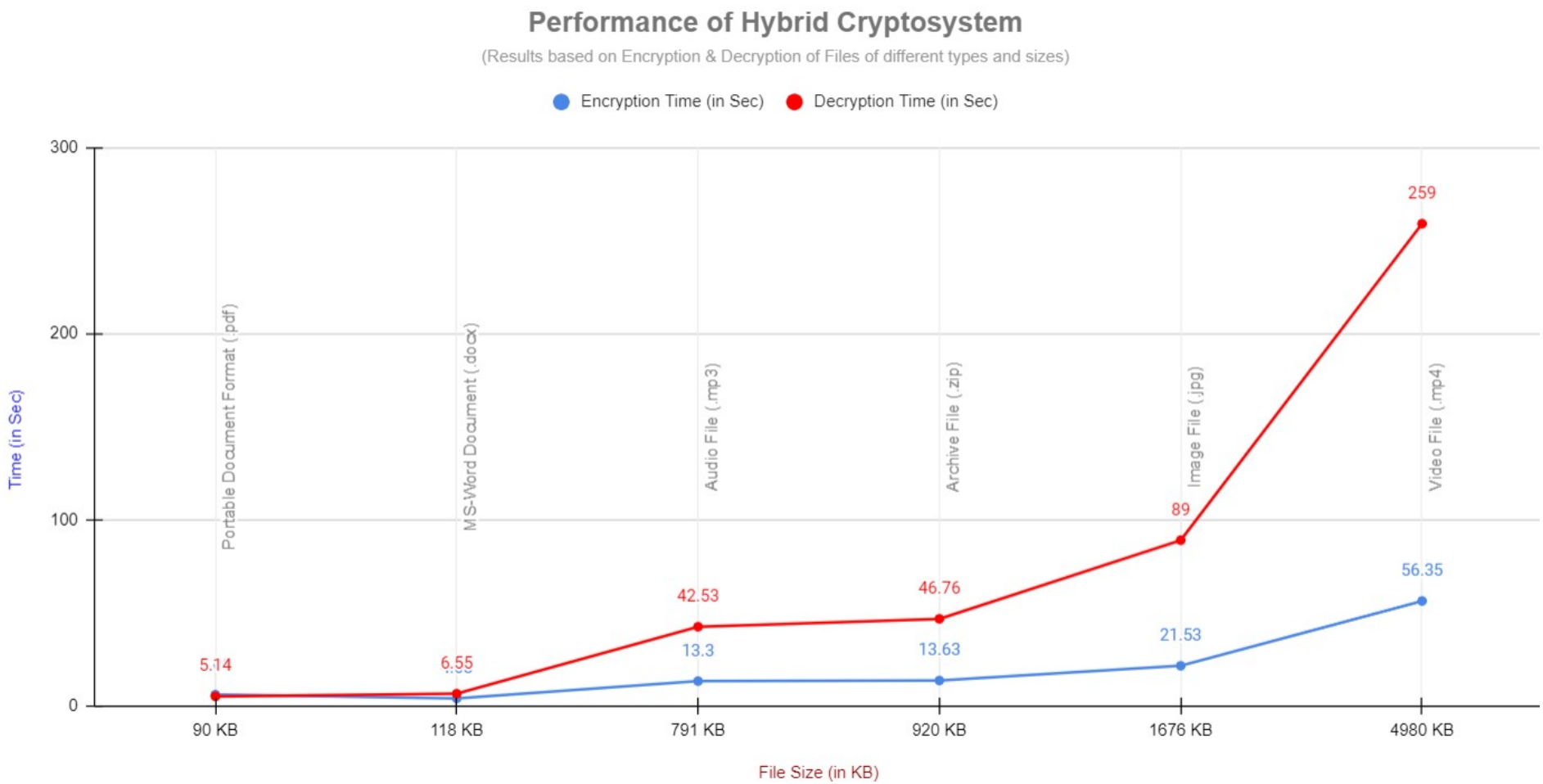
Performance Evaluation

The Hybrid Crypto-system implemented in Python was tested against different file types of varying sizes and 'srm2017' as the password. The following results were obtained.

File Type	Size (in KB)	Encryption Time (in sec)	Decryption Time (in sec)
Portable Document Format (.pdf)	90	6.06	5.14
MS-Word Document (.docx)	118	4.03	6.55
Audio File (.mp3)	791	13.3	42.53
Archive File (.zip)	920	13.63	46.76
Image File (.jpg)	1676	21.53	89
Video File (.mp4)	4980	56.35	259

The tests were conducted on a Windows 10 based laptop with Intel i3 processor and 4 GB of RAM.

Performance Evaluation



Comparison with existing Systems

Testing two existing systems - one Hybrid (AES-RSA) and one Standalone (Blowfish) with the Proposed Cryptosystem gives the following results.

File	File Type	Archive (.zip)	Font (.otf)	Video (.mp4)	PSD (.psd)	Audio (.mp3)	Key Security
	File Size (KB)	920	4134	4980	9544	15475	
Proposed Hybrid Crypto-system (Bowfish-RSA-AES)	Enc. Time (sec)	26.65	88	69	270	249	Yes, using Key Encyrption and Steganogaphy
	Dec. Time (sec)	48	301	254	779	1162	
	Enc. Rate (KB/sec)	34.52	46.9	72.17	35.3	62.14	
	Dec. Rate (KB/sec)	19.12	13.73	19.6	12.25	13.3	
Standalone Crypto-system (Blowfish)	Enc. Time (sec)	27	82	71	182	251	No
	Dec. Time (sec)	32	119	98	328	579	
	Enc. Rate (KB/sec)	34.07407407	50.41463415	70.14084507	52.43956044	61.65338645	
	Dec. Rate (KB/sec)	28.75	34.7394958	50.81632653	29.09756098	26.72711572	
Hybrid Crypto-system (RSA-AES)	Enc. Time (sec)	25	89	68	221	204	No
	Dec. Time (sec)	37	207	129	601	861	
	Enc. Rate (KB/sec)	36.8	46.4494382	73.23529412	43.18552036	75.85784314	
	Dec. Rate (KB/sec)	24.86486486	19.97101449	38.60465116	15.88019967	17.97328688	

Comparison with existing Systems

The Aggregate results of the comparison testing is given below.

	Average Encryption Time	Average Decryption Time	Average Encryption Rate	Average Decryption Rate
Proposed Hybrid Crypto-system (Bowfish-RSA-AES)	140.53	508.8	50.206	15.6
Standalone Crypto-system (Blowfish)	122.6	231.2	53.74450004	34.0260998
Hybrid Crypto-system (RSA-AES)	121.4	367	55.10561916	23.45880341

The results of the Comparison test shows that the Proposed System has a significantly higher Decryption Time, compared to the other two, indicating that the Proposed System is hard to break and will take higher computing power and time to break than the other two, making is highly secured.

References I


M. Z. Abdullah and Z. J. Khaleefah.
Design and implement of a hybrid cryptography textual system.
In *2017 International Conference on Engineering and Technology (ICET)*, pages 1–6, 2017.


C. Biswas, U. D. Gupta, and M. M. Haque.
An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography.
In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pages 1–5, 2019.


S. B. C. J. T. S. Chaudhari Swapnil, Mangesh Pahade.
A research paper on new hybrid cryptography algorithm.
05 2018.

References II

M. M. Hoobi.
Efficient Hybrid Cryptography Algorithm.
Journal of Southwest Jiaotong University, 2020.

A. Jain and V. Kapoor.
Novel hybrid cryptography for confidentiality, integrity, authentication.
International Journal of Computer Applications, 171:35–40, 08 2017.

Y. Liu, W. Gong, and W. Fan.
Application of aes and rsa hybrid algorithm in e-mail.
In *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, pages 701–703, 2018.

References III

M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan, and K. I. Santoso.

Performance comparison between aes256-blowfish and blowfish-aes256 combinations.

In *2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, pages 137–141, 2018.

D. R. B. Pooja Patil.

Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text and Images.

International Research Journal of Engineering and Technology (IRJET), 07(09), 2020.

References IV


R. B. E. J. S. Gokulraj, P. Ananthi.
Secure File Storage Using Hybrid Cryptography.
SSRN, 2021.


A. Taha, D.-D. Salama, S. Abdelminaam, M. Khalid, and K. Hosny.
Enhancement the security of cloud computing using hybrid cryptography algorithms.
International Journal of Advancements in Computing Technology, 9, 12 2017.