Fortifying Connectivity: A Hybrid Algorithm Approach for Augmented Security and Efficiency in Bluetooth Technology

Rashmi Sharma
School of Studies Engineering & Technology,
Guru Ghasidas Vishwavidyalaya, A Central University,
Bilaspur, Chhattisgarh,495006 India.
Email: rashmivks03 [AT] gmail.com

Dr. Manish Shrivastava
School of studies Engineering & Technology,
Guru Ghasidas Vishwavidyalaya, A Central University,
Bilaspur, Chhattisgarh,495001 India.
Email: manbsp [AT] gmail.com

Abstract: **Bluetooth technology has become an integral part of our daily lives, providing wireless connectivity and seamless communication between wide ranges of devices. Bluetooth uses a master-slave architecture, where one device acts as the master, and the other devices act as slaves. The master device initiates and controls the connection, while the slave devices respond to connection requests from the master. In this research we are enhancing the security and efficiency of Bluetooth technology using hybrid approached algorithm i.e., combination of Two fish and ElGamal algorithm for making the communication process more secure and protected from foreign access. This research paper proposes a novel approach to enhance Bluetooth security by applying a hybrid algorithm that combines the strengths of Two fish and ElGamal encryption schemes. Two fish, a symmetric-key algorithm known for its high-speed data processing and resistance to attacks, will provide the foundation for encrypting data during Bluetooth communication. Concurrently, ElGamal, a public-key algorithm celebrated for its robust security and strong cryptographic properties, will complement the hybrid approach by ensuring secure key exchange between devices. The fusion of Two fish and ElGamal aims to overcome the limitations of using either algorithm in isolation, while capitalizing on their respective advantages to form a more potent and reliable security solution. By employing Two fish for efficient data encryption and ElGamal for secure key exchange, we anticipate a formidable defense against various attack vectors, including eavesdropping, man-in-the-middle attacks, and brute-force attempts.**

***Keywords**: Bluetooth, Architecture, Related Work, Versions, Two fish algorithm, ElGamal Algorithm, Conclusion.*

I. INTRODUCTION

The name "Bluetooth" was inspired by the Viking king Harald Bluetooth, known for his ability to bring people together. Similarly, Bluetooth technology aims to connect devices and facilitate easy data transfer. Bluetooth operates in the 2.4 GHz frequency range and uses radio waves for communication. It employs a technique called frequency hopping spread spectrum (FHSS) to minimize interference from other devices operating in the same frequency band. Bluetooth technology has found widespread applications in areas such as audio streaming, wireless headphones, hands-free calling in cars, file sharing, wireless input devices, home automation, and Internet of Things (IoT) devices. Overall, Bluetooth provides a convenient and reliable means of wireless communication, making it easier for devices to connect and interact with one another, enhancing the user experience and enabling a wide range of applications.

Traditional security mechanisms employed in Bluetooth have faced increasing challenges due to the rapid evolution of sophisticated cyber threats. To address these vulnerabilities and reinforce the security landscape of Bluetooth technology, researchers have turned to hybrid cryptographic approaches that combine the strengths of multiple algorithms. The goal of this research paper is to address the imperative need for enhanced security in Bluetooth technology through the application of a hybrid algorithm. In this context, the fusion of two powerful cryptographic algorithms, Twofish and ElGamal, offers a promising solution to fortify Bluetooth against potential threats and attacks. By leveraging the strengths of both algorithms, we aim to create a robust and efficient security framework that can protect sensitive information and communications in Bluetooth-enabled environments.

To counteract these security challenges, we propose the integration of Twofish and ElGamal algorithms as a hybrid approach. Twofish, known for its robustness and resistance to cryptanalysis, offers a highly secure symmetric key encryption method. Simultaneously, ElGamal, an asymmetric key algorithm, provides efficient digital signatures and key exchange mechanisms, enhancing the security of data transmissions in public-key cryptography.

II. RELATED WORK

A study & comparative analysis of cryptographic algorithms for various file formats (2016, IJSR):This research paper compares different cryptographic algorithms' performance concerning encryption, decryption, and throughput time while considering various file features like data types, data sizes, and key sizes.

Improved Twofish algorithm: A digital image enciphering application (2017, IEEE):This paper presents an enhancement to the Twofish algorithm by utilizing substitution boxes (S-Boxes) to improve its mathematical complexity, making it more secure for digital image enciphering applications.

Performance evaluation of Twofish algorithm on IMAN1 supercomputer (2018, IJSTR):The paper evaluates the performance of the Twofish algorithm on the IMAN1 supercomputer, comparing its sequential and parallel implementations using the Message Passing Interface (MPI).

Evolution of AES, Blowfish & Twofish Encryption algorithm (2018, IJSER): This paper analyzes and compares the efficiency of three encryption algorithms, AES, Blowfish, and Twofish, based on criteria like space, time, and security to determine their suitability for various applications.

Testing Vulnerability in BLE (2018, ACM,SE):The paper examines tools related to sniffing Bluetooth traffic in Android operating systems to assess the vulnerability of Bluetooth Low Energy (BLE) technology.

Security vulnerability in Bluetooth technology as used in IoT (2018, MDPI):This paper discusses security vulnerabilities in Bluetooth technology concerning IoT applications and proposes using application software patches to resolve these vulnerabilities.

Novel hybrid encryption algorithm based on AES, RSA, and Twofish for Bluetooth encryption (2018, SCIRP): The paper introduces a hybrid encryption algorithm that combines AES, RSA, and Twofish to enhance the security level of Bluetooth encryption. The future work involves analyzing the current encryption mechanism.

On secure simple pairing in Bluetooth standard V5.0 (2019, MDPI): This paper develops a formal privacy model to evaluate the privacy vulnerability in the LESSP protocol for secure simple pairing in Bluetooth V5.0. It suggests future work on assessing the privacy of the association model in the LESSP protocol.

Hybrid Cryptosystem using RSA, DSA, Elgamal & AES (2019, IJSTR): The paper presents a hybrid encryption approach that integrates asymmetric algorithms like RSA, DSA, Elgamal, and symmetric algorithm AES to ensure data integrity during exchange.

Two fish algorithms for encryption & decryption (2019, JETIR): This paper focuses on the VLSI architecture of the Twofish block cipher to enable efficient encryption and decryption operations.

Implementation of AES cryptography & Twofish hybrid algorithms for the cloud (2020, Journal of Physics):The goal of this paper is to enhance data encryption results to prevent unauthorized access and hacking in cloud environments using a hybrid of AES and Twofish algorithms.

Comparative study on Blowfish & Twofish algorithm in IoT application (2020, IJERA):This paper provides a parallel presentation of Twofish & Blowfish algorithms and compares their suitability for IoT applications.

Attack and defenses in short-range wireless technology for IoT (2020, IEEE): The paper surveys attacks related to the wireless infrastructure of IoT and discusses defense mechanisms to protect against such attacks.

Key negotiation downgrade attack on Bluetooth and BLE (2020, EPTL): The paper successfully demonstrates key negotiation downgrade attacks on various Bluetooth and BLE devices from different manufacturers.

Disrupting continuity of Apple's wireless ecosystem security (2021, USENIX): This paper discusses disrupting the security of Apple's wireless ecosystem and potentially identifies vulnerabilities.

Two-layer encryption based on Paillier & Elgamal cryptosystem for privacy violation (2021, MECS): The paper focuses on addressing privacy protection challenges and ensuring secure information utilization through a two-layer encryption approach based on Paillier and Elgamal cryptosystems.

Based on mesh sensor network: Design and Implementation of security monitoring system with Bluetooth technology (2022, IAES): This paper introduces a new security monitoring system based on a low-cost Bluetooth sensor network deployed in a mesh sensor network.

Performance evaluation of cryptographic algorithm: DES, 3DES, Blowfish, Twofish & Threefish (2022, IJCNIS): The paper compares the performance of five symmetric block cipher algorithms, including DES, 3DES, Blowfish, Twofish, and Threefish, based on simulation results. It suggests exploring other performance measures in future work.

Cryptographic method to enhance data security using Elgamal algorithm & Kamal Transform (2022, IOSR-JCE): This paper proposes a cryptographic method using the Elgamal algorithm and Kamal Transform to enhance the security of communication.

Cloud data security system using cryptography & steganography: A review (2022, IJSR):This paper provides an analysis of the performance of cryptographic and steganography techniques for cloud data security.

Secure sensitive data sharing using RSA & El Gamal Cryptographic algorithms with a hash function (2022, MDPI): The paper compares the performance of RSA and El Gamal cryptographic algorithms during encryption, decryption, signature generation, and signature verification processes, suggesting their specific strengths in each operation. This paper explores the use of RSA and El Gamal cryptographic algorithms with a hash function for secure sensitive data sharing. The study reveals the strengths of each algorithm in different stages of encryption and signature processes.

SL. NO.	***PAPER***	***YEAR***	***PUBLICATION***	***DESCRIPTION***
1.	A study & comparative analysis of cryptographic algorithms for various file formats.	2016	IJSR	Performance of different algorithm have been made with respect to encrypt, decrypt, and throughput time with the variation of various file features like different data type, data size,key size.
2.	Improved twofish algorithm: A digital image enciphering application.	2017	IEEE	Twofish algorithm's mathematical complexity is improved by using substitution boxes(S-Boxes)
3.	Performance evaluation of twofish algorithm on IMAN1 supercomputer.	2018	IJSTR	In this paper, the sequential & parallel implementation in IMAN1 super computer using message passing interface(MPI)
4.	Evolution of AES, Blowfish & Two fish Encryption algorithm.	2018	IJSER	Efficient Encryption algorithm is analysed on the basis of less space, time,& security among these encryption algorithm.
5.	Testing Vulnerability in BLE	2018	ACM, SE	Android operating systems tools relate to sniffing Bluetooth traffic were examined.
6.	Security vulnerability in Bluetooth technology as used in IOT	2018	MDPI	Application Software Patches are used to resolve vulnerabilities in computer system. Future research-focus on power attack on BLE.
7.	Novel hybrid encryption algorithm based on AES, RSA and two fish for Bluetooth encryption.	2018	SCIRP	Triple protection of AES, RSA and two fish enhances the level of security. Future work -analysis of current encryption mechanism.
8.	On secure simple pairing in Bluetooth standard V5.0.	2019	MDPI	Formal privacy model is developed to evaluate the [privacy vulnerability in LESSP protocol. Future work-Yet no work on privacy of association model in LESSP protocol
9.	Hybrid Cryptosystem using RSA, DSA, Elgamal & AES.	2019	IJSTR	Integration & combination of an asymmetric & symmetric algorithm such as RSA,Elgamal,DSA & AES were presented. Hybrid encryption has been used to ensure integrity in terms of data exchanged.
10.	Two fish algorithm foe encryption & decryption.	2019	JETIR	VLSI architecture of Twofish block cipher is presented.
11.	Implementation of AES cryptography & two fish hybrid algorithms for cloud.	2020	Journal of Physics	The goal is to strengthen the results of the data encryption in the case will be hacked, unauthorized people.
12.	Comparative study on Blowfish & Two fish algorithm in IOT application.	2020	IJERA	Parallel presentation of Twofish & Blowfish algorithm.
13.	Attack and defenses in short range wireless technology for IOT.	2020	IEEE	We provide survey of attacks related to wireless infrastructure of IOT.
14.	Key negotiation down grade attack on Bluetooth and BLE.	2020	EPTL	We successfully attack 38 Bluetooth devices and 19 BLE devices from different manufacturer.
15.	Disrupting continuity of apple's wireless ecosystem security.	2021	USENIX	Disrupting continuity of apple's wireless ecosystem security.
16.	Two-layer encryption based on paillier & Elgamal cryptosystem for privacy Violation.	2021	MECS	Focuses on challenges of privacy protection & secure utilization of information.
17.	Based on mesh sensor network: Design and Implementation of security monitoring system with Bluetooth technology.	2022	IAES	A New security monitoring system has been created. Creation of low-cost Bluetooth sensor security network
18.	Performance evaluation of cryptographic algorithm: DES,3DES,Blowfish,Twofish & Threefish.	2022	IJCNIS	Comparison of 5 symmetric block cipher algorithm on the basis of simulation result. Future Work- algorithm need to be tested with respect to several performance measure other than encryption speed.
19.	Cryptographic method to enhance the data security using elgamal algorithm & Kamal Transform.	2022	IOSR-JCE	This paper is all about the cryptography method using elgamal algorithm & Kamal transform to improve security of communication.
20.	Cloud data security system using cryptography & steganography: A review.	2022	IJSR	This paper is based on analyzes the performance of cryptographic & steganography techniques.
21.	Secure sensitive data sharing using RSA & Elgamal Cryptographic algorithms with hash function.	2022	MDPI	RSA performs better than elgamal during the encryption & signature verification process , while elgamal performs better than RSA during decryption & signature generation process.

III. PROPOSED ALGORITHM

We have taken combination of two existing algorithms that are the first one is Two fish algorithm and the next one is Elgamal algorithm. By combining the strengths of Twofish and ElGamal, a hybrid security approach for Bluetooth technology emerges. This approach aims to provide a multi-layered defense against a range of security threats. Twofish could be used for data encryption during Bluetooth communication sessions, ensuring that data exchanged between devices remains confidential. Simultaneously, ElGamal could be employed for secure key exchange, enhancing Bluetooth pairing mechanisms and preventing unauthorized access.

Twofish, designed by Bruce Schneier and others, offers a high level of security through its complex key expansion and substitution-permutation network structure. Its symmetric nature allows for efficient data encryption and decryption, making it suitable for resource-constrained devices like those commonly found in Bluetooth-enabled devices.
ElGamal, on the other hand, leverages the mathematical complexity of discrete logarithm problems for asymmetric encryption. It provides a powerful way to ensure data confidentiality and authenticity without requiring the exchange of secret keys. The integration of ElGamal within Bluetooth could enable secure key exchange and secure communication channels, addressing vulnerabilities associated with Bluetooth's default pairing mechanisms.

A. Pseudocode of Hybrid algorithm.

```
# Pseudo code for encrypting with Twofish followed by El Gamal

plaintext = "Hello, world!"  # The text to be encrypted

# Step 1: Encrypt with Twofish
twofish_key = generate_twofish_key()
twofish_iv = generate_twofish_iv()
twofish_ciphertext = twofish_encrypt(plaintext, twofish_key, twofish_iv)

# Step 2: Encrypt with ElGamal
elgamal_public_key, elgamal_private_key = generate_elgamal_keys()
elgamal_ciphertext = elgamal_encrypt(twofish_ciphertext, elgamal_public_key)

# Output the final encrypted result
encrypted_text = elgamal_ciphertext
```

```
# Pseudo code for decrypting with ElGamal followed by Twofish

elgamal_ciphertext = encrypted_text   # The ciphertext obtained from encryption

# Step 1: Decrypt with ElGamal
twofish_ciphertext = elgamal_decrypt(elgamal_ciphertext, elgamal_private_key)

# Step 2: Decrypt with Twofish
plaintext = twofish_decrypt(twofish_ciphertext, twofish_key, twofish_iv)

# Output the final decrypted result
decrypted_text = plaintext
```

IV. REASON BEHIND HYBRID APPROACH

A hybrid approach combines the strengths of different cryptographic algorithms, making it harder for attackers to exploit vulnerabilities specific to a single algorithm. Twofish and ElGamal are well-regarded cryptographic algorithms known for their security properties, and combining them can provide a more robust security solution. ElGamal, as an asymmetric encryption scheme, provides forward secrecy. This means that even if an attacker compromises the private key in the future, they won't be able to decrypt past communications encrypted using previous public keys. This adds an extra layer of protection to the Bluetooth communication. hybrid approach allows developers to adapt their solution quickly. If vulnerabilities or weaknesses are discovered in one of the algorithms, the system can be updated to use a different, more secure algorithm while still maintaining compatibility with the existing infrastructure.

V. PROS OF HYBRID APPROACH

The hybrid approach that combines the Two fish and ElGamal algorithms in cryptography offers several advantages:

Confidentiality: Two fish provides strong symmetric key encryption, ensuring the confidentiality of the data being transmitted. It is computationally efficient and well-suited for encrypting large amounts of data. By using Twofish, the hybrid approach ensures the confidentiality of the message.

Key Distribution: The ElGamal algorithm provides a secure method for exchanging the symmetric key used in the Twofish algorithm. ElGamal is a public-key encryption algorithm that enables secure key distribution without requiring a pre-shared secret key. This eliminates the need for secure key exchange protocols.

Asymmetric Encryption: The ElGamal algorithm's public-key encryption feature allows for secure encryption using the recipient's public key. This ensures that only the recipient, who possesses the corresponding private key, can decrypt the message. By combining ElGamal with Two fish, the hybrid approach leverages the benefits of asymmetric encryption for secure message transmission.

Digital Signatures: In addition to encryption, the ElGamal algorithm can also be used for digital signatures. By incorporating digital signatures into the hybrid approach, it enables not only secure encryption but also authentication and integrity verification of the transmitted message. This provides a comprehensive security solution.

Efficiency and Performance: The hybrid approach combines the efficiency of symmetric encryption with the security benefits of public-key encryption. By using symmetric encryption (Two fish) for the bulk of the data and asymmetric encryption (ElGamal) for key distribution and encryption of the symmetric key, the hybrid approach achieves a balance between security and performance.

Flexibility: The hybrid approach allows for flexibility in choosing appropriate encryption algorithms for different parts of the communication process. Different algorithms can be used for different aspects, based on their strengths and weaknesses. This flexibility provides an opportunity to optimize the encryption process according to specific requirements and constraints.

Compatibility: Two fish and ElGamal are both well-established and widely used encryption algorithms. By combining them in a hybrid approach, compatibility is ensured, as they are both standard algorithms with established implementations and support in cryptographic libraries.

Overall, the hybrid approach of combining Two fish and ElGamal offers the advantages of strong symmetric encryption, secure key distribution, asymmetric encryption, digital signatures, efficiency, flexibility, and compatibility. It provides a robust and comprehensive solution for secure and confidential communication.

VI. IMPLIMENTATION

I have implemented a single pair of hybrid algorithm i.e. Two fish along with El Gamal algorithm to verify the efficiency, processing speed and security of Bluetooth technology, which are not yet used to ensure Bluetooth Security. So, by applying a hybrid approach with Two fish & El Gamal Algorithm, in order to ensure security , El Gamal algorithm will be more challenging to solve because of its complicated calculation.

A. ALGORITHM

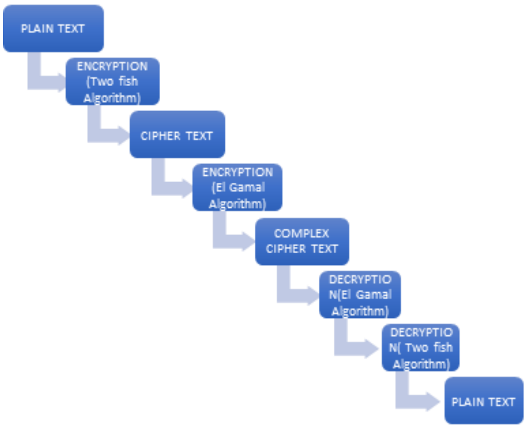
A.1. ENCRYTION ALGORITHM

- Generate a random Two fish key (K_twofish) and a random Two fish initialization vector (IV_twofish).
- Generate an El Gamal public-private key pair (PK_elgamal, SK_elgamal).
- Encrypt the message using the Two fish encryption algorithm with K_twofish and IV_twofish. This will produce the Two fish ciphertext.
- Encrypt the Two fish ciphertext using the El Gamal encryption algorithm with PK_elgamal. This will produce the El Gamal ciphertexts.
- Return the El Gamal ciphertexts.

A.2. DECRYPTION ALGORITHM

- Decrypt the El Gamal ciphertexts using the El Gamal decryption algorithm with SK _elgamal. This will produce the decrypted blocks.
- Combine the decrypted blocks into a single numerical representation.
- Decrypt the numerical representation using the Two fish decryption algorithm with K_twofish and IV_twofish. This will produce the Two fish plaintext.
- Remove any padding from the Two fish plaintext.
- Return the decrypted plaintext.

B. WORKING FLOW OF HYBRID APPROACH


PLAIN TEXT
ENCRYPTION (Two fish Algorithm)
CIPHER TEXT
ENCRYPTION (El Gamal Algorithm)
COMPLEX CIPHER TEXT
DECRYPTIO N(El Gamal Algorithm)
DECRYPTIO N(Two fish Algorithm)
PLAIN TEXT

Here's a simplified outline of how the hybrid approach using Twofish and ElGamal could work:

1. Key Generation:
   - Generate a symmetric key for the Two fish algorithm and a key pair (public key and private key) for the ElGamal algorithm.
2. Encryption:
   - Generate a random session key for the Two fish algorithm.
   - Encrypt the actual plaintext message using the symmetric Two fish algorithm with the session key.
   - Encrypt the session key using the recipient's public key with the ElGamal algorithm.
3. Transmission:
   - Send the encrypted session key along with the encrypted message.
4. Decryption:
   - Decrypt the session key using the recipient's private key with the ElGamal algorithm.
   - Decrypt the encrypted message using the symmetric Two fish algorithm with the decrypted session key.

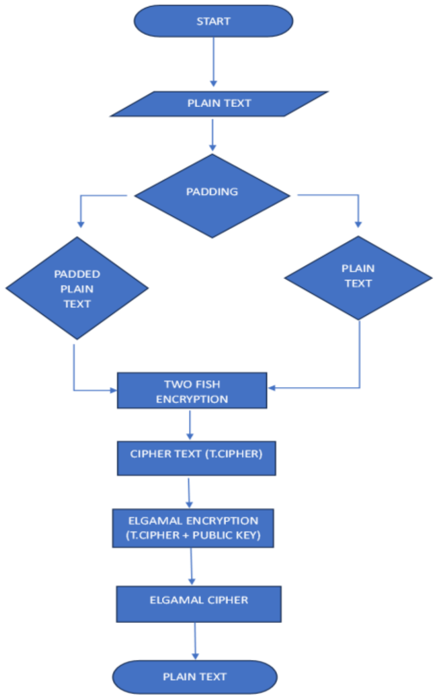
By combining Two fish and El Gamal in this way, we achieve the benefits of both algorithms:

- Two fish provides efficient and secure symmetric encryption for the actual message, ensuring confidentiality.
- ElGamal provides secure asymmetric encryption for the session key, allowing for secure key exchange and confidentiality of the symmetric key.

This hybrid approach benefits from the efficiency of symmetric encryption and the secure key exchange of asymmetric encryption, providing a robust solution for secure communication.

It's important to note that the exact implementation and integration of Two fish and El Gamal may vary depending on the specific requirements and considerations of the system or application.

VII. FLOW CHART



VIII. RESULT

When applying a hybrid approach that combines the Two fish and El Gamal algorithms, we can achieve a combination of symmetric and asymmetric encryption for enhanced security and efficiency.

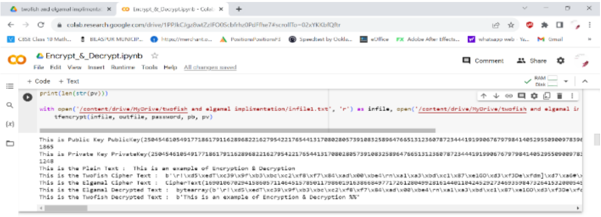
When applying a hybrid approach that combines the Two fish and El Gamal algorithms, we can achieve a combination of symmetric and asymmetric encryption for enhanced security.

By combining Two fish and El Gamal in a hybrid approach, we benefit from the advantages of both algorithms. Two fish provides efficient and secure encryption for the actual data, while ElGamal provides the ability to securely encrypt and transmit the symmetric key used for data encryption.

This hybrid approach ensures confidentiality and secure transmission of data. It addresses the key exchange challenge in symmetric encryption by using asymmetric encryption to securely share the symmetric key. The combination of symmetric and asymmetric encryption provides a robust and practical solution for secure communication and data protection.

Applying a hybrid approach that combines the Twofish and ElGamal algorithms in Bluetooth technology can provide enhanced security and privacy for data transmission. By leveraging the strengths of both algorithms, the hybrid approach aims to mitigate potential vulnerabilities and provide robust encryption and authentication mechanisms. Here are some potential benefits:

OUTPUT SCREEN FOR 128 BIT KEY SIZE.

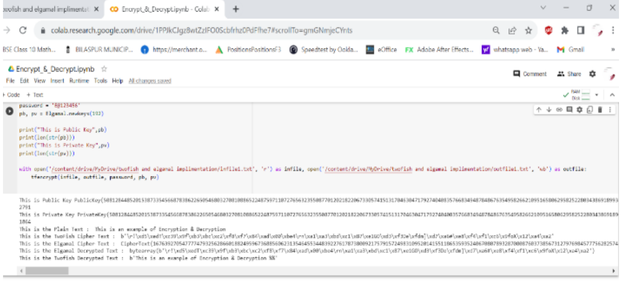


```
print(len(str(pv)))

with open('/content/drive/MyDrive/twofish and elgamal implimentation/infile1.txt', 'r') as infile, open('/content/drive/MyDrive/twofish and elgamal in
    tfencrypt(infile, outfile, password, pb, pv)
```

```
This is Public Key PublicKey([illegible]
1865
This is Private Key PrivateKey([illegible]
1248
This is the Plain Text :  This is an example of Encryption & Decryption
This is the TwoFish Cipher Text :  b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfdm]\xd7\xa6#\x
This is the Elgamal Cipher Text :  CipherText([illegible]
This is the Elgamal Decrypted Text :  bytearray(b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfd
This is the Twofish Decrypted Text :  b'This is an example of Encryption & Decryption %%'
```

OUTPUT SCREEN FOR 192 BIT KEY SIZE.



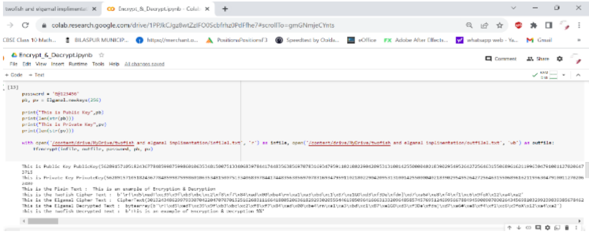
```
password = 'E@123456'
pb, pv = Elgamal.newkeys(192)

print("This is Public Key",pb)
print(len(str(pb)))
print("This is Private Key",pv)
print(len(str(pv)))

with open('/content/drive/MyDrive/twofish and elgamal implimentation/infile1.txt', 'r') as infile, open('/content/drive/MyDrive/twofish and elgamal implimentation/outfile1.txt', 'wb') as outfile:
    tfencrypt(infile, outfile, password, pb, pv)
```

```
This is Public Key PublicKey([illegible]
2791
This is Private Key PrivateKey([illegible]
1864
This is the Plain Text :  This is an example of Encryption & Decryption
This is the TwoFish Cipher Text :  b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfdm]\xd7\xa6#\xe8\xf4\xf1\xc6\x9foX\x12\xa4\xa2'
This is the Elgamal Cipher Text :  CipherText([illegible]
This is the Elgamal Decrypted Text :  bytearray(b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfdm]\xd7\xa6#\xe8\xf4\xf1\xc6\x9foX\x12\xa4\xa2')
This is the Twofish Decrypted Text :  b'This is an example of Encryption & Decryption %%'
```

OUTPUT SCREEN FOR 256 BIT KEY SIZE.



```
[13]
password = 'E@123456'
pb, pv = Elgamal.newkeys(256)

print("This is Public Key",pb)
print(len(str(pb)))
print("This is Private Key",pv)
print(len(str(pv)))

with open('/content/drive/MyDrive/twofish and elgamal implimentation/infile1.txt', 'r') as infile, open('/content/drive/MyDrive/twofish and elgamal implimentation/outfile1.txt', 'wb') as outfile:
    tfencrypt(infile, outfile, password, pb, pv)
```

```
This is Public Key PublicKey([illegible]
3715
This is Private Key PrivateKey([illegible]
[illegible]
This is the Plain Text :  This is an example of Encryption & Decryption
This is the Twofish Cipher Text :  b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfdm]\xd7\xa6#\xe8\xf4\xf1\xc6\x9foX\x12\xa4\xa2'
This is the Elgamal Cipher Text :  CipherText([illegible]
This is the Elgamal Decrypted Text :  bytearray(b'\r|\xd5\xedT\xc39\x9f\xb3\xbc\xc2\xf8\xf7\x84\xad\x00\xbe4\rn\xa1\xa3\xbd\xc1\x87\xe1GO\xd3\xf3De\xfdm]\xd7\xa6#\xe8\xf4\xf1\xc6\x9foX\x12\xa4\xa2')
This is the Twofish Decrypted Text :  b'This is an example of Encryption & Decryption %%'
```

By applying the dual encryption algorithm i.e. Two fish algorithm along with El Gamal algorithm in Bluetooth technology.

- Data transmission takes place between the devices in a seconds i.e. 1sec-5sec.So processing speed is reduced.
- Security is enhanced as we goes on increasing the key size of El Gamal Algorithm.
- For 128-bit key size, data is processed within 1 seconds.
- For 192-bit key size, data is processed within 5 seconds
- For 256-bit key size, data is processed within 10 seconds.

IX. ACKNOWLEDGEMENT

I would like to thank my supervisor, Dr. Manish Shrivastava, for his invaluable guidance, continuous support, and encouragement throughout the research process. His expertise and insights have been instrumental in shaping the direction of this paper.

REFERENCES

[1] Hamouda, Baha Eldin, https://www.researchgate.net/publication/341936439_Comparative_Study_of_Different_Cryptographic_Algorithms, Journal of information security,DOI:10.4236/jis.2020.113009.

[2] TANVEER UL HAQ 1 , TARIQ SHAH 1, Improved Twofish Algorithm: A Digital Image Enciphering Application,IEEE, Doi: 10.1109/ACCESS.2021.3081792.

[3] https://www.researchgate.net/publication/325792828_Performance_Evaluation_of_Twofish_Algorithm_on_IMAN1_Supercomputer, June 2018International Journal of Computer Applications 179(50):1-7,DOI:10.5120/ijca2018916654

[4] E.Jeevalatha, Mr.S.SenthilMurugan, Evolution of AES, Blowfish and Two fish Encryption Algorithm, International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018 ISSN 2229-5518, DOI:10.13140/RG.2.2.31024.38401

[5] Thomas Willingham, Cody Henderson, Blair Kiel, Md Shariful Haque, and Travis Atkison. 2018. Testing Vulnerabilities in Bluetooth Low Energy. In ACM SE '18: ACM SE '18: Southeast Conference, March 29–31, 2018, Richmond, KY, USA. ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/ 3190645.3190693.

[6] https://www.researchgate.net/publication/326511381_Security_Vulnerabilities_in_Bluetooth_Technology_as_Used_in_IoTJ. Sens. Actuator Netw. 2018, 7(3), 28; https://doi.org/10.3390/jsan7030028

[7] Albahar, M.A., Olawumi, O., Haataja, K. and Toivanen, P. (2018) Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Two fish for Bluetooth Encryption. Journal of Information Security, 9, 168-176. https://doi.org/10.4236/jis.2018.92012.

[8] *Sun DZ, Sun L, Yang Y. On Secure Simple Pairing in Bluetooth Standard v5.0-Part II: Privacy Analysis and Enhancement for Low Energy. Sensors (Basel). 2019 Jul 24;19(15):3259. doi: 10.3390/s19153259. PMID: 31344911; PMCID: PMC6696427.Sensors 2019, 19(15), 3259; https://doi.org/10.3390/s19153259*

[9] [9] Levinia B. Rivera, Jazzmine A. Bay, Edwin R. Arboleda, Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 10, OCTOBER 2019, https://www.researchgate.net/publication/336818536_Hybrid_Cryptosystem_Using_RSA_DSA_Elgamal_And_AES.

[10] Anil G. Sawant, 2 Dr. Vilas N. Nitnaware, TWOFISH ALGORITHM FOR ENCRYPTION AND DECRYPTION, JETIR, https://www.jetir.org/papers/JETIRW006063.pdf.

[11] K I Santoso, M A Muin and M A Mahmudi, Implementation of AES cryptography and two fish hybrid algorithms for cloud, DOI 10.1088/1742-6596/1517/1/012099, Journal of Physics:

Conference Series, Volume 1517, 2019 1st Borobudur International Symposium on Applied Science and Engineering (BIS-ASE) 2019 16 October 2019, Magellan, Indonesia Citation K I Santoso et al 2020 J. Phys.: Conf. Ser. 1517 012099

[12] Ms.S. Selvakumari, Comparative Study on Blowfish & Two fish Algorithms in Iot Applications, https://www.academia.edu/42794395/Comparative_Study_on_Blowfish_and_Twofish_Algorithms_in_Iot_Applications

[13] K. Lounis and M. Zulkarnaen, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.DOI: 10.1109/ACCESS.2020.2993553

[14] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. 2020. Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy. ACM Trans. Priv. Secure. 23, 3, Article 14 (June 2020), 28 pages. https://doi.org/10.1145/3394497

[15] Disrupting Continuity of Apple’s Wireless Ecosystem Security: New Tracking, DoS, and MitM Attacks on iOS and macOS Through Bluetooth Low Energy, AWDL, and Wi-Fi, https://tubiblio.ulb.tu-darmstadt.de/id/eprint/126124

[16] Anjan K Koundinya, Two-Layer Encryption based on Paillier and ElGamal Cryptosystem for Privacy Violation, I.J. Wireless and Microwave Technologies, 2021, 3, 9-15 Published Online June 2021 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijwmt.2021.03.02

[17] Bilal Hashim Hameed, Anmar Yahya Taher, Raed Khalid Ibrahim, Adnan Hussein Ali, Yasser Adnan Hussein, DOI: http://doi.org/10.11591/ijeecs.v26.i3.pp1781-1790

[18] Haneen Abdulrazak, Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Two fish, and Threefish, DOI: https://doi.org/10.17762/ijcnis.v14i1.5262, https://www.ijcnis.org/index.php/ijcnis/article/view/5262

[19] Akash Thakkar1, Ravi Gor2, Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal Transform, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 3, Ser. III (May. –June. 2022), PP 08-14 www.iosrjournals.org, https://www.iosrjournals.org/iosr-jce/papers/Vol24-issue3/Ser-3/B2403030814.pdf

[20] AKSA Anudini, G. Gayamini, and Prof. Thushara Weerawardane (2022); Cloud Data Security System Using Cryptography and Steganography: A Review; International Journal of Scientific and Research Publications (IJSRP) 12(9) (ISSN: 2250-3153), DOI: http://dx.doi.org/10.29322/IJSRP.12.09.2022.p12936

[21] **Emmanuel A. Adeniyi**, Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions, *Information* 2022, *13*(10), 442; **https://doi.org/10.3390/info13100442**