VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Fall Semester 2021-22

Information Security Analysis and Audit

Slot: F2/L11+L12

Course Code: CSE3501

J Component

Project Title:

Text and Image Encryption using Symmetric and Asymmetric Algorithms

Under guidance of:

Prof/Dr: IYAPPARAJA .M

Team members:

1.	Ajay Aadhav V V	18MIS0136
2.	Naveenkumar J	18MIS0395

Abstract:

Text Encryption:

With the rapid growing of internet and networks applications, data security becomes more important than ever before. Encryption algorithms play an important role in information security systems. In this, we have a study of the popular encryption algorithm: Blowfish and Cipher block chaining using AES. We overviewed the base functions and analyzed the security for algorithms. The main concern is about the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. Here the comparison is made on these parameters: speed, block size, and key size

ImageEncryption:

Vulnerability of communication of digital images is an extremely important issue nowadays, particularly when the images are communicated through insecure channels. To improve communication security, many cryptosystems have been presented in the image encryption literature. This project proposes a novel image encryption technique based on the algorithms DES, AES and RSA which is faster than current methods. The proposed algorithm eliminates the step in which the secrete key is shared during the encryption process. It is formulated based on the symmetric encryption (using DES and AES) and asymmetric encryption (using RSA). The image is encrypted using DES and AES, then, the secret key is encrypted by means of RSA and it is hidden in the ciphered image. The analysis results show that while enjoying the faster computation, our method performs close to optimal in terms of accuracy.

Introduction:

BLOWFISH:

Blowfish is a keyed, symmetric cryptographic block cipher designed by Bruce Schneier in 1993 and placed in the public domain. Blowfish is included in a large number of cipher suites and encryption products, including Splash ID. Blowfish's security has been extensively tested and proven. As a public domain cipher, Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like Splash ID that functions on a wide variety of processors found in mobile phones as well as in notebook and desktop computers.

Some of the Blowfish algorithm specifications can be summarized as

1. Symmetric block cipher.

2.64-bitBlock.

3. Variable-length key, from 32 bits (4 Bytes) to448

4. Run at an acceptable clock speed.

5. Suitable and efficient for hardware implementation

6. Unpatented and no license is required.

CIPHER BLOCK CHAINING:

In ECB mode, the problem is that there is a chance of leakage of information.

This is more vulnerable when two messages which has same two blocks of plain texts is being encrypted, the cipher texts blocks of the plain text blocks is same. With this, there is a chance that the attacker can come to know the relation be- tween the plain text blocks. He may not come to know the entire plain text but there is a chance to know some relationship between the plain text and the cipher text. But in CBC mode since the IV is random and the cipher of one plain text depends the previous plain text and hence different cipher texts are produced for same plain text block.

•CBC is a mode of operation for a block cipher (one in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block).

•Cipher block chaining uses what is known as an IV of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of cipher text to depend on all the preceding cipher text blocks.

•As a result, the entire validity of all preceding blocks is contained in the immediately previous cipher text block. A single bit error in a cipher text block affects the decryption of all subsequent blocks.

ImageEncryption:

The advance encryption standard (AES) specifies a federal information processing standards publication (FIPS) approved cryptographic algorithm that can be used to protect electronic data. It was publish by National Institute of Standard and Technology.

AES is a symmetric 128-bitblock encryption technique. AES works at multiple network layers simultaneously. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits. It provides following services:

- It is a politically safe decision: the encryption standard of the US National Institute of Standards and Technology (NIST), and the US government reportedly approves AES with 192 or 256-bit keys for encrypting top secret documents.

- Nobody yet has (publicly) a full attack on AES, or a partial attack that is practical (though some impractical partial attacks exist).

- AES is algebraically simpler than other block ciphers: effectively, it can be written as a series of mathematical equations.

DES was a generally utilized cryptosystem for securing the characterized information transmissions. DES is a symmetric key cryptosystem that is nothing but for both encryption process and decryption process, using same secret key. These improvements facilitate the threats and attacks on the information or data to uncover its secrecy progressively and load the enormous test of fulfill the undertaking of securing the communications

The **RSA encrypt** key is **encrypt** the **image**, so that it convert into cipher text format and it will be store as a text file. The opposite method of **encryption**, the reverse process is compute by another one decryption key of **RSA** algorithm and it decrypts the **image** from the cipher text.

Rivest Shamir Aldeman is the most commonly used public key encryption algorithm. RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider. RSA is too slow for encrypting large volumes of data but it is widely used for key distribution.

In the present communication images are widely use. One of the major issue with transfer the data over the Internet is the security and authenticity. The security is basically protecting the data from an unauthorized users or attackers. Encryption is one of the technique which is use for secure the information. Image encryption is a technique that convert original image to another format with the encryption techniques. The same way in the decryption no one can access the information without knowing a decryption key.

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
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

PROPOSED METHOD:

Text Encryption:

BLOWFISH:

The algorithm consists mainly of two parts; the key-expansion part and the data- encryption part. Key expansion converts a key of at most 448 bits into 4168 bytes. There is a P-array and four 32-bitS-boxes. The P-array contains 18 of 32-bit sub keys, while each S-box contains 256 entries. Data encryption occurs via a 16-round Feistel net- work. Each round consists of a key-dependent permutation, and a key- and data-de- pendent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Security attacks against network are increasing significantly with time. Our communication media should even be secure and confidential. For this purpose, these three suggestions arrive in every one's mind:

(i) one can transmit the message secretly, in order that it are often saved from hackers,

(ii) the sender ensures that the message arrives to the specified destination, and

(iii) the receiver ensures that the received message is in its original form and coming from the

proper sender.

For this, one can use two techniques,

(i) one can use invisible ink for writing the message or can send the message through the confidential person

(ii) one can use a scientific approach called "Cryptography".

Cryptography is that the technique wont to avoid unauthorized access of knowledge for instance , data are often encrypted employing a cryptographic algorithm in conjunction with the key management. it'll be transmitted in an encrypted state, and later decrypted by the intended party.

If a 3rd party intercepts the encrypted data, it'll be difficult to decipher. The security of recent cryptosystems isn't supported the secrecy of the algorithm, but on the secrecy of a comparatively small amount of data , called a secret key. the elemental and classical task of cryptography is to supply confidentiality by encryption methods.

CIPHER BLOCK CHAINING:

Block cipher is used to encrypt the text in which the algorithm is applied to encrypt a block of data rather than encrypting one bit after another as in stream ciphers. When a huge bulk of data has to be encrypted, block ciphers are widely used. It operates on a fixed length groups of bits. We have several block cipher modes of operations which use block cipher to provide authenticity or confidentiality. Here we compare AES algorithm with DES algorithm and hashing algorithm to determine that AES is better than the other two algorithms used for comparison.

Challenges:

Challenges faced in cipher block chaining algorithm:

- If one bit of the transferred message will be corrupted, it will damage the one more following block. Other blocks would be safe.
- In case of loss or an insert at least one bit into cipher text, there will be a shift of bits and borders of blocks that will lead to a wrong decryption of all subsequent blocks of cipher text.
- The malefactor can add blocks by the end of the ciphered message, supplementing with that a clear text.
- Two identical messages have identical cipher texts if the same initialization vector (initialization vector (IV)) was used.

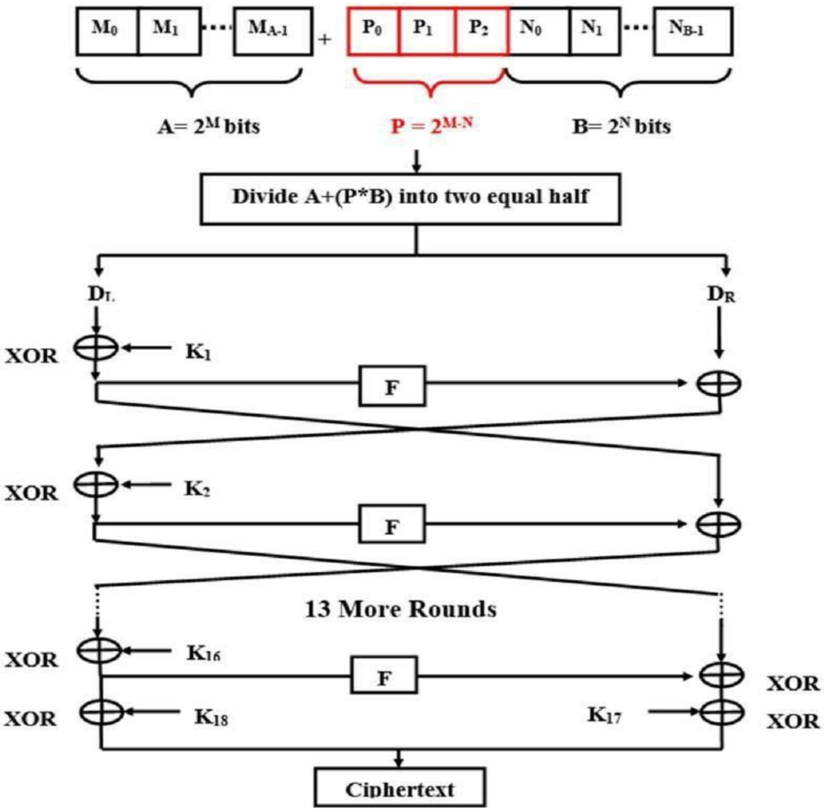
Challenges faced in blowfish algorithm:

- The challenges faced for Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel. Each pair of users needs a unique, so as number of users increase, key management becomes complicated. For example N(N-1)/2 keys re- quired.
- Blowfish can't provide authentication and non-repudiation as two people have same key. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput.
- The disadvantages of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel. Each pair of users needs a unique, so as number of users increase, key management becomes complicated. For example N(N-1)/2 keys re- quired.
- Blowfish is suitable for applications where the key does not change frequently like communication links or file encryptors.
- However for applications like packet switching or as one-way hash function, it is unsuitable. Blowfish is not ideal for smart cards, which requires more compact ciphers

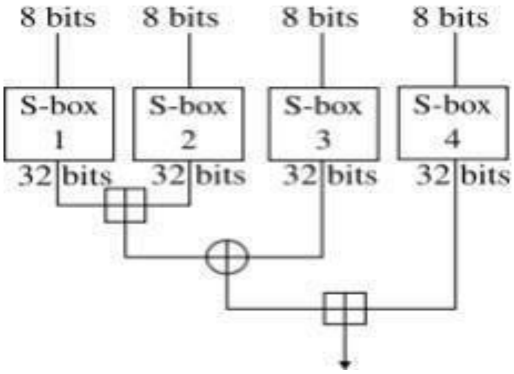
Assumptions:

With the rapid growing of internet and networks applications, data security becomes more important than ever before. Encryption algorithms play a important role in information security systems. In this, we have a study of the popular encryption algorithm: Blowfish and Cipher block chaining using AES. We overviewed the base functions and analysed the security for algorithms. The Objective is about the performance of algorithms under different settings, the presented comparison takes into consideration the behaviour and the performance of the algorithm when different data loads are used. Here the comparison is made on these parameters: speed, block size, and key size.

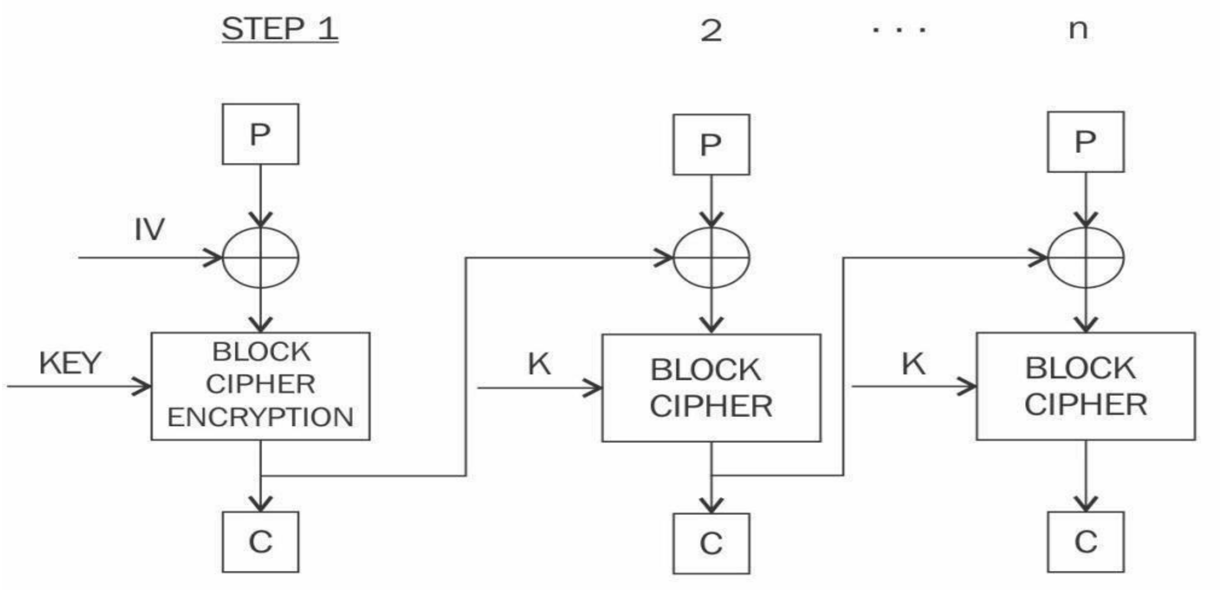
ARCHITECTURE SPECIFICATIONS: Blowfish algorithm architecture:



S- Box:



Cipher block chaining architecture:



2.1 Hardware specifications:

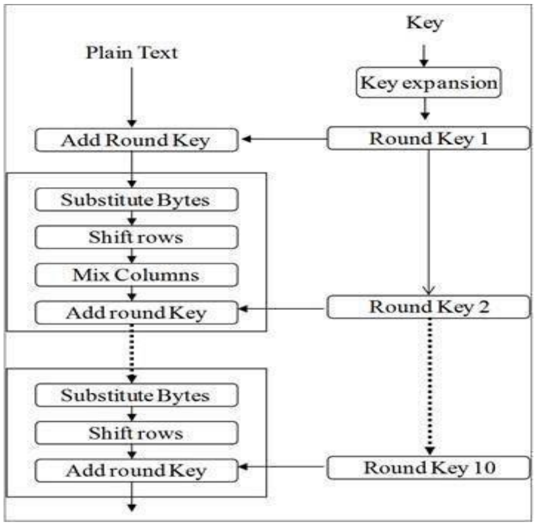
System configuration	:	Any Desktop or Laptop systems with high level
RAM	:	4GB/8GB for faster output
Hard Disk	:	500GB
Microprocessor	:	2.0GHz
Microprocessor type	:	Core i3/Core i5

2.2 Software specifications:

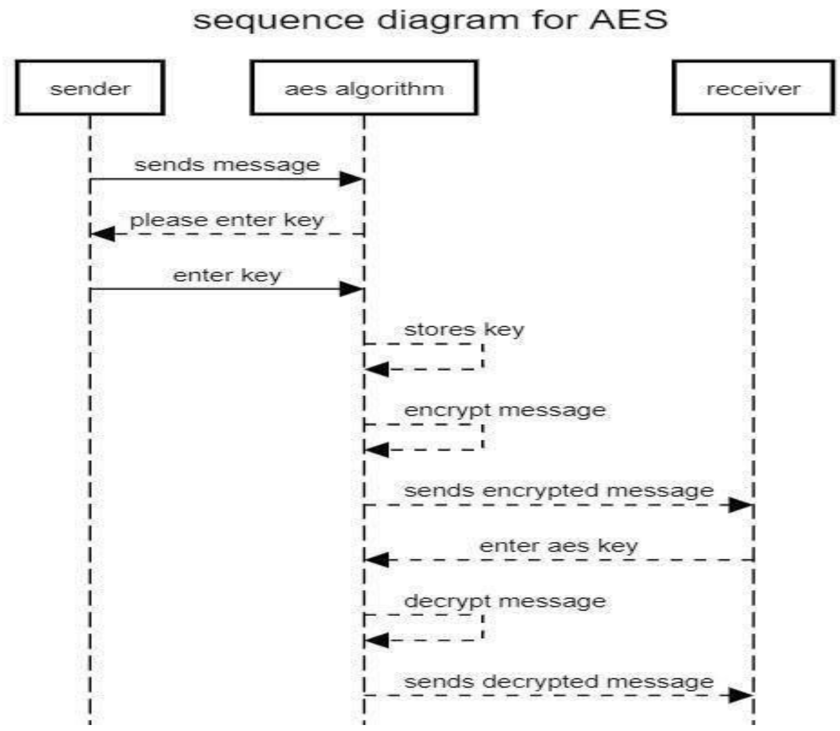
OS	:	Windows-10
Programming Language	:	Java, Python
Platform used	:	Netbeans,

SYSTEM DESIGN

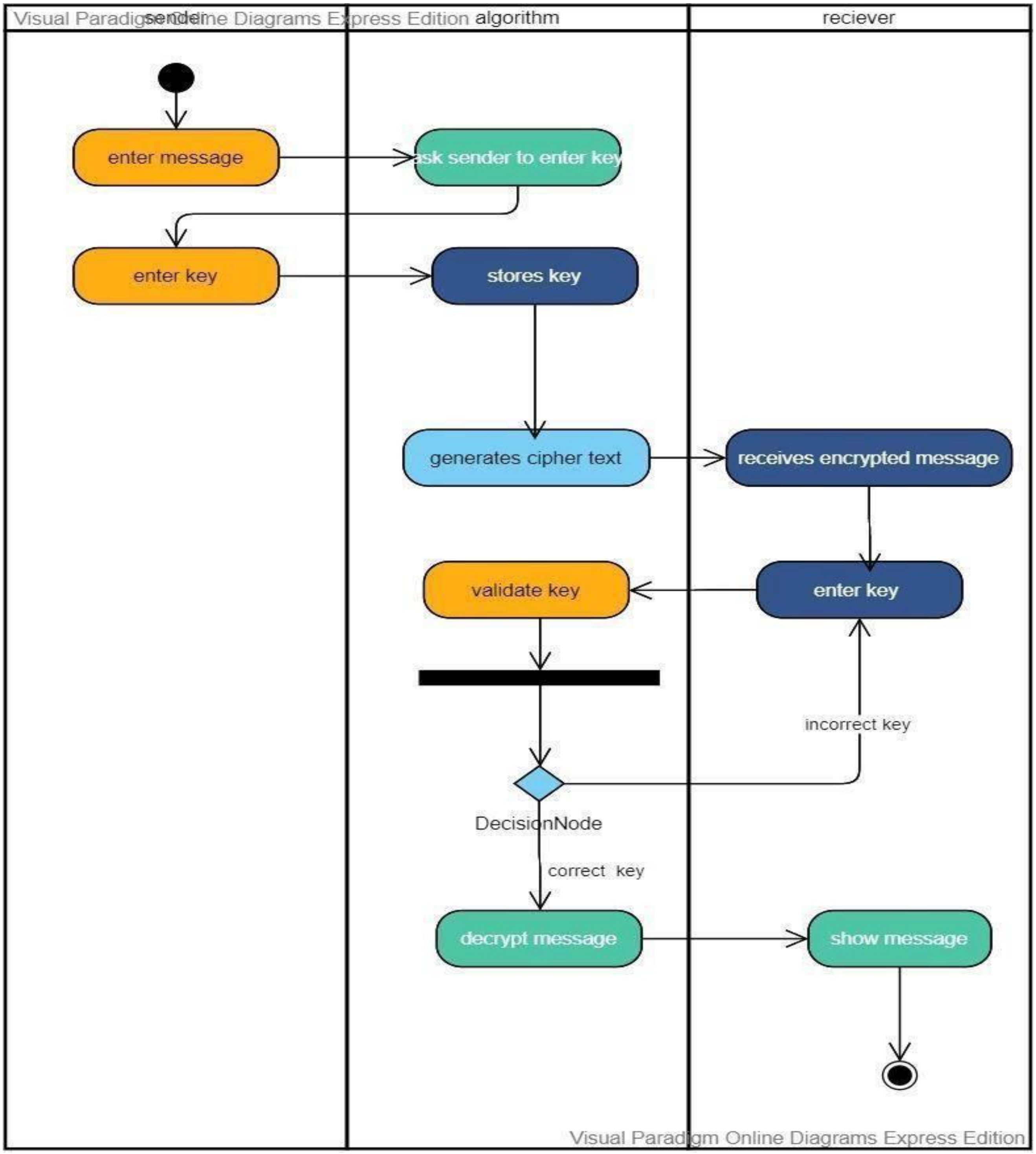
High-level design:



Low Level Design



Process flow of text encryption and decryption :



ImageEncryption:

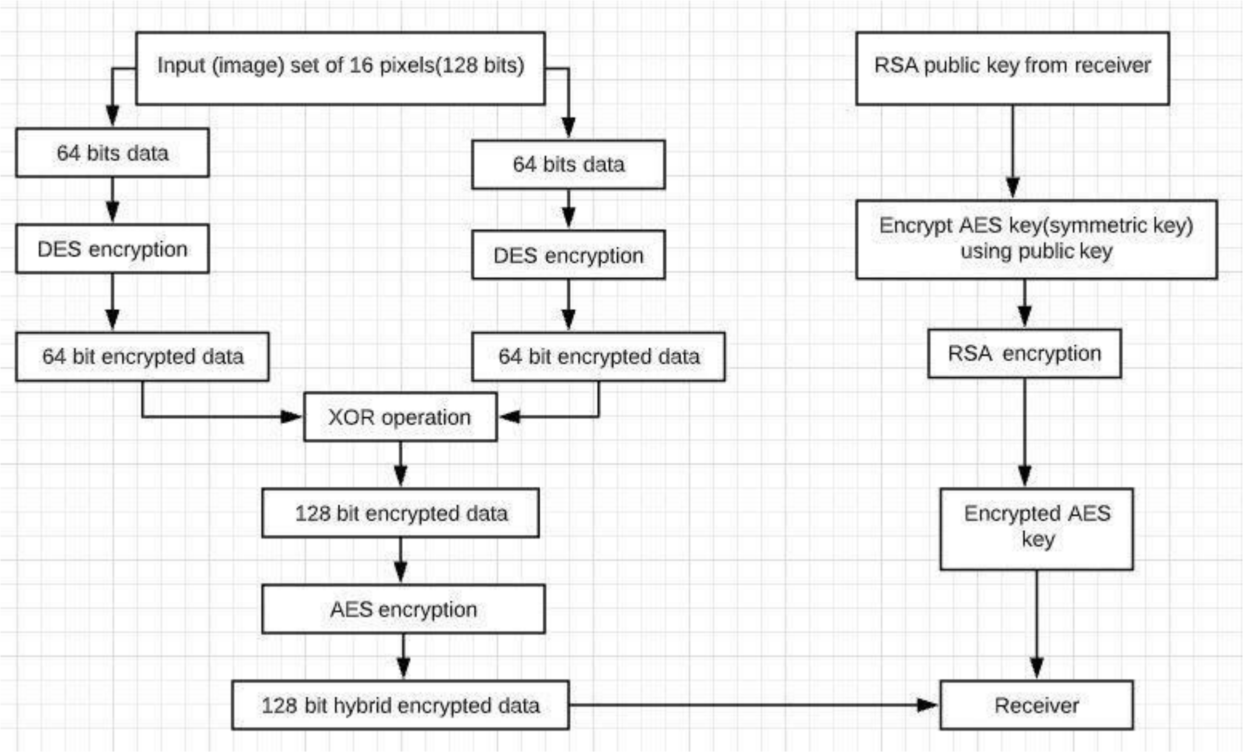
For image encryption we proposed a method making use of AES, DES and RSA algorithms in order to provide a secure channel for message transmission.

RSA: Though AES is perfect algorithm for image encryption in terms of security, speed and implementation, AES has no security proof, so we used RSA as it involves some mathematical proof. Also AES is a symmetric algorithm which means encryption and decryption is done by same key, there is no assured guarantee for the "secret key" being protected from unauthorized people. As RSA is an asymmetric algorithm it ensures the secure channel.

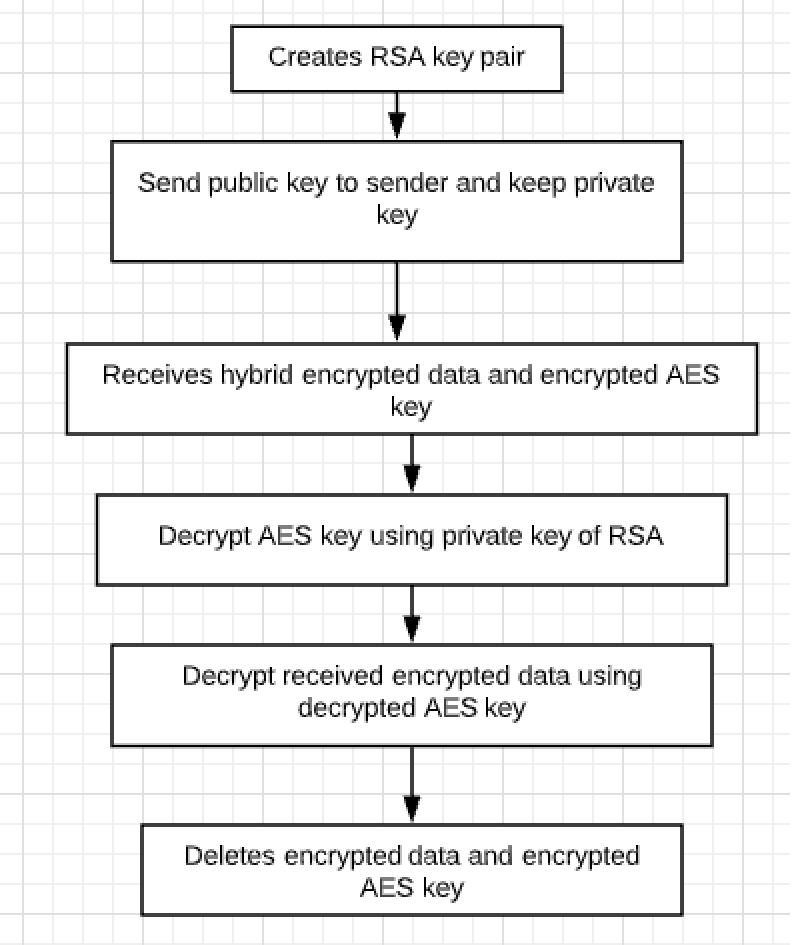
DES: On using DES we will be free from all sorts of algebraic and linear attacks in image encryption.

Tool used: LUCIDCHART

Sender:



Receiver:


Creates RSA key pair
Send public key to sender and keep private key
Receives hybrid encrypted data and encrypted AES key
Decrypt AES key using private key of RSA
Decrypt received encrypted data using decrypted AES key
Deletes encrypted data and encrypted AES key

Consider a communication between a sender (A) and a receiver (B):

Encryption:

- ✓ A obtains B's public key.
- ✓ Encrypts the message using DES and AES algorithms.
- ✓ Encrypts the AES symmetric key using B's public key. Send both of these encryptions to B.

Decryption:

- ✓ B uses here private key to decrypt AES key.
- ✓ Uses this decrypted symmetric key to decrypt the message sent.

2.1 Hardware specifications:

- System configuration : Any Desktop or Laptop systems with high level
- RAM : 4GB/8GB for faster output
- Hard Disk : 500GB
- Micro-processor : 2.0GHz
- Microprocessor type : Core i3/Core i5

2.2 Software specifications:

- OS : Windows-10
- Programming Language : Python
- Platform used : Python compiler (command prompt)

Literature survey by 18MIS0395 on "Text Encryption":

1)

Title	**Author &**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
A study of new trends in Blowfish algorithm.	Gurjeevan singh,ashwani kumar,KS sandha	Comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption.	From the results it is easy to observe that AES has an advantage over other algorithms in terms of encryption time, decryption time and throughput. But adding additional key and replacing the old XOR by new operation '#' as a purposed by this study to give more robustness to Blowfish Algorithm and make it stronger against any type of intrusion.	3DES showed poor performance results compared to other algorithms since it requires more processing power. In the case of changing data type such as image, RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption; Higher key size leads to clear change in the battery and time consumption. Blowfish also showed poor performance compared to AES and some operations need to be added so the blowfish algorithm becomes better,

Paragraph Inference:

The reenactment results demonstrate that AES has a superior execution than other normal calculations. AES should be better calculation which was contrasted with unique Blowfish Algorithm. Be that as it may, including extra key and supplanting the old XOR by new task '#' as a purposed by this investigation to give more power to Blowfish Algorithm and make it more grounded against an interruption. This development Blowfish Algorithm is progressively proficient in vitality utilization and security to diminish the utilization of battery control gadget. In the new proposed model of Blowfish by further expanding the key length, Blowfish will give the better outcomes.

References

[1] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."Dr.Dobb's Journal, March 2001, PP.137-139.

[2]Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."IBM Journal of Research and Development, May 1994, pp. 243-250.

[3] Diaa Salama Abdul. Elminaam, Hatem Abdul Kader and Mohie Mohamed Hadhoud, Evaluating the Effects of Symmetric Cryptography Algorithms on PowerConsumptionfor Different Data Types, International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.2010.

2)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**
Blowfish encryption Algorithm For information security	Saiku marmanku, kvasanth	In this paper, a Blowfish encryption algorithm for information security is designed and analyzed. In the proposed Blowfish algorithm reduce rounds of algorithm and proposed single blowfish round.	In the proposed Blowfish algorithm reduce rounds of algorithm and proposed single blowfish round. Here the algorithm is modified so it provides great security thus no one in between sender and receiver will hack the data	If the encryption process is done wrong for the blowfish algorithm, the decryption process will also remain wrong.

Paragraph Inference:

In the proposed system of blowfish algorithm reduced the rounds of blowfish algorithm and in the algorithm each single round is introduced new modified. In the blowfish algorithm there will be 64 bits then the bits are separate into 32bits and there will be four s-boxes. Each s-box contains 32bits. Now design the algorithm like two s-boxes connecting with Xor as like same other two 2 s-boxes connected with Xor and then from the two Xor added then from there get key plain text. The present simulation result shows that the encryption and decryption is done using blowfish algorithm. Here the algorithm is modified so it pro- vides great security thus no one in between sender and receiver will hack the data

References

[1] Alan G. Konheim. 2007. COMPUTER SECURITY AND CRYPTOGRAPHY.By John Wiley and Sons,Inc.

[2] AlfredJ.M.,PaulV.C.and ScottA.V.2001.HandbookofAppliedCryptography.FifthAddition.

[3] BruceSchneier. 1996.Applied Cryptography, SecondEdition:Protocols,Algoirthms, and Source Code in C. Wiley Computer Publishing, John Wiley and Sons,Inc.

3)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**
Using Blowfish Encryption to Enhance Security Feature of an Image	Shreya nk N Gowda	Blowfish using Mean square error and peak signal to noise ratio	The Encryption enhances the security. And the randomness of the algorithm security increases. The purpose of hidden information is secure perfectly.	The time taken is for MSE and PSNR values. It will be harder to differentiate even more that the standard LSB.

Paragraph inference:

Here the image will be encrypted using key and the image is break down into blocks of data. Each broken block is encrypted at random to one image. All the blocks are embedded into images and then sent to receiver using hashing. At the receiver side the image is extract the correct sequence of data by the hash image. The decryption is done using the key send by the sender. The mean square error (MSE) and peak signal to noise ratio (PSNR) are used to compare image compression quality. MSE represent the cumulative squared error and PSNR represent a measure of the peak error.

References

[1] TNieandTZhang."AstudyofDESandBlowfishencryptionAlgorithm."TENCON 2009 IEEE Region 10 Conference. pp 1-4, January2009

[2] Babu, K Ravindra, S U Kumar, and A V Babu. "A Survey on cryptography and Steganography methods for information security." International Journal of Computer Applications Volume 12 Issue 3 pp 13-17, December2010.

[3] K Wu and C Wang, “Steganography using reversible texture synthesis” IEEE Transactions on Image Processing Vol.24 pp 130-139,January2015.

4)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**
Comparative study of Symmetric key algorithms DES, AES and blowfish	H. Fathima, KSR Matriculation, KSR kalvi nagar	Comparing the three encryption algorithms which are generally used for bulk data and link encryption	Permutation problem is cleared in DES. Blowfish algorithm allows a tradeoff between higher speed and higher security. AES has advantage over the DES in terms of throughput & decryption time	There can be same output from the S Boxes on different inputs on permutation DES

Paragraph Inference:

This paper presents a peer analysis in the field of encryption algorithms, concentrating on private key block ciphers which are generally used for bulk data and link encryption. We have initially surveyed some of the popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to unreadable state. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information.

References

[1].Schneier, Bruce (2004-09-27). "Saluting the data encryption legacy". CNet. Retrieved 2015-07-22.

[2]. Biaoshuai Tao & Hongjun Wu (2015). "Improving the Biclique Cryptanalysis of AES”.

[3]. SPIEGEL ONLINE, Hamburg, Germany (28 December 2014). "Inside the NSA's War on Internet Security". SPIEGEL ONLINE. Retrieved 4 September 2015.

5)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**
Practical implementation of blowfish algorithm for boosting security aspect in networks	B Suresh kumar, Rohit kumar upadhya	The brief analysis of blowfish algorithm which is a symmetric block cipher that can be used for both encryption and decryption	Blowfish algorithm is one of the best block cipher technique for large amount of data blocks. Sub-keys are created with help of permutation and substitutions.	An attacker might find two keys that differ only in 64 bit value XOR ed with P1 and P2 known as sub keys produce the same encrypted value. If so he can find two keys that produce all the same sub keys

Paragraph inference:

Secret key cryptography is older one and it contains only one key on both sides for encryption and decryption based on Data encryption standards. Blow fish algorithm is one of the best block cipher technique for large amount of data blocks. In this research we studies deeply about the blow fish algorithm and its operation. Also studied how to create sub key with the help of permutation and substitutions.

References

[1] B. Schneier, Applied Cryptography, John Wiley & Sons, New York,1994.

[2] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)

[3] Fast Software Encryption, Cambridge Security Workshop Proceedings (December

1993), Springer-Verlag, 1994, pp.191-204.

6)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**
Performance Analysis of AES and Blowfish Encryption Algorithm	M.Abirami, S. Chellaganeshavalli	The AES and Blowfish encryption algorithm. Basically these algorithms are symmetric key encryption algorithms using block cipher	Blowfish has superior performance than AES since Blowfish has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm.	BLOWFISH algorithms since it requires more processing power. The AES and Blowfish encryption algorithm. Basically these algorithms are symmetric key encryption algorithms using block cipher

Paragraph inference:

The main objective of this dissertation is to analyze encryption security, evaluated encryption speed and power consumption for both the algorithms. It is proved that the Blowfish encryption algorithm may be more suitable for wireless network application security.

References

[1] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001 http://csrc.nist.gov/publications /fips/fips197/fips-197.pdf

[2] Bruce Schneier. "The Blowfish Encryption Algorithm Retrieved", October 25, 2008.

[3] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" proceedings of International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp.125-127

7)

Title	**Author**	**Algorithm/methodology used**	**Advantages**	**Disadvantages**

Performance Study of Key Developer Data Encryption and Decryption Algorithm (KDDEDA) with AES, DES and BLOWFISH	Miss. A.Usha, Dr. A. Subramani M.Phil. Scholar	The proposed a new cryptographic algorithm named as KDDEDA [Key Developer Data Encryption and Encryption Algorithm]	The traditional algorithms have some of the drawbacks like speed, key size and performance. this can be satisfied here	There is no data protection along the way. However, full disk encryption still has its drawbacks. The first is that it cannot protect data in transit.

Paragraph inference:

Information security is an important issue in network communication. Because of the significance, accuracy and sensitivity of the information it is a big security and privacy issue, making it necessary to find appropriate solution, security and privacy has become as important concern. Cryptography is making sure to secured data protection. Cryptography concept is used facilitate for secret communication among the military communications. The traditional algorithms have some of the drawbacks like speed, key size and performance. The proposed a new cryptographic algorithm named as KDDEDA [Key Developer Data Encryption and Encryption Algorithm], The KDDEDA using to transmit confidential data for source to destination with speed data transmission and performance. KDDEDA also analyse encryption/decryption time, memory space, key size, block size and performance.

References

[1] A.Subramani and A.Usha,Analyse The Encryption And Decryption Conversion Time Of Various Algorithms On Different Setting Of Dataset. I-manager‟s Journal on Information Technology. Vol. 5 l No. 3 l June – August 2016.

[2] Srinivas B.L, Anish Shanbhag and Austin Solomon D‟Souza.”A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm”. International Journal of Innovative Research in Computer and Communication Engineering.Vol.2, Special Issue 5, October2014.

[3] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar. “Comparative Analysis between DES and RSA Algorithm‟s”. International Journal Of Advanced Research In Computer Science And Software Engineering. Volume 2, Issue 7, July 2012.

Conclusion drawn on analysis of above papers:

Some of the research papers described about the comparison between the different symmetric algorithms using the different comparisons and for some comparisons, AES was the best encryption technique that is to be used and for some comparisons blowfish was the better algorithm. Blow fish algorithm is one of the best block cipher technique for large amount of data blocks. The reenactment results demonstrate that AES has a superior execution than other normal calculations. AES should be better calculation which was contrasted with unique Blowfish Algorithm. Be that as it may, including extra key and supplanting the old XOR by new task '#' as a purposed by this investigation to give more power to Blowfish Algorithm and make it more grounded against an interruption. This development Blowfish Algorithm is progressively proficient in vitality utilisation and security to diminish the utilisation of battery control gadget. In the new proposed model of Blowfish by further expanding the key length, Blowfish will give the better outcomes. So the new proposed blowfish algorithm provides more secure encryption and decryption

Literature survey by 18MIS0136 on "Text Encryption":

1)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
PCBC: A Secure Parallel Cipher Block Chaining Mode of Operation based on logistic Chaotic Map	El-Semary, A. M., Azim, M. M. A., & Diab, H	secure parallel cipher block chaining (SPCBC) mode of operation CCM mode for the secure automated key management techniques	Resist attacks including the known plaintext and chosen plaintext/cipher-text attack	Error propagation is handled till 1 block

Paragraph inference:

In this Secure Parallel Cipher Block Chaining (SPCBC) method of activity that gives improved security over the present modes. The SPCBC mode accomplished this stringent security through consolidating one-time chain keys with plaintext obstructs before their encryption. The SPCBC used the highlights of irregularity, clammer like conduct, and affectability to beginning conditions and control parameters of calculated guide to acquire dynamic chain keys. Also, it utilized a nonce to ensure the uniqueness of the created chain keys.

References

[1] W. Stallings, Cryptography and Network Security, 5th ed. Boston, MA: PrenticeHall,2011

.[2] L.R.Knudsen,"Blockciphers:a survey," in State of the Artin Applied Cryptography.Heidel-berg: Springer, 1998, pp.18-48.

[3] H. M. Heys, "Analysis of the statistical cipher feedback mode of block ciphers," IEEE Transactions on Computers, vol. 52, no. 1, pp. 77-92,2003.

2)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
Security Issues in Cloud Computing: A Survey.	Kumar, N., & Samriya, J. K	Magnified Cipher Block Chaining Mode Encryption using DES for encryption. Enhanced Cipher Block Chaining Mode Decryption	To prevent data security attacks in the cloud.	By increasing the block size, the method should use the suitable size of the data of a particular algorithm, So that they can also encrypt for a huge amount of the data and time complexity can decrease

Paragraph inference:

The Encrypted information utilizing amplified figure square anchoring method of activity gives more security instead of the existed figure obstruct in light of the fact that this accompanied another thought that in every current calculation the yield of the primary square is send as a contribution to the following square yet here, they are sending the yield of the principal hinder as a contribution to the another square depending up on the mid qualities and position of squares. By utilizing the calculation, they encode and interpret the data and giving greater privacy additionally to give greater security they have sent the KEY to approved individual as it were.

References

[1] Aly M. El-Semary, Mohamed Mostafa A. Azim and Hossam Diab, "SPCBC: A SecureParallel Cipher Block Chaining Mode of Operation based on logistic Chaotic

[2] Map," KSII Transactions on Internet and Information Systems, vol. 11, no. 7, pp.

3608-3628, 2017. DOI: 10.3837/tiis.2017.07.017

3)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
Analysis of the statistical cipher feed- back mode of block ciphers	Heys, H. M	Implementation of an SCFB System	adaptive chosen plaintext attacks recovery time from sync losses	the delay caused by the SCFB mode of operation the buffering requirements are directly equivalent to the delay of data as it is transferred through the SCFB encryption system.

Paragraph inference:

The statistical cipher feedback (SCFB) mode, SCFB mode configures the block cipher as a key stream generator for use in a stream cipher such that it has the property of statistical self synchronization, thereby allowing the stream cipher to recover from bit slips in the communication channel. In this Statistical self-synchronization mode it involves feeding back cipher text to the input of the block cipher like the conventional cipher feedback (CFB) mode, except that the feed- back only occurs when a special synchronization pattern is recognized in the cipher text. The efficiency, resynchronization, and error propagation characteristics of SCFB is examined and comparison of these to conventional modes such as CFB and output feedback (OFB) is made in the paper.

References

[1] O. Jung, C. Ruland, "Encryption with Statistical Self-Synchronization in Synchronous Broadband Networks", Proc. Cryptographic Hardware and Embedded Systems (CHES '99), pp. 340-352, 1999.

[2] A.J. Menezes, P. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography., 1997

[3] "Information Technology Security Techniques Modes of Operation for an -bit Block Cipher", 1997

4)

Title	Author	Algorithm/ methodology used	Advantages	Disadvantages
A resourceful combined block cipher mode of operation for packetized network communication	Adekunle, A. A., &Wood- head, S. R	EAD algorithm Based on the CTR mode	pre-computation attacks ciphertext block manipulation	The performance evaluation of con- struct in hardware and when it is integrated in a security framework is not discussed.

Paragraph inference:

A combined block cipher mode of operation is represented in this paper that provides an efficient authenticated encryption with associated-data (AEAD) security service for packet based network communication on a large scale. This AEAD schemes employ a nonce, this nonce is done in order to achieve semantic security in the system. So, For this purpose the sender will need to maintain the state thoroughly. The method by which the associated-data, H, is made known to the receiver is outside of the model and they do not consider the associated data that has to be part of the cipher text, though the receiver will need it in order to decrypt.

References

[1] M. Dworkin, “Recommendation for block cipher modes of operation: methods and techniques,” Na- tional Institute of Standards and Technology, Washington, DC, Report No.NIST-SP-800-38A, 2001.

[2] J. Daemen and V. Rijmen, “AES Proposal: Rijndael,” Sep. 1999; http://citeseerx.ist.psu.edu/ viewdoc/ download;jsessionid=802425701A71D9FD462B507C726C7A01?doi=10.1.1.36.640&rep=rep1&type=pdf.

[3] W. Stallings, Cryptography and Network Security, 2nd ed. Upper Saddle River, NJ: Prentice-Hall,1999.

5)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
Quantitative evaluation of chaotic cbc mode of operation	Abidi,A., Wang, Q., Bouallegue, B.,Mach-hout, M., & Guyeux, C	chaotic CBC mode of operation by using Devaney’s Chaotic Dynamical Systems	effects of a modification of the IV	This mode of operation does not possess other qualitative properties of disorder like the topological mixing.

Paragraph inference:

In this paper, both expansivity and sensibility of symmetric ciphers are regarded for the scenario, in the case of the CBC mode of operation. These quantitative topology metrics is being taken from the mathematical theory of chaos that al- lows to measure in which extent a slight error in the initial condition is magnified during iterations. In this approach It is stated that, in addition to being chaotic as defined in the following Devaney’s formulation, the CBC mode of operation is indeed largely to deal sensible to initial errors or modifications on either the IV or the message to encrypt. When Its expansivity has been regarded too, but this property is not satisfied, as it has been established thanks to a counterexample.

References

[1] A. Adekunle and S. R. Woodhead, “Aresourceful combined block cipher mode of operation for packetised network communication,” in Proceedings of 2010 4th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST), Amman, Jordan, 2010, pp. 180-185.

[2] H. M. Heys and L. Zhang, “Pipelined statistical cipher feedback: a new mode for high-speed self- synchronizing stream encryption,” IEEE Transactions on Computers, vol. 60, no. 11, pp. 1581-1595,2011.

[3] O. Jung and C. Ruland, “Encryption with statistical self-synchronization in synchronous broad- band networks,” in Proceedings of the 1st International Workshopon Cryptographic Hardware and Embedded Systems (CHES’99), Worcester, MA,1999, pp. 340-352.

6)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
Analytical Study on Encryption Techniques and Challenges in Network Security	Anuraj C.K1 , Dr.Shelbi Joseph2	symmetric algorithms such as DES, 3DES, AES, and Blowfish are compared in this paper to evaluate the efficiency	It will be useful to identify most suitable algorithm for different application areas like cloud, Bigdata, IOT, WSN and MANET.	Recovery of complex data Like all other types of encryption, the disk encryption of full disk is that the recovery of data on disks is complicated. Think about it, if encrypted data could be easily restored, encryption would be meaningless.

Paragraph inference:

This paper presents the various ways to classify and compare different symmetric encryption algorithms based on the process, structure and modes used for encryption and decryption. Also the performance of the widely used symmetric algorithms such as DES, 3DES, AES, and Blowfish are compared in this paper to evaluate the efficiency. The encryption algorithms are used by many application areas, but most of them are not free from attacks. The analysis of block cipher encryption algorithms based on the application areas and vulnerability to various attacks are listed in this paper.

References

[1]. National Bureau ofStandards – Data Encryption Standard, FIPS Publication 46, 1977.

[2]. Wayne G. Barker, "Introductiontotheanalysis of the Data Encryption Standard (DES)", A cryptographicseries, Vol. 55, p. viii + 190, Aegean Park Press, 1991.

[3]. J. Daemen and V. Rijmen, "AES Proposal: Rijndael", Original AES submissiontoNIST, 1999. AES Processing Standards Publications, http://www.csrc. nist.gov/publications/fips/fips197/fips-197.pdf

[4]. BruceSchneier, "TheBlowfishencryption algorithm", Dr. Dobb'sJournalof Software Tools, 19(4), p. 38, 40, 98, 99, April 1994

7)

Title	**Author**	**Algorithm/ methodology used**	**Advantages**	**Disadvantages**
An Introduction of Advanced Encryption Algorithm: A Preview	Asfiya Shireen Shaikh Mukhtar1 , Ghousiya Farheen Shaikh Mukhtar2	Encryption and decryption process used mathematical calculation with some shifting and rotating operation with or without a key. Cryptography can be divided into three types of algorithm Symmetric key algorithm, asymmetric key algorithm and hash function.	Confidentiality can be achieved by encryption and decryption. The method of disguising plaintext result in such a way as to hide its substance is called encryption.	There is no data protection along the way However, full disk encryption still has its drawbacks. The first is that it cannot protect data in transit

Paragraph inference:

Cryptography provides the confidentiality, integrity, authentication, nonrepudiation Confidentiality is the process of maintaining the secrecy of information and data.

Confidentiality can be achieved by encryption and decryption. The method of disguising plaintext result in such a way as to hide its substance is called encryption. Encryption plaintext result in unreadable gibberish called cipher text. The process of reverting cipher text to its original plaintext is called decryption. Encryption and decryption process used mathematical calculation with some shifting and rotating operation with or without a key. Cryptography can be divided into three types of algorithm Symmetric key algorithm, asymmetric key algorithm and hash function.

References

[1] Pratap Chandra Mandal,"Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)ISSN:2277 128X, Volume 2,Issue 9, September 2012

[2] W. Stallings, ''Cryptography and Network Security 4th Ed,'' Prentice Hall, 2005

[3] Shashi Mehrotra Seth, Rajan Mishra on " Comparative Analysis Of Encryption Algorithms For Data communication " in IJCST Vol. 2, Issue 2, June 2011 I,pp. 292-294

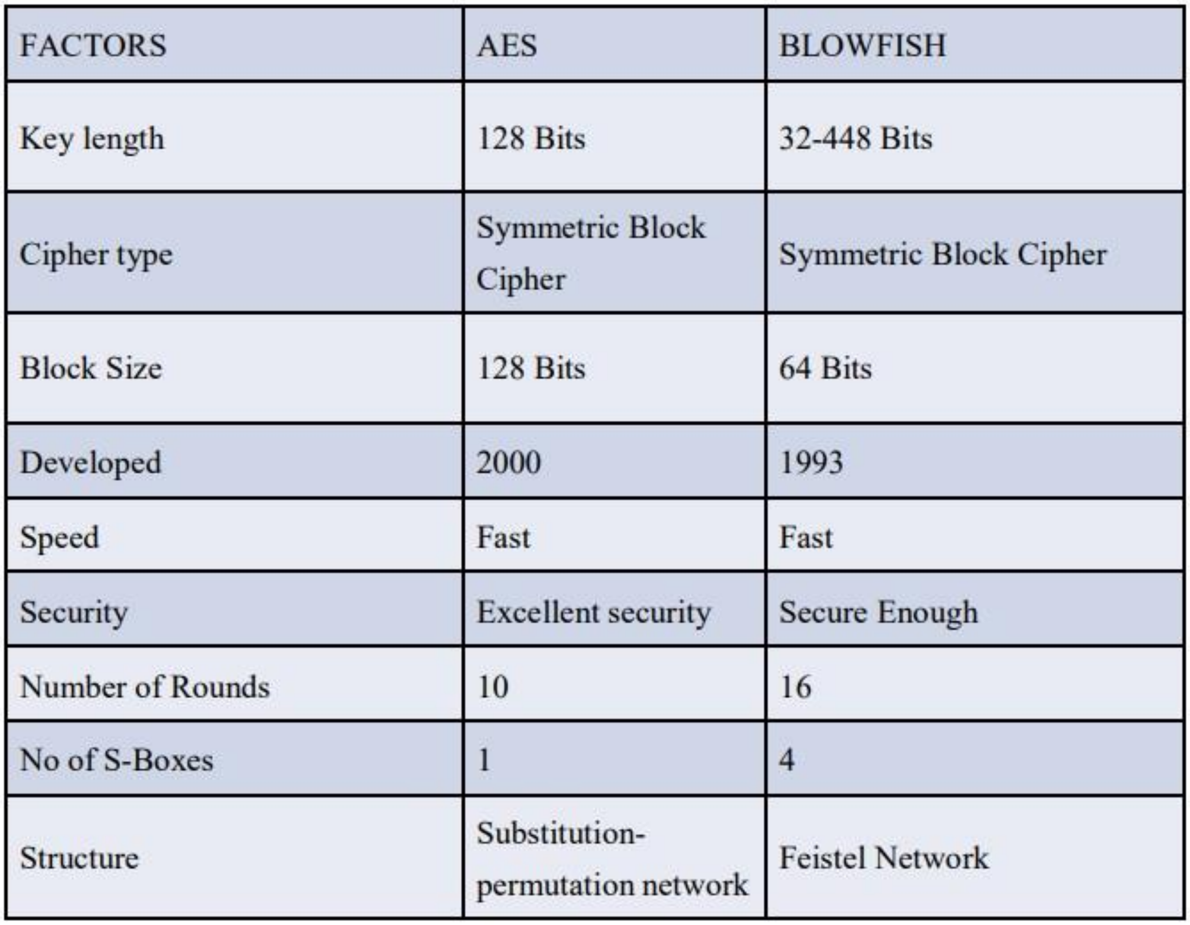
[4] Monika Agrawal, Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882.

Conclusion drawn from analysis of above papers:

In ECB mode, the problem is that there is a chance of leakage of information.

This is more vulnerable when two messages which has same two blocks of plain texts is being encrypted, the cipher texts blocks of the plain text blocks is same. With this, there is a chance that the attacker can come to know the relation be- tween the plain text blocks. He may not come to know the entire plain text but there is a chance to know some relationship between the plain text and the cipher text. But in CBC mode since the IV is random and the cipher of one plain text depends the previous plain text and hence different cipher texts are produced for same plain text block.

COMPARISON BETWEEN THE CIPHER BLOCKCHAINING USING AES AND BLOWFISHALGO-RITHM



FACTORS	AES	BLOWFISH
Key length	128 Bits	32-448 Bits
Cipher type	Symmetric Block Cipher	Symmetric Block Cipher
Block Size	128 Bits	64 Bits
Developed	2000	1993
Speed	Fast	Fast
Security	Excellent security	Secure Enough
Number of Rounds	10	16
No of S-Boxes	1	4
Structure	Substitution-permutation network	Feistel Network

Literature survey by 18MIS0395 on "Image Encryption":

S.No	Title	Author and year; Reference	Algorithm/ methodology used	Advantages	Drawbacks
1	Secure Image encryption through key hashing and wavelet transform techniques	Tapas Bandyopadhyay Bandyopadhyay , B N Chatterji On February 2012 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.7270&rep=rep1&type=pdf	Digital Image Encryption	The proposed algorithm does not provide any clue for statistical attack. The encrypted image histogram, approximated by a uniform distribution, is quite different from plain image histogram. In the proposed encryption process, for creating confusion the image wavelet transform is first calculated and then converted into binary string and the hash of the secret key value (SHA1) is finally bit xored to create the encrypted image.	An attacker can analyze the histograms of an encrypted image by using some attacking algorithms to get some useful information of the original image. The proposed image encryption scheme exploit the security behavior of the hash function and wavelet transform of the image.
2	A Novel Image Encryption Approach Based on a Hyperchaotic System, Pixel-Level Filtering with Variable Kernels, and DNA-Level Diffusion	Jiang wu,Jiayi Shi and Taiyong Li on December 2019 https://www.mdpi.com/1099-4300/22/1/5	Pixel-level Filtering with kernels of variable shapes and parameters , and DNA-level Diffusion, so-called PFDD	permutation or diffusion is conducted with different-levels of data (pixel-level, bit-level, and DNA-level), improving the effectiveness of the PFDD; a novel pixel-level filtering strategy with different kernel types and parameters determined by hyperchaotic sequences increases the diversity of kernels and hence enhances the security of	A kernel with a fixed shape and fixed parameters is used to do convolution. Its speed slightly underperforms against remaining methodologies like IC-BSIF.

3				the PFDD; and the DNA-level diffusion is able to expand a tiny change in a plain image to the whole cipher image to resist differential attacks very well.	
4	Image Security using AES and RNS with Reversible Watermark ing	Prof. Prajakta Bhangale , Anushree Gawad , Jyoti Maurya, Rucha S. Raje on may 2017 http://ijiset.com/vol4/v4s5/IJISET_V4_I05_53.pdf	AES and RNS with reversible watermarking	Applying hybrid of DWT and DCT transforms helps to overcome the drawbacks of individual methods and helps in effective watermarking. The proposed combination is highly efficient as it enhances image security and provides authentication.	Most of the signal energy lies in low-frequency sub band. This band contains the most important visual information of an image. High frequency bands of the image are often removed during compression or noise attacks.
5	An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems	Abdulkarim Amer Shtewi,Bahaa Eldin M.Hasan,Abd El Ratah Hegazy on may 2010 https://iceeng.journals.ekb.eg/article_33293_d49b3b7dd9443981193ba2416a27d26a.pdf	Advanced Encryption standard(AES)	The encrypted images (cipher image) regions are totally invisible. The visual inspection shows the possibility of applying the proposed MAES successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them. The histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.	The running speed is low, particularly for real time Internet multimedia application

6	An Analysis of Most Effective Virtual Machine Image Encryption Technique for Cloud Security.	Mr. RakeshNag Dasari,Dr. Y.Prasanth, Dr.O.NagaRaju on November 24,2017 http://www.ripublication.com/ijaer17/ijaerv12n24_218.pdf	DES, RSA, AES, Dynamic Encryption	The virtual machine images are in raw format and service related information cannot be extracted directly, nonetheless the VMs can be replicated easily from the VM Images.	The file format is limited in use as the growth of dat and applications generating more data cannot be predefined. Due to the lack of delta change management properties, the portability is restricted
7	Image Encryption with RSA and RGB randomize d Histograms	Gajendra Singh Chandel, Pragna Patel on May 2015 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1080.2550&rep=rep1&type=pdf	RSA(Rivest, Shamir, Adleman)	Then RSA is applied for encryption on the split data and it will be decrypted by the intended user and join all the split data by applying the reverse mechanism which is also bared by security key. So two key securities are applied first for split data and second for encryption.	Chaos-based ciphers are susceptible to traditional differential and linear cryptanalysis attacks.
8	A Survey on Image Encryption and Decryption using Blowfish & Watermark ing	Preeti Gaur, Neeraj Manglani on May 2015 https://d1wqtxts1xzle7.cloudfront.net/48662748/A_Survey_on_Image_Encryption_and_Decryption_using_Blowfish___Watermarking.pdf	BlowFish and WaterMark ing	Concept of Nesting increases embedding capacity of watermark into the main image. Encryption of watermarks before embedding them into main image helps to increase the security of the watermark. Use of Blowfish algorithm helps to make the method more robust.	The disadvantage of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel. Each pai of users needs a unique, so as number of users increase, key management becomes complicated Blowfish can't provide

9					authentication and non-repudiation as two people have same key. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput
10	Chaos Image Encryption based on DCT Transforms and Henon Map	Abdullah M.Awad, Rehab F.Hassan, Ali M.Sagheer on october 2015 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.735.386&rep=rep1&type=pdf	RC4 based on Discrete Cosine Transform (DCT) by using Henon map	The key space is enough to protect this method and refuse the brute force attack with high security. It is fast technique where the average of each encryption or decryption stag. The reconstructed image has good quality compared to original image. In DCT the information transmission is very low and key space is great enough to face the aggressive attack with acceptable encryption result.	

<u>Conclusion drawn from analysis of above papers:</u>

Network security is the most vital Component in Information security because it is responsible for securing all information passed through networked computers. From the above literature survey I realized that DES algorithm purpose is to provide standard method for protecting sensitive commercial and unclassified data. In this same key is used for both encryption and decryption while AES algorithm is known formats great security and speed in both hardware and software implementation. When coming to RSA, it is asymmetric algorithm unlike AES and

DES. RSA is widely used public-key algorithm. It is used for encryption to provide security so that only concerned user can access it.

While RSA and AES are not scalable, DES is scalable due to varying key and block size. Power Consumption is low for AES and DES while it is high for RSA. The simulation speed is faster in all three algorithm. As RSA takes longer time for encryption and decryption, AES & DES come up with relatively lower time for encryption and decryption. Though AES provides high security and fast encryption and decryption process, there is no security for "symmetric key" as it is a symmetric algorithm.

On the basis of my literature survey I found many issues regarding security, processing time, speed, sensitivity etc., but in this project we came up with a better solution of using all the three algorithm DES, AES &RSA which all image encryption which is free from all sorts of attacks like denial of service attacks, Man-in-the middle attack, Statistical attacks etc..

Literature survey by 18MIS0136 on "Image Encryption":

S.No	Title	Author and year; References	Algorithm/ methodology used	Advantages	Disadvantages
1	Image Encryption Using Chaotic Maps	Priya R Sankpal, P A Vijaya 31 March 2014	Chaotic maps	One possible solution to this problem is to encrypt the data. The data can be text, image, audio, video etc. In today's world most of the multimedia applications involve images. Earlier image encryption techniques like AES,DES,RSA etc. exhibit low levels of security and also weak anti attack ability. This problem was overcome by using chaos based cryptography	The chaotic systems are very sensitive to initial conditions and control parameters which make them suitable for image encryption
2	File Encryption, Decryption Using AES Algorithm in Android Phone	Suchita Tayde , Asst. Prof. Seema Siledar 5, May 2015	AES	AES algorithm is not only for security but also for great speed. It can be implemented on various platforms especially in small devices like mobile phone. Encryption can provide security. This application allows user to run this application on android	Although when the data size was very small this difference was not clearly visible. But for file having size greater than 100 KB, it was very clearly visible.

				platform to encrypt the file before it is transmitted over the network.	
3	Survey of Chaos based Image Encryption and Decryption Techniques	Ephin M Assistant Professor SG/IT Karunya University Coimbatore, India Judy Ann Joy PG Scholar, MMT Karunya University Coimbatore, India N. A. Vasanthi Dean/CSE Nehru Institute of Engg.&Tech. Coimbatore, India	AES, DES and RSA algorithms	Nowadays security becomes an important issue of communication and storage of images. One of the method used to ensure the high security of images is encryption. Images are used in many fields such as biometric authentication, medical science, military; they are stored or transferred through the network and the security of such image data is important. Due to some intrinsic features of the images, such as bulk data capacity and high correlation among pixels	Not suitable for practical applications
4	Digital color image encryption using RC4 stream	Riah Ukur Ginting, 02 December 2013	RC4	A new secure algorithm for image encryption, which based on RC4 stream cipher algorithm and chaotic logistics map. The results are	very sensitive to small changes of key

	cipher and chaotic logistic map			(i) is able to make the cipher-image cannot be visually identified, (ii) can eliminate the statistical correlation between the plain-image and cipher-image	
5	Simulation of Image Encryption using AES Algorithm	P.Karthigai kumar, 2011	AES	Optimized and Synthesizable VHDL code is developed for implementation of encryption and process. Xilinx ISE9.2i software is used for synthesis. Timing simulation is performed to verify the functionality of the designed circuit.	Most of the work has been presented on hardware implementation of AES using FPGA
6	A Review on DES, AES and Blowfish for Image Encryption & Decryption	Aarti Devi1 , Ankush Sharma2 , Anamika Rangra,2010	AES,DES,BLOWFISH	In today's world it is a crucial concern that while transfer image from one network to another network over the internet, the proper encryption and decryption is applied so that unauthorized access can be prevented. Surveys and researches are done some problem identification.	If the images have large data size and also has real time constrain problem hence similar method cannot be used to protect images as well as text from unauthorized access.

7	Securing Medical Images by Image Encryption using Key Image	Shrija Somaraj Research Scholar Bharathiar University Coimbatore Chennai, India, October 2014.	Image Encryption, Image Decryption , Bit Plane, XOR operation, Key image.	The methods use a binary image of the same size as key for encrypting the original image. Experiments have shown that both algorithms are suitable for 2D as well as 3D images. These algorithms are implemented in MATLAB environment and tested on various medical images which have shown good results. These methods can be used for encrypting other images also.	Consequently, the traditional ciphers like IDEA,AES,DES, RSA etc. are not suitable for real time image encryption as these ciphers require a large computational time and high computing power

<u>Conclusion drawn on analyzing above papers:</u>

So we understood that it is very essential to prevent the data from unauthorized access. So from these papers we studied some of the existing technique and use of AES, DES, RSA and also some of the algorithm which is fast in nature for encryption and decryption along with some Technique. So this Technique make our system more secure to transmit our secret information over the network. Also these papers helped us to overcome issues like security, performance, privacy and Reliability in Image Encryption. This Proposed System is not just limited to particular area but also widely applied in secure storage and transmission of Confidential images over the internet or any shared network environment.

APPLICATION AREAS:

BLOWFISH

Areas of applications:

A standard encryption algorithm must be suitable for many different applications:

1.Bulk encryption: The algorithm should be efficient in encrypting data files or a continuous data stream.

2.Random bit generation: The algorithm should be efficient in producing 9 Block Cipher Blowfish single random bits.

3.Packet encryption: The algorithm should be efficient in encrypting packet- sized data. (An ATM packet has a 48- byte data field.) It should implementable in an application where successive packets may be encrypted or decrypted with different keys.

4.Hashing: The algorithm should be efficient in being converted to a one- way hash function.

Products Using Blowfish Algorithm

- Blowfish Advanced CS by Markus Hahn:
- File encryption and wipe utility for all Win32 systems. File browser, job automation, auto password confirmation, secure key setup with SHA-1, and data compression with LZSS. Uses Blowfish, Two fish, and Yarrow. Opensource.
- 2. Access Manager by Citi-Software Ltd: A password manager for Windows. Free for personal use.
- A Edit: A free Windows word processor incorporating text encryption.

CIPHER BLOCK CHAINING:

- many banking systems use AES-128 and AES-256 to secure online banking or internet banking.
- It is used in Wireless Sensor Network’s
- For robust cloud computing security

ADVANTAGES AND DISADVANTAGES

Advantages of Blowfish:

- Blowfish is one of the fastest block ciphers in general use, except when changing keys.

- Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is slow compared to other block ciphers.
- This prevents its use in certain applications, but is not a problem in others.
- In an application, it's actually a benefit in the password-hashing method uses an algorithm derived from Blowfish that makes use of the slow key schedule. Blowfish is not subject to any patents and is there- fore freely available for everyone. This has contributed a lot in cryptographic software.

Disadvantages of Blowfish :

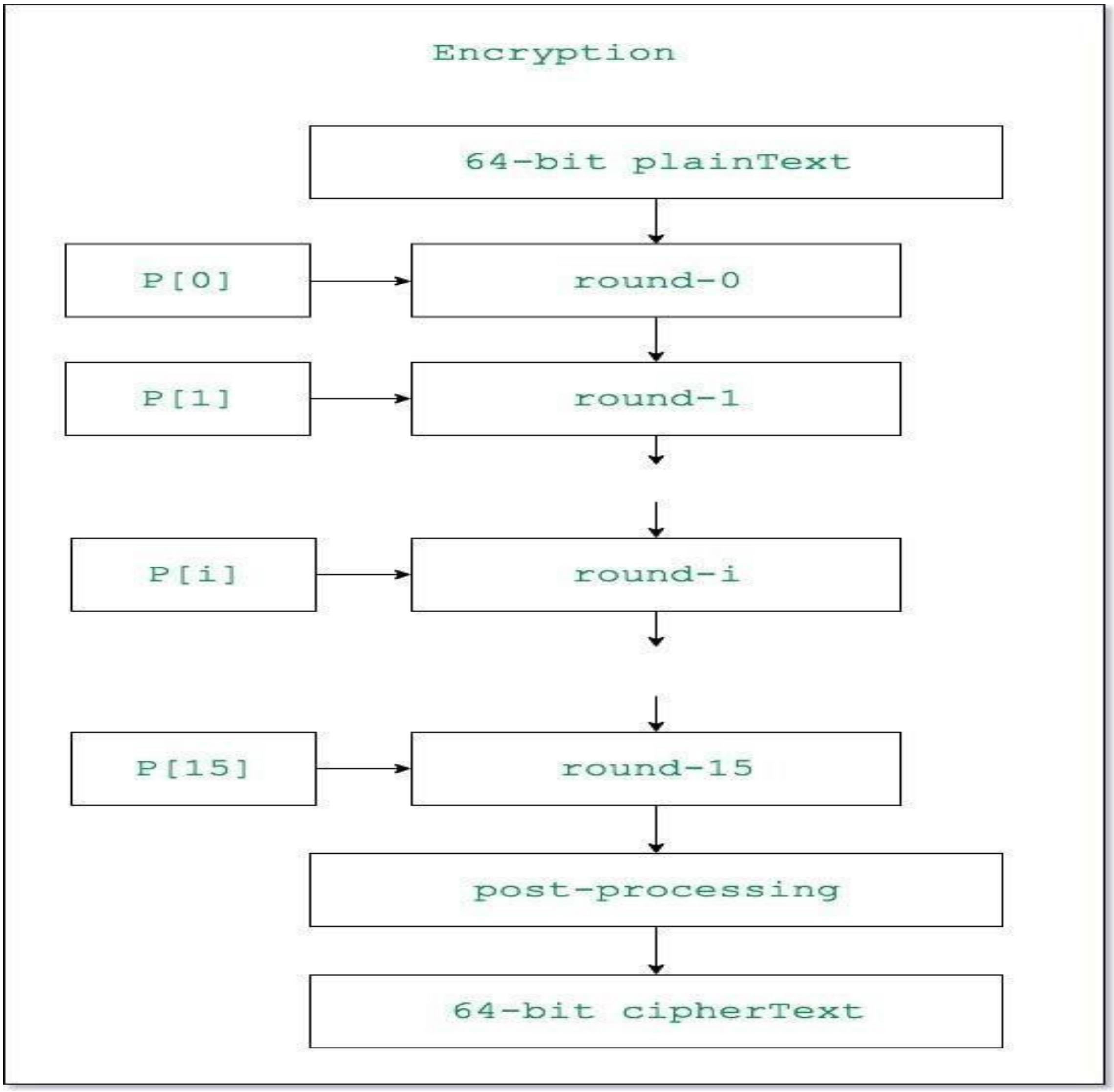
- The disadvantages of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel.
- Each pair of users needs a unique, so as number of users increase, key management becomes complicated. For example N(N-1)/2 keys re- quired. Blowfish can't provide authentication and non-repudiation as two people have same key.
- It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput.
- The disadvantages of Blowfish are it must get key to the person out of band specifically not through the unsecured transmission channel. Each pair of users needs a unique, so as number of users increase, key management becomes complicated. For example N(N-1)/2 keys re- quired.
- Blowfish can't provide authentication and non-repudiation as both have same key. It also has weakness in decryption process over other algorithms in terms of time consumption and serially in throughput.
- Blowfish is suitable for applications where the key does not change frequently like communication links or file encryptors.
- However for applications like packet switching or as one-way hash function, it is unsuitable. Blowfish is not ideal for smart cards, which requires more compact ciphers.

ADVANTAGES AND LIMITATIONS OF CBC:

- ✓ Each ciphertext block depends on all message blocks.
- ✓ Thus a change in the message affects all ciphertext blocks after the change as well as the original block .Need Initial Value (IV) known to sender & receiver how- ever if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate hence either IV must be a fixed value (as in EFTPOS) or it must be sent encrypted in ECB mode before rest of message.

- ✓ At end of message, handle possible last short block.

Architecture:



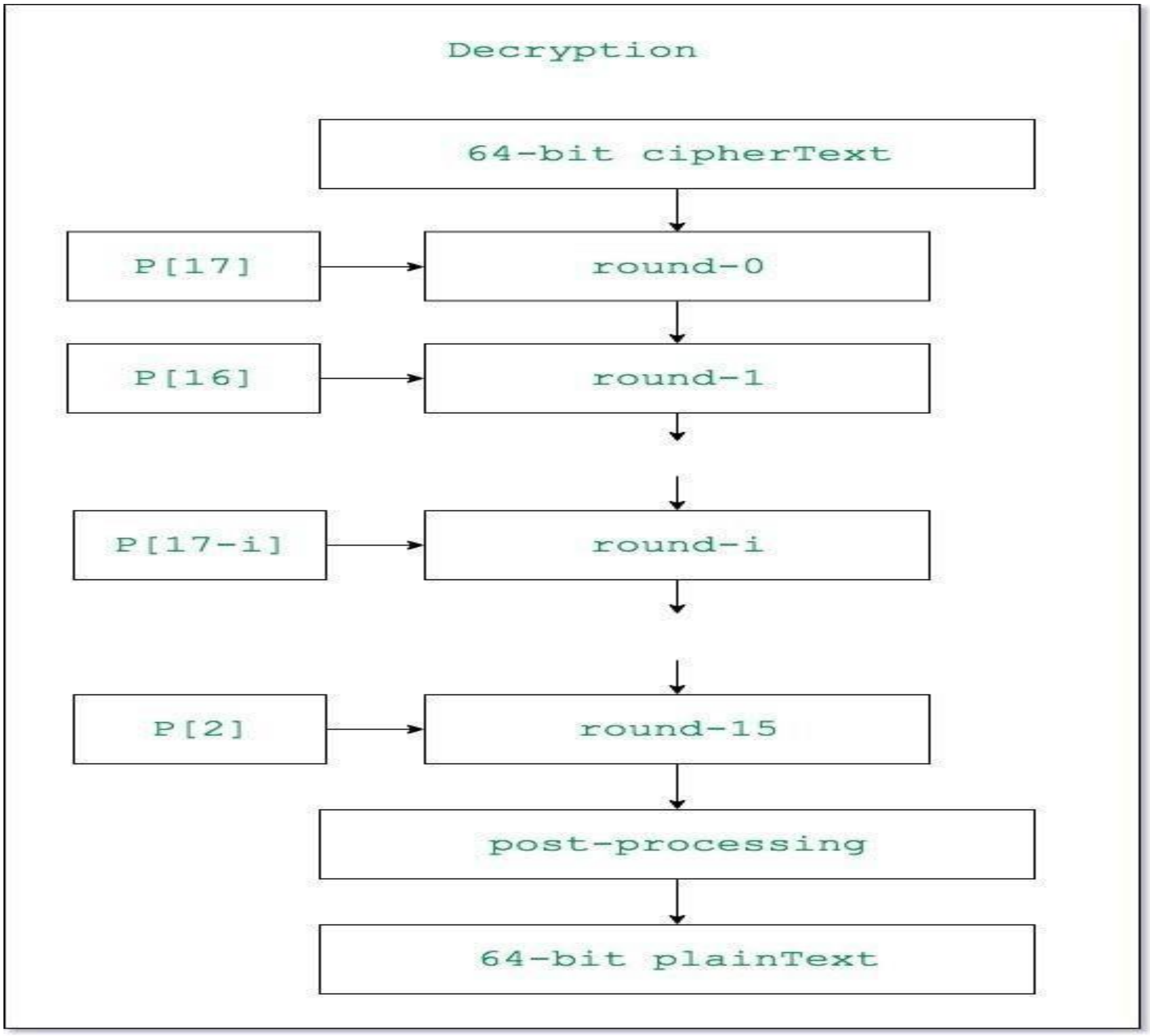


Image Encryption using AES, DES and RSA:

Code:

AES:

```
from tkinter import*

from tkinter import ttk

import tkinter as tk

from tkinter.filedialog import *

import   tkinter.messagebox

from PIL import Image,ImageTk
```

```
import hashlib
import enc_script
import os
def pass_alert():
   tkinter.messagebox.showinfo("Password Alert","Please enter a password.")
def encrypt():
    global file_path_e
    enc_pass = passg.get()
    if enc_pass == "":
        pass_alert()
    else:
        #LOAD THE IMAGE
        filename = tkinter.filedialog.askopenfilename()
        file_path_e = os.path.join(os.path.dirname(__file__))
        #GENERATE KEY & INITIALIZATION VECTOR
        hash=hashlib.sha256(enc_pass.encode())
        p = hash.digest()
        key = p
        iv = p.ljust(16)[:16]
        print("Encoding key is: ",key)
        input_file = open(filename,'rb')
        input_data = input_file.read()
        input_file.close()
        enc_script.enc_image(input_data,key,iv,file_path_e)
        tkinter.messagebox.showinfo("Encryption Alert","Encryption ended successfully. File
stored as: encrypted.enc")
def decrypt():
    global file_path_e
    enc_pass = passg.get()
    if enc_pass == "":
        pass_alert()
    else:
        filename = tkinter.filedialog.askopenfilename()
        file_path_e = os.path.dirname(filename)
        hash=hashlib.sha256(enc_pass.encode())
        p = hash.digest()
        key = p
        iv = p.ljust(16)[:16]
        input_file = open(filename,'rb')
        input_data = input_file.read()
        input_file.close()
        enc_script.dec_image(input_data,key,iv,file_path_e)
        tkinter.messagebox.showinfo("Decryption Alert","Decryption ended successfully File Stored as: output.png")
# GUI STUFF
top=tk.Tk()
top.geometry("500x150")
top.resizable(0,0)
top.title("ImageEncryption")
title="Image Encryption Using AES"
msgtitle=Message(top,text=title)
msgtitle.config(font=('helvetica',17,'bold'),width=300)
msgtitle.pack()
sp="---------------------------------------------------------------------"
```

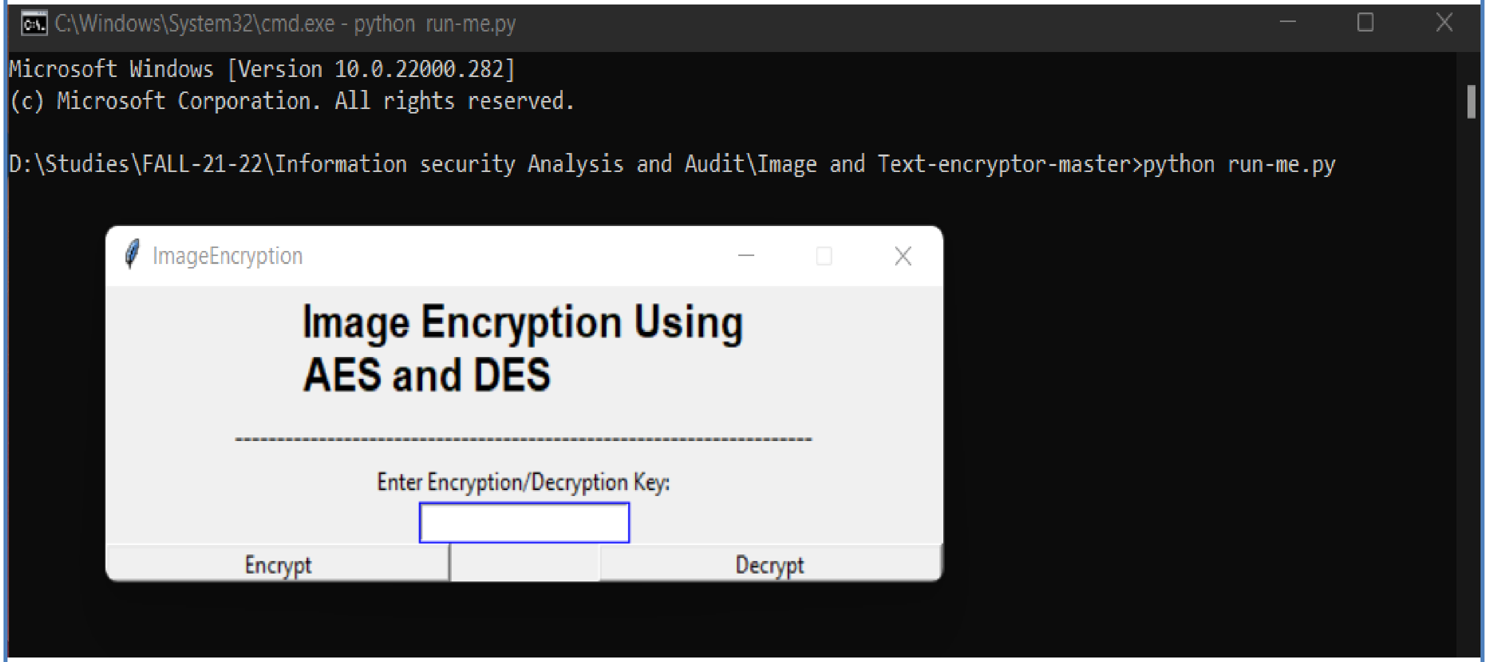
```
sp_title=Message(top,text=sp)
sp_title.config(font=('arial',12),width=650)
sp_title.pack()
passlabel = Label(top, text="Enter Encryption/Decryption Key:")
passlabel.pack()
passg = Entry(top, show="*", width=20)
passg.config(highlightthickness=1,highlightbackground="blue")
passg.pack()
encrypt=Button(top,text="Encrypt",width=28,height=3,command=encrypt)
encrypt.pack(side=LEFT)
decrypt=Button(top,text="Decrypt",width=28,height=3,command=decrypt)
decrypt.pack(side=RIGHT)
top.mainloop()
```

RSA:

```
import random
def gcd(a, b):
   if (b == 0):
       return a
   else:
       return gcd(b, a % b)
def xgcd(a, b):
   x, old_x = 0, 1
   y, old_y = 1, 0
   while (b != 0):
       quotient = a // b
       a, b = b, a - quotient * b
```

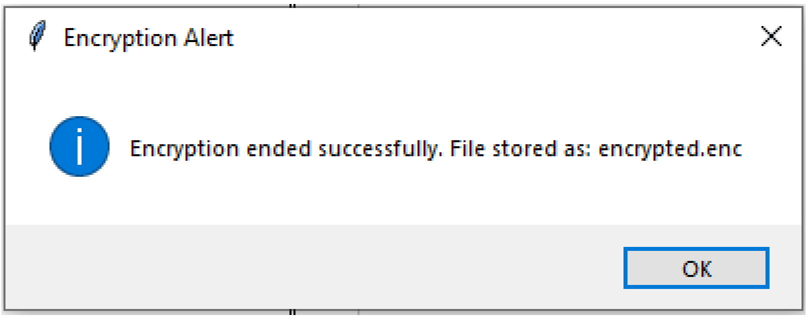
```
        old_x, x = x, old_x - quotient * x
        old_y, y = y, old_y - quotient * y
    return a, old_x, old_y
def chooseE(totient):
    while (True):
        e = random.randrange(2, totient)
        if (gcd(e, totient) == 1):
            return e
def chooseKeys():
    # choose two random numbers within the range of lines where
    # the prime numbers are not too small and not too big
    rand1 = random.randint(100, 300)
    rand2 = random.randint(100, 300)
    # store the txt file of prime numbers in a python list
    fo = open('primes-to-100k.txt', 'r')
    lines = fo.read().splitlines()
    fo.close()
    # store our prime numbers in these variables
    prime1 = int(lines[rand1])
    prime2 = int(lines[rand2])
    # compute n, totient, e
    n = prime1 * prime2
    totient = (prime1 - 1) * (prime2 - 1)
    e = chooseE(totient)
    # compute d, 1 < d < totient such that ed = 1 (mod totient)
    # e and d are inverses (mod totient)
    gcd, x, y = xgcd(e, totient)
    # make sure d is positive
    if (x < 0):
        d = x + totient
    else:
        d = x
    # write the public keys n and e to a file
    f_public = open('public_keys.txt', 'w')
    f_public.write(str(n) + '\n')
    f_public.write(str(e) + '\n')
    f_public.close()
    f_private = open('private_keys.txt', 'w')
    f_private.write(str(n) + '\n')
    f_private.write(str(d) + '\n')
    f_private.close()
def encrypt(message, file_name = 'public_keys.txt', block_size = 2):
    try:
        fo = open(file_name, 'r')
    # check for the possibility that the user tries to encrypt something
    # using a public key that is not found
    except   FileNotFoundError:
        print('That file is not found.')
    else:
        n = int(fo.readline())
        e = int(fo.readline())
        fo.close()
        encrypted_blocks = []
        ciphertext = -1
        if (len(message) > 0):
            # initialize ciphertext to the ASCII of the first character of message
            ciphertext = ord(message[0])
        for i in range(1, len(message)):
            # add ciphertext to the list if the max block size is reached
            # reset ciphertext so we can continue adding ASCII codes
            if (i % block_size == 0):
                encrypted_blocks.append(ciphertext)
                ciphertext = 0
            ciphertext = ciphertext * 1000 + ord(message[i])
        # add the last block to the list
        encrypted_blocks.append(ciphertext)
        for i in range(len(encrypted_blocks)):
            encrypted_blocks[i] = str((encrypted_blocks[i]**e) % n)
        encrypted_message = " ".join(encrypted_blocks)
        return   encrypted_message
def decrypt(blocks, block_size = 2):
    fo = open('private_keys.txt', 'r')
    n = int(fo.readline())
    d = int(fo.readline())
    fo.close()
    list_blocks = blocks.split(' ')
    int_blocks = []
    for s in list_blocks:
        int_blocks.append(int(s))
    message = ""
    for i in range(len(int_blocks)):
        int_blocks[i] = (int_blocks[i]**d) % n
        tmp = ""
        for c in range(block_size):
            tmp = chr(int_blocks[i] % 1000) + tmp
            int_blocks[i] //= 1000
        message += tmp
    return message
def main():
    # we select our primes and generate our public and private keys,
    # usually done once
    choose_again = input('Do you want to generate new public and private keys? (y or n) ')
    if (choose_again == 'y'):
        chooseKeys()
    instruction = input('Would you like to encrypt or decrypt? (Enter e or d): ')
    if (instruction == 'e'):
        message = input('What would you like to encrypt?\n')
        option = input('Do you want to encrypt using your own public key? (y or n) ')
        if (option == 'y'):
            print('Encrypting...')
            print(encrypt(message))
        else:
            file_option = input('Enter the file name that stores the public key: ')
            print('Encrypting...')
            print(encrypt(message,  file_option))
    elif (instruction == 'd'):
        message = input('What would you like to decrypt?\n')
        print('Decryption...')
        print(decrypt(message))
    else:
        print('That is not a proper instruction.')
main()
```

Output:



```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>python run-me.py
```

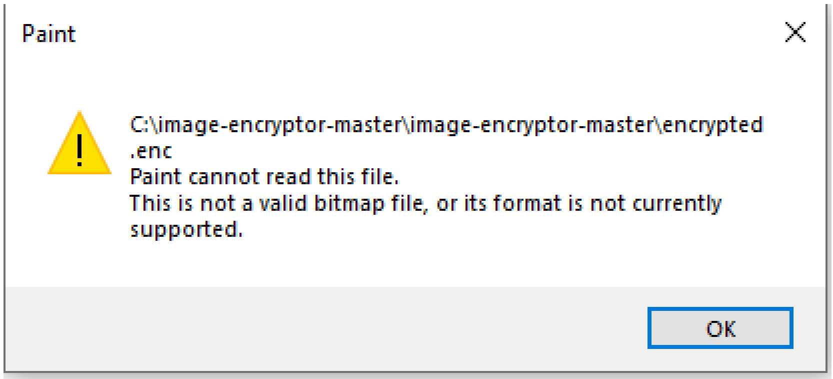
C:\Windows\System32\cmd.exe - python run-me.py
ImageEncryption
Image Encryption Using
AES and DES
Enter Encryption/Decryption Key:
Encrypt
Decrypt



Encryption ended successfully. File stored as: encrypted.enc

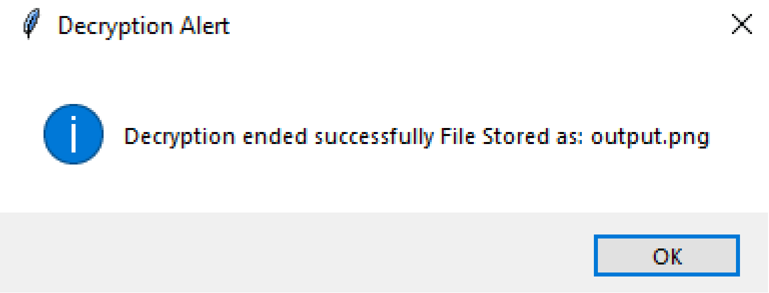
Before encryption:

After encryption



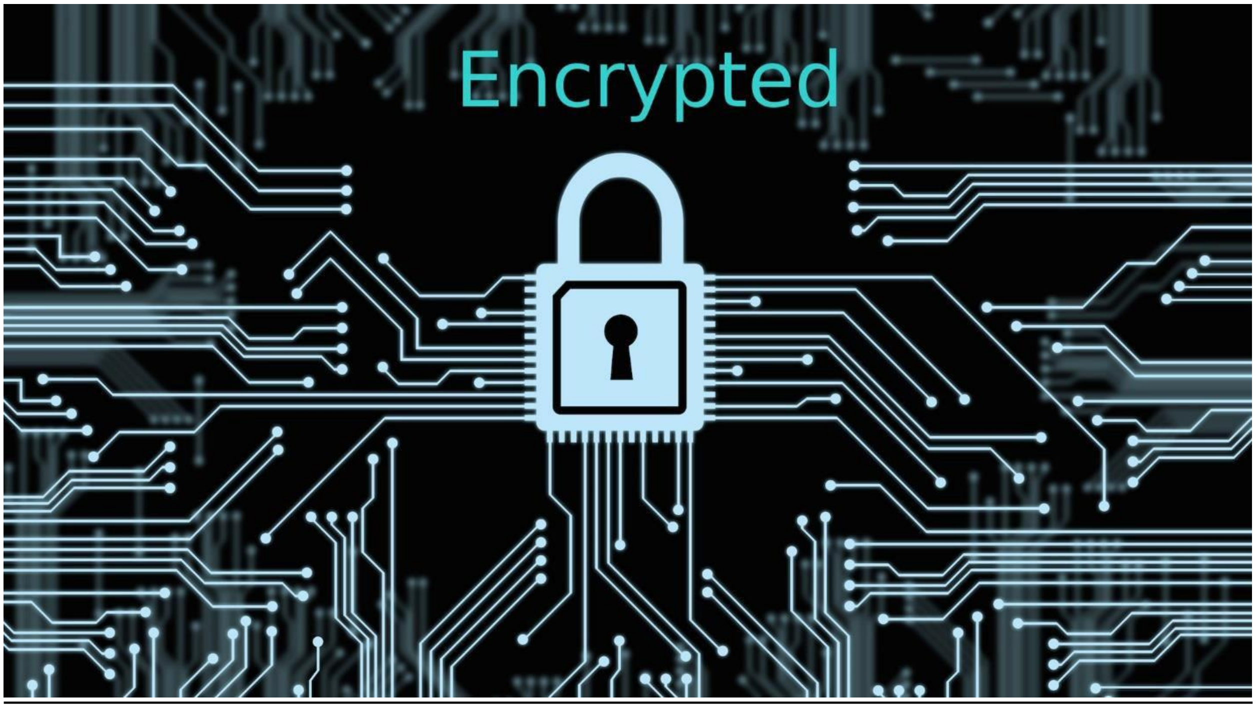
C:\image-encryptor-master\image-encryptor-master\encrypted
.enc
Paint cannot read this file.
This is not a valid bitmap file, or its format is not currently supported.

as

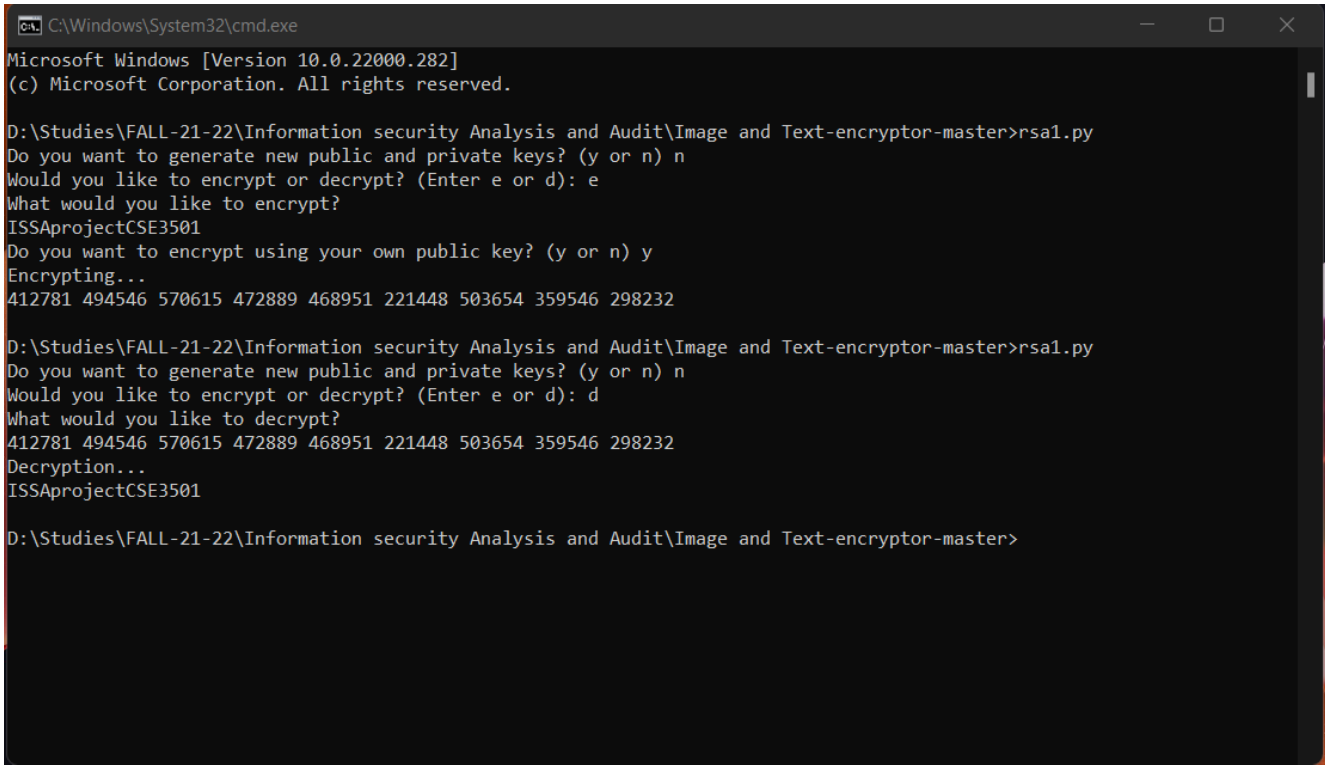


Decryption ended successfully File Stored as: output.png

After Decryption:



RSA:



```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>rsa1.py
Do you want to generate new public and private keys? (y or n) n
Would you like to encrypt or decrypt? (Enter e or d): e
What would you like to encrypt?
ISSAprojectCSE3501
Do you want to encrypt using your own public key? (y or n) y
Encrypting...
412781 494546 570615 472889 468951 221448 503654 359546 298232

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>rsa1.py
Do you want to generate new public and private keys? (y or n) n
Would you like to encrypt or decrypt? (Enter e or d): d
What would you like to decrypt?
412781 494546 570615 472889 468951 221448 503654 359546 298232
Decryption...
ISSAprojectCSE3501

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>
```

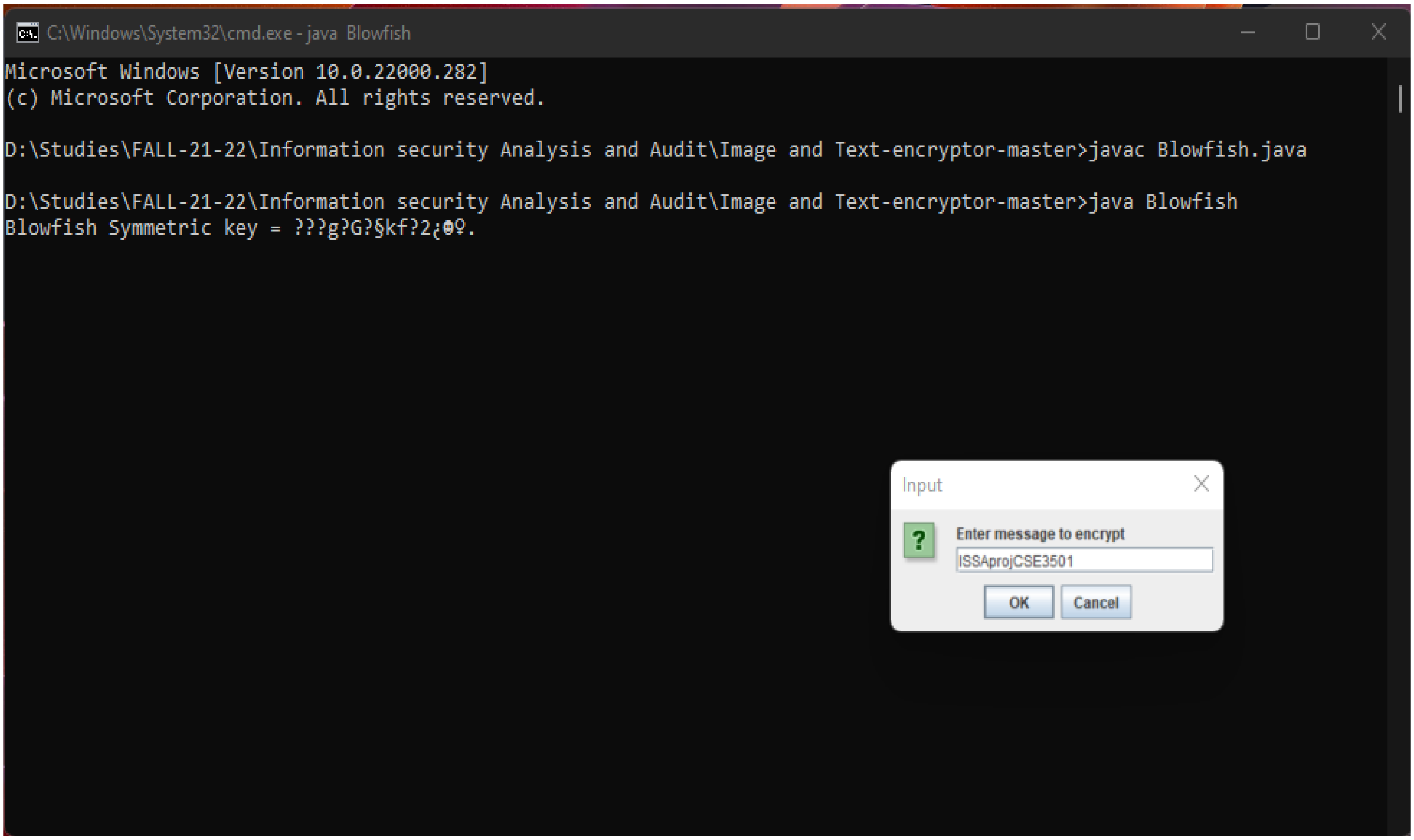
Text Encryption:

Code (BLOWFISH):

```
import javax.swing.*;

import java.security.SecureRandom;

import javax.crypto.Cipher;

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;

import javax.crypto.spec.SecretKeySpec;

import java.util.Random ;

class Blowfish {

byte[] skey = new byte[1000];

String skeyString;

static byte[] raw;

String inputMessage,encryptedData,decryptedMessage;

public Blowfish() {

try {

generateSymmetricKey();

inputMessage=JOptionPane.showInputDialog(null,"Enter message to encrypt");

byte[] ibyte = inputMessage.getBytes();

byte[] ebyte=encrypt(raw, ibyte);

String encryptedData = new String(ebyte);

System.out.println("Encrypted message "+encryptedData);

JOptionPane.showMessageDialog(null,"Encrypted Data "+"\n"+encryptedData);

byte[] dbyte= decrypt(raw,ebyte);

String decryptedMessage = new String(dbyte);
System.out.println("Decrypted message "+decryptedMessage);

JOptionPane.showMessageDialog(null,"Decrypted Data "+"\n"+decryptedMessage);}

catch(Exception e) {

System.out.println(e);}}

void generateSymmetricKey() {

try {

Random r = new Random();

int num = r.nextInt(10000);

String knum = String.valueOf(num);

byte[] knumb = knum.getBytes();

skey=getRawKey(knumb);

skeyString = new String(skey);

System.out.println("Blowfish Symmetric key = "+skeyString);}

catch(Exception e) {

System.out.println(e);}}

private static byte[] getRawKey(byte[] seed) throws Exception {

KeyGenerator kgen = KeyGenerator.getInstance("Blowfish");

SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");

sr.setSeed(seed);

kgen.init(128, sr); // 128, 256 and 448 bits may not be available

SecretKey skey = kgen.generateKey();

raw = skey.getEncoded();

return raw;}

private static byte[] encrypt(byte[] raw, byte[] clear) throws Exception {

SecretKeySpec skeySpec = new SecretKeySpec(raw, "Blowfish");

Cipher cipher = Cipher.getInstance("Blowfish");
```

```
cipher.init(Cipher.ENCRYPT_MODE,    skeySpec);

byte[] encrypted = cipher.doFinal(clear);

return encrypted;}

private static byte[] decrypt(byte[] raw, byte[] encrypted) throws Exception {

SecretKeySpec skeySpec = new SecretKeySpec(raw, "Blowfish");

Cipher cipher = Cipher.getInstance("Blowfish");

cipher.init(Cipher.DECRYPT_MODE,    skeySpec);

byte[] decrypted = cipher.doFinal(encrypted);

return decrypted;}

public static void main(String args[]) {

Blowfish bf = new Blowfish();}}
```

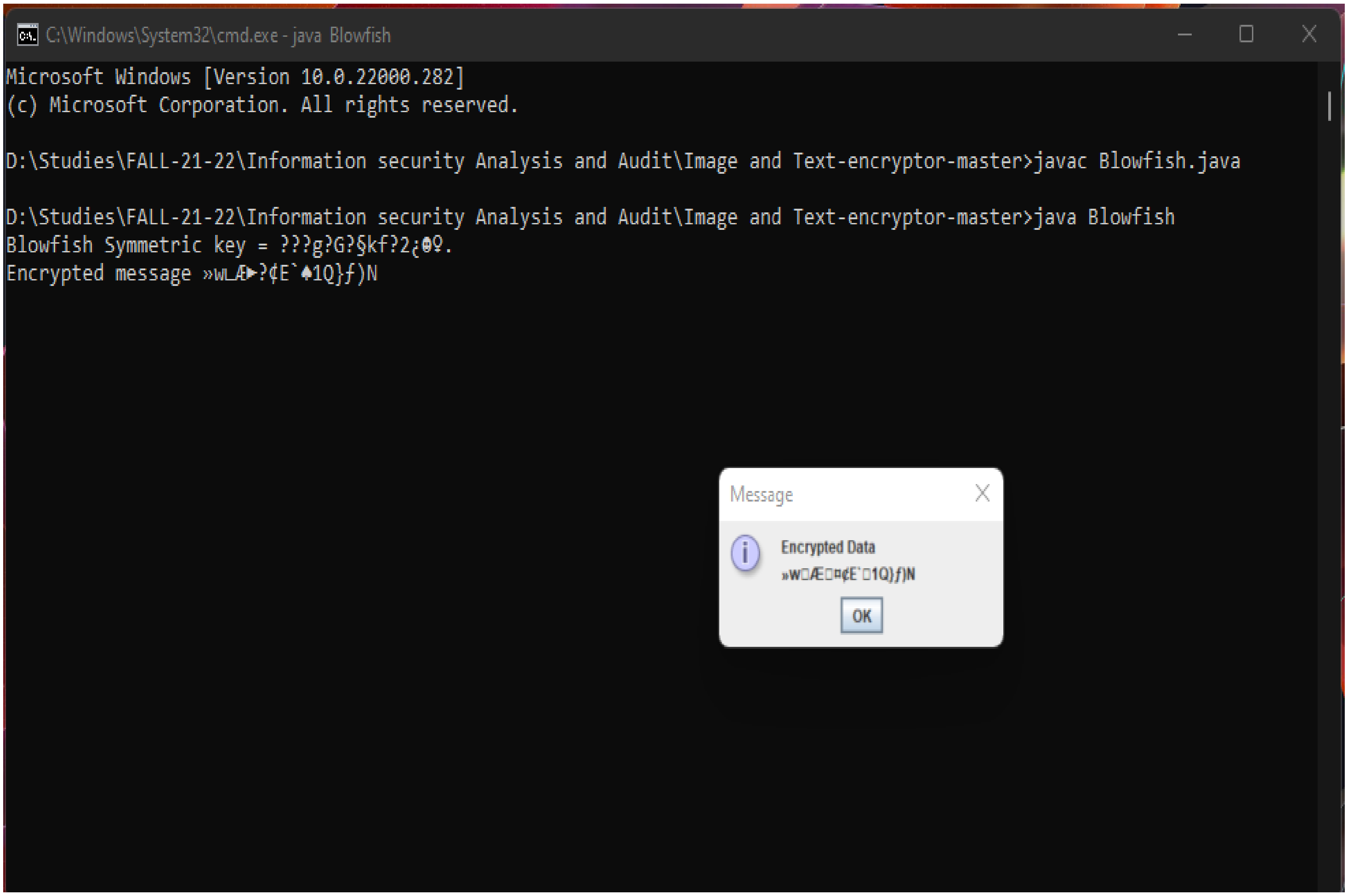
Output:



```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>javac Blowfish.java

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>java Blowfish
Blowfish Symmetric key = ???g?G?§kf?2¿☻♀.
```

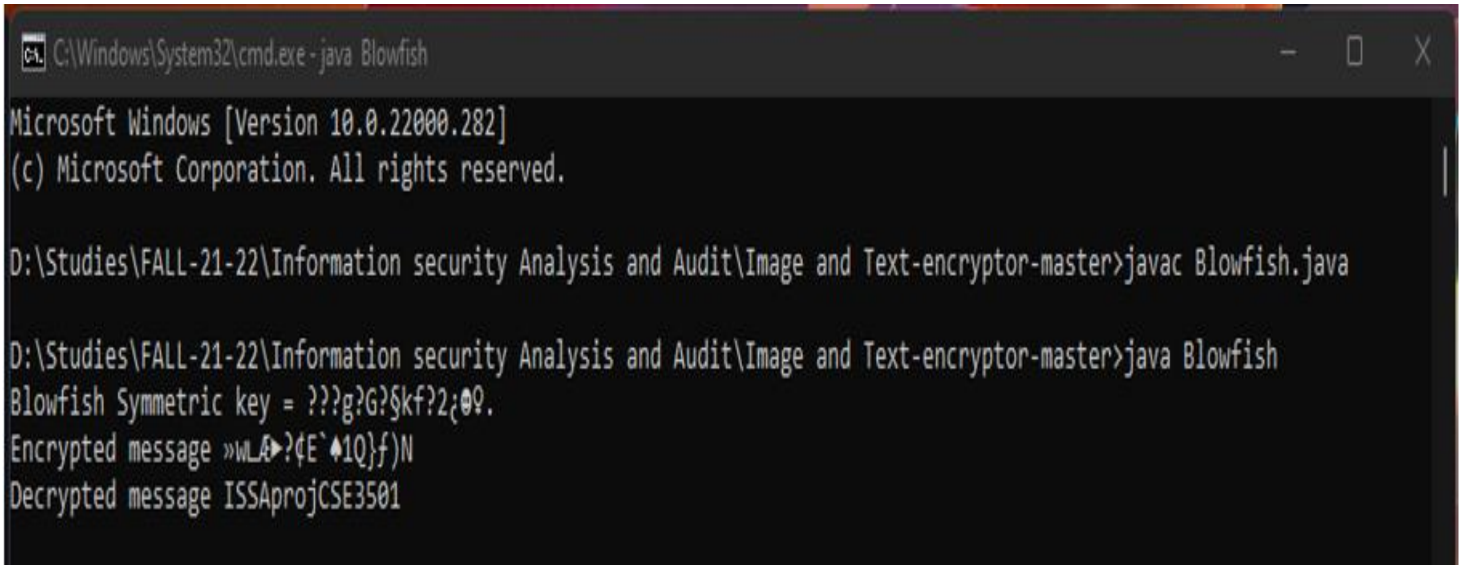
Enter message to encrypt

ISSAprojCSE3501

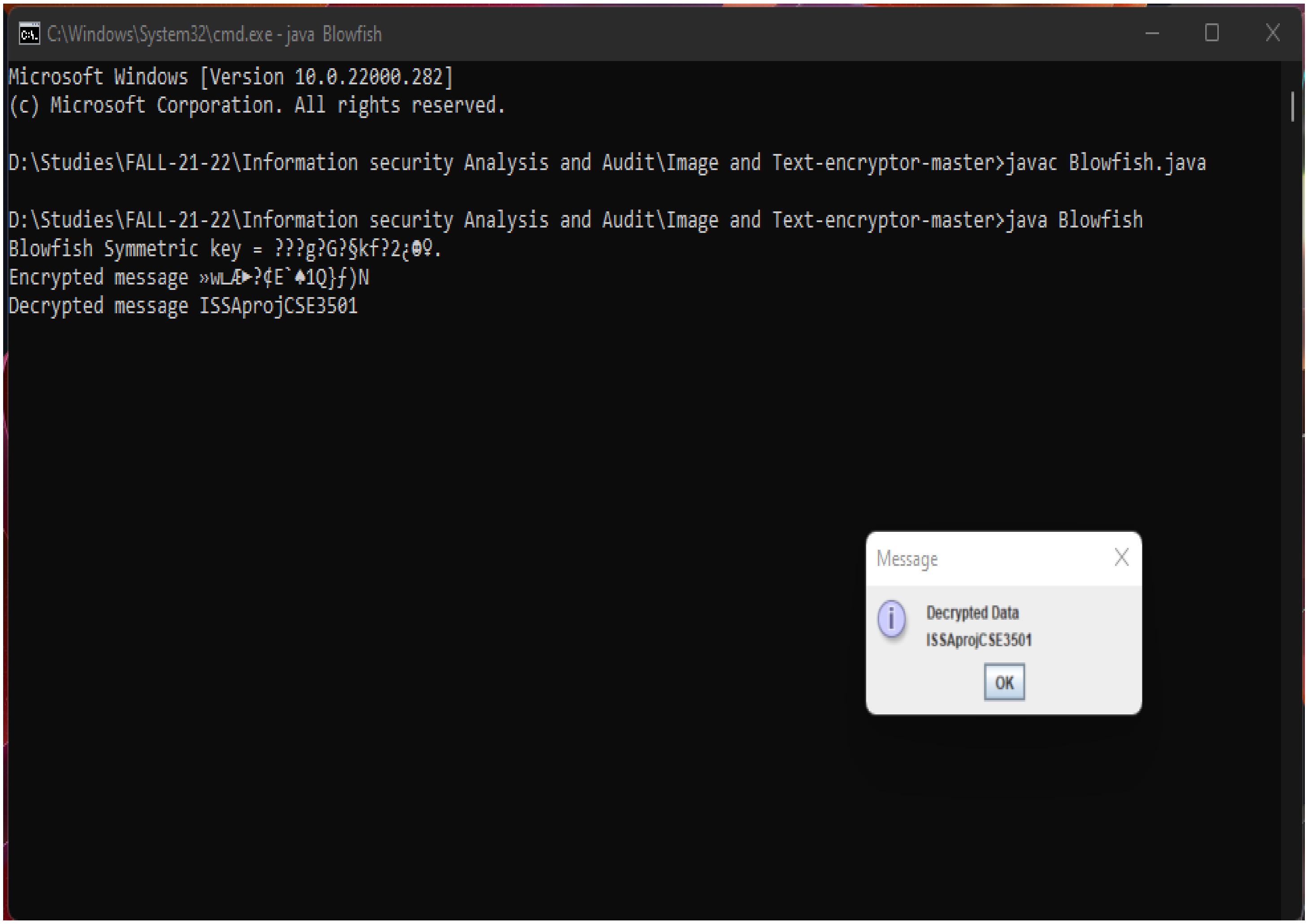


```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>javac Blowfish.java

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>java Blowfish
Blowfish Symmetric key = ???g?G?§kf?2¿☻♀.
Encrypted message »w└Æ►?¢E`♠1Q}ƒ)N
```

Encrypted Data
»w□Æ□¤¢E`□1Q}ƒ)N



```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>javac Blowfish.java

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>java Blowfish
Blowfish Symmetric key = ???g?G?§kf?2¿☻♀.
Encrypted message »w└Æ►?¢E`♠1Q}ƒ)N
Decrypted message ISSAprojCSE3501
```



```
Microsoft Windows [Version 10.0.22000.282]
(c) Microsoft Corporation. All rights reserved.

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>javac Blowfish.java

D:\Studies\FALL-21-22\Information security Analysis and Audit\Image and Text-encryptor-master>java Blowfish
Blowfish Symmetric key = ???g?G?§kf?2¿☻♀.
Encrypted message »wLÆ►?¢E`♠1Q}ƒ)N
Decrypted message ISSAprojCSE3501
```

Decrypted Data
ISSAprojCSE3501

Conclusion:

Text Encryption:

The presented results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power.

Blowfish algorithm, it is a variable-length key block cipher. Applications where there is a strong communication link and where the key will not be changed too often there we will using the Blowfish algorithm It is quicker than DES. Blowfish is a 16 pass block encryption algorithm that can be never broken.

BLOWFISH is used frequently because:

- ✓ It is fast as it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles perbyte.
- ✓ It is compact as it can run in less than 5K ofmemory.
- ✓ It simply uses addition, XOR, lookup table with 32-bitoperands.
- ✓ It is secure as the key length is variable ,it can be in the range of 32 448 bits: default 128 bits keylength.

Image Encryption:

The study of various algorithms shows that the strength of model depends upon the key management, type of cryptography, number of keys, number of bits used in a key. All the keys are based upon the mathematical properties. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially strong. AES uses permutation- substitution, which involves a series of substitution and permutation steps to create the encrypted block.

Though AES seems to be the best algorithm the only disadvantage is that it is symmetric algorithm which means same key for both encryption and decryption which gives rises to an insecure channel. Hence through this project we are providing a secure channel using RSA which is an asymmetric algorithm

References:

1) Singh, G. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Int. J. Comput. Appl. 2013, 67. [Google Scholar] [CrossRef]

2) Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004, 21, 749–761. [Google Scholar] [CrossRef]

3) Li, X.; Li, T.; Wu, J.; Xie, Z.; Shi, J. Joint image compression and encryption based on sparse Bayesian learning and bit-level 3D Arnold cat maps. PLoS ONE 2019, 14, e0224382. [Google Scholar] [CrossRef]

4) Zhou, S.; Zhang, Q.; Wei, X.; Zhou, C. A Summarization on Image Encryption. IETE Tech. Rev. 2010, 27, 503–510. [Google Scholar] [CrossRef]

5) Li, X.; Xie, Z.; Wu, J.; Li, T. Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations. Complexity 2019, 2019, 7485621. [Google Scholar] [CrossRef]

6) Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. Image Vis. Comput. 2006, 24, 926–934. [Google Scholar] [CrossRef]

7) Borujeni, S.E.; Eshghi, M. Chaotic Image Encryption Design Using Tompkins-Paige Algorithm. Math. Probl. Eng. 2009, 2009, 762652. [Google Scholar] [CrossRef]

8) Sheela, S.J.; Suresh, K.V.; Tandur, D. Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimed. Tools Appl. 2018, 77, 25223–25251. [Google Scholar] [CrossRef]

9) Li, T.; Yang, M.; Wu, J.; Jing, X. A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing. Complexity 2017, 2017, 9010251. [Google Scholar] [CrossRef]

10) Li, T.; Shi, J.; Li, X.; Wu, J.; Pan, F. Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes. Entropy 2019, 21, 319. [Google Scholar] [CrossRef]

11) Norouzi, B.; Mirzakuchaki, S. A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dyn. 2014, 78, 995–1015. [Google Scholar] [CrossRef]

12) Zhu, H.; Zhang, X.; Yu, H.; Zhao, C.; Zhu, Z. An image encryption algorithm based on compound homogeneous hyper-chaotic system. Nonlinear Dyn. 2017, 89, 61–79. [Google Scholar] [CrossRef]

13) Xue, H.W.; Du, J.; Li, S.L.; Ma, W.J. Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets. Opt. Laser Technol. 2018, 106, 506–516. [Google Scholar] [CrossRef]

14) Chai, X.; Zheng, X.; Gan, Z.; Han, D.; Chen, Y. An image encryption algorithm based on chaotic system and compressive sensing. Signal Process. 2018, 148, 124–144. [Google Scholar] [CrossRef]

15) Gong, L.; Qiu, K.; Deng, C.; Zhou, N. An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. Opt. Lasers Eng. 2019, 121, 169–180. [Google Scholar] [CrossRef]

16) Zhou, N.; Jiang, H.; Gong, L.; Xie, X. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. Opt. Lasers Eng. 2018, 110, 72–79. [Google Scholar] [CrossRef]