JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Comparative analysis using cryptographic algorithms for securing data

Ms. K. Vaishnavi, Ms. T. Ramya Sri, Ms. K. Sankeerthana
Department of Information Technology
Stanley College of Engineering and Technology for Women (Autonomous)

ABSTRACT
In the word of internet in every second huge amount of data being generated every day on the internet. Securing information from hackers and providing security is a biggest challenge. To solve this problem, we have used cryptographic algorithms. Cryptography is very useful to ensure privacy and information security for making internet a safer place. Despite the numerous cryptographic algorithms being implemented in our world today, we still encounter issues of their usage. While some are very efficient in communication across networks, others are better in the file encryption such as images, text files etc. This security concern can be solved using various ways the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So, we have introduced a new security mechanism that uses a combination of multiple cryptographic algorithms where three algorithms are combined together to make strong bond in securing the data along with that we have also compared the algorithms to check the best level of security in faster time. These three algorithms generate symmetric key and inbuilt steganography for securing the data. The three cryptographic algorithms are, AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard), CAST (Carlisle Adams and Stafford Tavares) algorithms. The result of three algorithms provides strongest security with less time of encryption and decryption. All the algorithms use 128-bit keys. Comparing all the three algorithms for best performance and high-quality result.

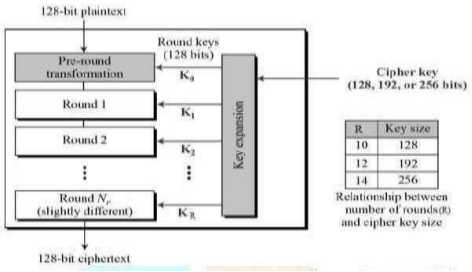
KEYWORDS:Cryptography, AES, 3DES, CAST, LSB Steganography

INTRODUCTION:
In the world of internet in every second huge amount of data is been generated everyday on the internet and stored in the cloud. Securing information has become vital to enhance this cryptograph come in play which helps us to secure our data from unauthorized users. Cryptography is a technique to secure data on the network from unauthorized users.
One essential aspect for secure communication is cryptography. Cryptography termed as an art of concealing information so that only the authenticated parties can have access to the private information. One of Cryptographic techniques is to changes the message data into a scrambled code that can be retrieved by only authorized users. The cryptography technique secures the sensitive information in unsecured transmission networks and which can be read by the intended recipient.
In the Cryptography, basic elements are plain text to cipher text. Plain text in the original data which the sender wants to send and Cipher text is the encrypted format of the plain text. The plain text is converted to the Cipher text using encryption algorithms and cipher text is converted back to plain text using decryption algorithm.
Similarly, steganography is to conceal and deceive. Steganography techniques to improve the security of the information. The Advanced Encryption Standard (AES), triple data Encryption standard (3DES), Carlisle Adams and Stafford Tavares (CAST) algorithms has been combine and used to encrypt the secret message. Then, the encrypted message has been hidden using steganography. In image steganography a message is embedded into an image by altering the values of some pixels, time computation and security.
There are various cryptographic algorithms that are used to make best security for over data since there is no one algorithm which can provide high performance at once. To solve this problem, we have combined all 3 algorithms together to strength the performance of each algorithm which provide valuable insights like time computation, cost efficiency, high quality.
In this, we implement and analyze the three cryptographic algorithms i.e.Advanced Encryption Standard(AES), Triple Data Encryption Standard(3DES), Carlisle Adams and Stafford Tavares (CAST) algorithms.

Advanced Encryption Standard AES:
The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continue serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations).
All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing. AES algorithm is of three types namely

AES-128bit, AES- 192bit, and AES-256bit. Each iteration encrypts and decrypts data in blocks using keys of either 128-bits or 192-bits or 256- bits, respectively. Rijndael method was enhanced to accept extra block sizes and also extra key lengths, but for AES, those functions were not inherited.

Fig.3.4.AES Algorithm



Triple Data Encryption Standard 3DES:

In cryptography, 3DES is an inherited enhanced version of DES (Data Encryption Standard). In theTriple DES algorithm, DES is a used trice to increase the security level. Triple DES is also referredto as TDES or Triple Data Encryption Algorithm (TDEA).

TDES has following key :-

- All keys being different
- Key 1 and key 2 being different & key 1 and key 3 is the same.
- All keys being identical.

TDES is slowly invisible from use, it is maximally replaced by the AES (Advanced Encryption Standard). A far-reaching anomaly is in the digital payments industry, which still uses 2TDES andscatters standards on that basis (e.g. EMV, the standard for interoperation of "Chip cards", and ICcapable POS terminals and ATM's). This guarantees that TDES will remain as an agile cryptographic standard in the future.

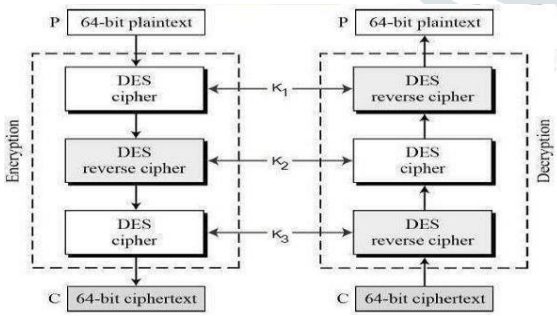


Fig.3.5.3DES Algorithm

CAST (Carlisle Adams and Stafford Tavares):

The CAST encryption algorithm belongs to a class of private key block ciphers which are composedof substitution boxes (S-boxes) with fewer input bits than output bits. Recently,a software implementation of the CAST cipher has been developed for application in computer security products. It is suggested that, with an appropriate number of substitution rounds, the CAST cipheris resistant to differential crypt analysis. In this paper, we show that the CAST cipher, with an appropriate number of rounds, is resistant to linear cryptanalysis. Similarly, to the Data Encryption Standard and other proposed block ciphers, the CAST algorithm consists of a series of rounds of substitutions in order to achieve the "confusion" and "diffusion" principles suggested by Shannon. The algorithm encrypts by dividing the -bit plaintext input blockin half. The right half-block,is transformed by a round function and then XORed bit-by-bit to the left half-block, . The right and left halves are then swapped. This is repeated for the number of roundsin the cipher.

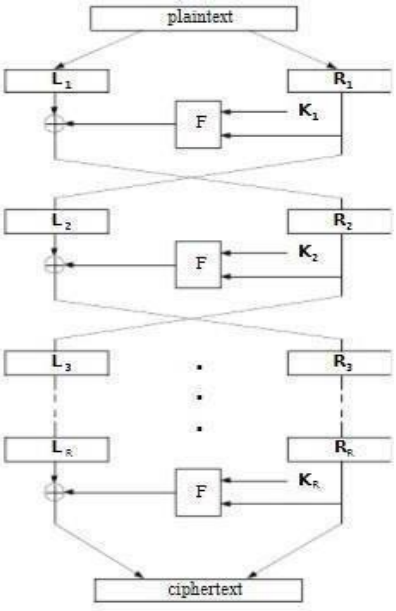


Fig.3.6 CAST

LSB STEGANOGRAPHY:

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hidethe data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data.

The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In thismethod the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques thathide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to avariety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

METHODOLOGY:

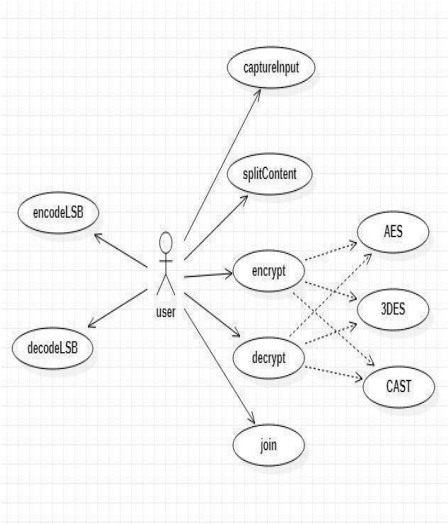


Fig 3.1 Use case Diagram

Encryption of data is a process of protecting the information through encoding. Algorithms scramble the data and are decrypted through an authentication key provided by the originator of the message or file.Data security and integrity depend on the algorithm used for encryption. As the encrypted data needs a key for access, it remains secure and confidential. Algorithms are also popularly known as ciphers and are not new.From the first world war to the cold war and modern encryption technology, ciphers have evolved.While an algorithm encrypts the data, a decryptor does the opposite. It unlocks the data and makes the information accessible. However, a decryption process is worthless without the key.Decryption keys are of different lengths, like 128 bits or 256 bits for private keys, and the longest being 2048 bits for the public keys.

Algo	Time computing		Security	Flex
	Encr	Decr		
AES	0.0010	0.0010	High	Yes
3DES	0.0040	0.0035	Medium	Yes
CAST	0.0009	0	High	Yes

Hybrid Cryptosystem Phases-

The hybrid cryptosystem used to maintain security of the files has two phases:

1. Encryption Phase
2. Decryption Phase

Encryption Phase:

1) Divides the file into N parts.
2) Encrypting all the parts of the file using the selected algorithms(AES, 3DES, and CAST.)
3) The keys for cryptography algorithms is then secured using a different algorithm(LSB Steganography). and the key for this algorithm is provided to the user as public key.

After the above 3 steps you will have a N files which are in encrypted form and a key which is downloaded as public key for decrypting the file and downloading it. To restore the file:

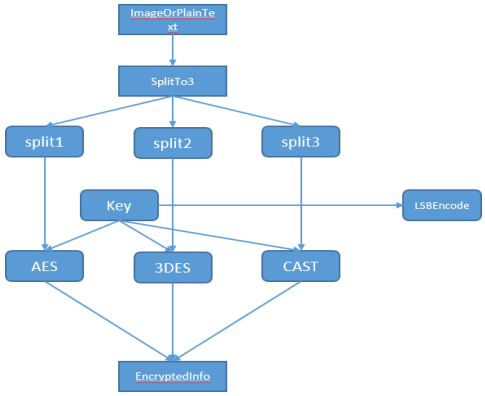


Fig.3.2 Hybrid Encryption

Decryption Phase:

1) Decrypt the keys of the algorithms.
2) Decrypt all the N parts of the file using the same algorithms which were used to encrypt them.
3) Combines all the N parts to form the original file and provide it to the user for downloading

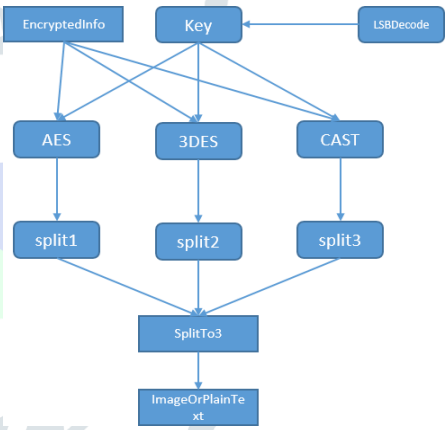


Fig 3.3 Hybrid Decryption

RESULT:

On the basis of result

Table: Result analysis

CONCLUSION:

The main aim of this system is to encrypt and decrypt data using cryptographic algorithms AES, 3DES andCAST and study and compare the Three algorithms based on their performance. Data encryption and decryption is done using cryptography and steganography techniques.

Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality for data security. In the future we can add public key cryptography for more security to avoid any attacks during the transmission of the data from the client to the server.

And we observed that the main difference between AES and 3DES is that AES is much faster than3DES, and it is also

more secure than 3DES. The encryption key lengths of AES are 128, 192, and256 bits, but the encryption key length of 3DES is still limited to 56 bits. where as**,** CAST uses a 40-bit to 128-bit key, and it's very fast and efficient than AES and 3DES.

REFERENCES:

[1] Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing Mr.Pradeep Semwal1 and Dr. MK Sharma2 https://researchtrend.net/ijet/pdf/164-F-754a.pdf

[2] Comparative Analysis on Different parameters of Encryption Algorithms for Information Security MdAsif Mushtaque1 https://www.ijcseonline.org/pub_paper/IJCSE-00187.pdf

[3]Comparative Analysis of Cryptographic Algorithms in Securing DataTaylor, Onate E.Emmah, Victor T. https://www.researchgate.net/publication/333755102_Comparative_Analysis_of_Cryptographic_Algorithms_in_Securing_Data

[4]Sunita Sharma,Amit Chugh:'Suvey Paper on Cloud Storage Security' Sunita Sharma1 , Amit Chugh2 ,Ajay Kumar3. ENHANCING DATA SECURITY IN CLOUD STORAGE. (2013).

[5] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.