A Review of Cryptography Techniques and Implementation of AES for Images

Mamta. Juneja, and Parvinder S. Sandhu

***Abstract*—**In this era of electronic communication, security of transmitted data is most important issue. Cryptography is widely used technique for hiding data in images for secured information transfer across intranets and internet. This paper presents a review of various cryptography techniques for images like Data Encryption Standard (DES), Triple DES (3DES), RC4, Blowfish and Advanced Encryption Standard (AES).Comparison analysis of these techniques is provided on various factors like key size, block size and number of rounds required for its implementation. AES outperforms the rest of techniques for performing encryption on text or other image files. An implementation of AES algorithm for encrypting and decrypting message, text files and images is provided in detail.

***Keywords*—**AES, Blowfish, Cryptography, DES, 3 DES, Decryption, Encryption, RC4.

I. Introduction

A. Cryptography

CRYPTOGRAPHY is the art of secret writing to generate encoded text called cipher text. In this, Encryption is applied to given text at sender side to change it to cipher text which is decoded to original text using Decryption at receiver end. Steganography and Cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Kerckhoffs law for cryptography states that the quality of a cryptographic system should only depend on a small part of information, namely the secret key i.e. knowledge of the system that is used, should not give any information about the existence of hidden messages. Finding a message should only be possible with knowledge of the key that is required to uncover it. Cryptography is the Science of information security which is derived from the Greek kryptos, meaning hidden [2]. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. It scrambles plaintext (ordinary text) into cipher text called encryption and then from cipher text to plain text is known as decryption. The various objectives of cryptography are as follows:

1) Confidentiality: The information cannot be understood by anyone except for whom it was unintended.

Mamta.Juneja is Assistant Professor in University Institute of Engineering and technology, Panjab Univesity, Chandigarh. E-mail: er_mamta@yahoo. com).

Prof. Dr. Parvinder S. Sandhu is with Rayat and Bahra Institute of Engineering and Bio-Technology, Punjab, India.

2) Integrity: The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3) Non-repudiation: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4) Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information.

Cryptography algorithms play an important role in information security. They can be divided into Symmetric and Asymmetric key cryptography. In Symmetric key encryption only one key is used to encrypt and decrypt data. The key should be distributed before transmission between two parties. Key plays an important role in encryption and decryption. If a weak key is used in the algorithm then easily data can be decrypted. The size of the key determines the strength of Symmetric key encryption.

Symmetric algorithms are of two types [3]: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. Encryption algorithms consume significant amount of computing resources such as battery power, CPU time, etc. Asymmetric key (or public key) encryption is used to solve the problem of key distribution. In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g. Digital Signatures). Public key is known to the public and private key is known only to the user. Prior to transmission there is no need for distributing them. Asymmetric encryption techniques are near to 1000 times slower than Symmetric techniques, since they require more computational processing power.

B. Cryptography Techniques

The various cryptography techniques are as follows [4]:

a) **DES (Data Encryption Standard)**: DES as defined in [5] is a block encryption algorithm. It was the first encryption standard published by NIST (National Institute of Standards and Technology). It is a symmetric algorithm, means same key is used for encryption and decryption. It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation; 8 bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six

different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text. Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher key.

b) **3DES (Triple DES):** 3DES is an enhancement of Data Encryption Standard. It uses 64 bit block size with 192 bits of key size. The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. 3DES is slower than other block cipher methods.

c) **AES (Advanced Encryption Standard):** AES as defined in [6], also known as the Rijndael's algorithm, is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices. AES has been tested for many security applications.

d) **Blowfish:** It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider [7-8] as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish is a very secure cipher but it is has been replaced by Two fish and Rijndael's due to its small 64 bit block size Blowfish is one of the fastest block ciphers which has developed to date. Slowness kept Blowfish from being used in some applications. Blowfish was created to allow anyone to use encryption free of patents and copyrights. Blowfish has remained in the public domain to this day. No attack is known to be successful against it, though it suffers from weak keys problem.

e) **RC4** is a stream cipher, symmetric key algorithm [9]. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text.

C. Comparison Analysis [4]

The comparison of all above cryptography techniques is given in Table 1.

TABLE I
COMPARISON OF VARIOUS CRYPTOGRAPHY TECHNIQUES

Algorithm	Key Size	Block Size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 Bits	10,12, 14
Blowfish	32-448 bits(128 bits by default)	64 bits	16
RC4	1-2048 bits	Stream cipher	-

DES is the old data encryption standard from the seventies. Its key size is too short for proper security (56 effective bits; this can be brute-forced, as has been demonstrated more than ten years ago). Also, DES uses 64-bit blocks, which raises some potential issues when encrypting several gigabytes of data with the same key (a gigabyte is not that big nowadays).
3DES is a trick to reuse DES implementations, by cascading three instances of DES (with distinct keys). 3DES is believed to be quite efficient but it is slow, especially in software (DES was designed for efficient hardware implementation, but it sucks in software; and 3DES sucks three times as much).
Blowfish is a block cipher, deployed in some software's, can use huge keys and is believed secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. Blowfish is efficient in software, at least on some software platforms.

AES is the successor of DES as standard symmetric encryption algorithm for which accepts keys of 128, 192 or 256 bits, uses 128-bit blocks (so no issue there), and is efficient in both software and hardware. It was selected through an open competition involving hundreds of cryptographers during several years. Some cryptanalysts have also suggested that AES performance is up to 40% faster in hardware and software than 3DES, although it's open to debate and interpretation. The known attacks against AES to date have involved timing, where keys are guessed by analyzing how long particular steps require. Because, AES has a well-defined algebraic structure, some cryptographers worry that there might be attacks on the algorithm itself possible, but none have publicly emerged to date. AES is efficient, elegant, and secure. It will be a top choice for data security in the next decade and beyond [10]. So this work is focused on implementing encryption using AES.

D. Advanced Encryption Standard (AES)

It was invented by Joan Daemen and Vincent Rijmen, and accepted by the US federal government in 2001 for top secret approved encryption algorithms. It is also referred to as Rijndael's algorithm as is based on the Rijndael's algorithm. Reportedly, this standard has never been cracked.

As explained in [6], AES is a block cipher. This means that it operates on fixed-length chunks of data (for example, blocks), applying the same transformation to each block. The transformation is controlled by use of the encryption key. Block ciphers (and thus AES) use symmetric keys, which

mean that the same key used to encrypt data is also used to decrypt it (or in some cases, a key only trivially different). In operation, a user inputs 128 bytes of plaintext, along with a key, and receives as output 128 bytes of cipher text. To decrypt the cipher text, the user inputs it and the key to the algorithm to retrieve the original 128 bytes of plaintext. Encryption proceeds via a number of rounds. For 128-bit keys, AES prescribes ten rounds; for 192-bit keys, it uses 12 rounds; and for 256-bit keys, it uses 14 rounds.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. In contrast, the parent Rijndael's algorithm can have both key and block sizes of 128, 160, 192, 224, or 256 bits. The 128 bits in a block are arranged in a grid of 4 x 4 bytes (also known as the state). Each round of encryption consists of four steps to generate a new state:

1. AddRoundKey
2. SubBytes
3. ShiftRows
4. MixColumns

In the final round of encryption, the MixColumns step is replaced with another AddRoundKey step.

II. ENCRYPTING IMAGES USING AES

A. Working of AES:

Input text file is encrypted using standard encryption technique AES as defined in to provide two tier security to proposed system. It ensures that message would not be understood by any even in that case its existence is disclosed due to being encrypted.

Algorithm:

Step 1 (AddRoundKey): A sub key is combined with the state. The sub key is derived from the main key using a key schedule, which generates an endless supply of sub key using a well-defined set of rotations, exponents, and multiplications. The sub key is the same size as the state, and the two are combined using the logical exclusive OR operation (XOR). This state obscures the original state and provides a new encrypted state.

Step 2 (SubBytes): Each byte in the state is substituted using an S-Box. The S-Box or Substitution Box is another transformation, this time achieved by finding the multiplicative inverse of the byte in Rijndael's finite field, then transforming that result using binary linear algebra (an affine transform). Choosing good S-Box transforms is critical to the security of an encryption algorithm. Again, the result of this step is to obscure the original state and provide a new, encrypted state.

Step 3 (ShiftRows): The bytes in the rows of the 4 x 4 state are shifted within the row. The first row is left unchanged, the second row is shifted left one byte, and the third and fourth rows are shifted left two and three bytes, respectively.

Step 4 (MixColumns): The four bytes of each column are combined using an invertible linear transform. Four input bytes generate four output bytes, with each input byte influencing each output byte. You can view this as a matrix multiply within a finite field. An equivalent view is that it is a modulo multiply of a pair of polynomials. This operation provides diffusion, meaning that it spreads the input of a single character of plaintext across several characters. Repetition of the ShiftRows and MixColumns steps ensures that changing a single letter of the plaintext changes every character in the output block of cipher text.

Inner Workings of a Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

Substitute bytes
Shift rows
Mix Columns
Add Round Key

The tenth round simply leaves out the Mix Columns stage.

The first nine rounds of the decryption algorithm consist of the following:

Inverse Shift rows
Inverse Substitute bytes
Inverse Add Round Key
Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage as shown in Figure 1.

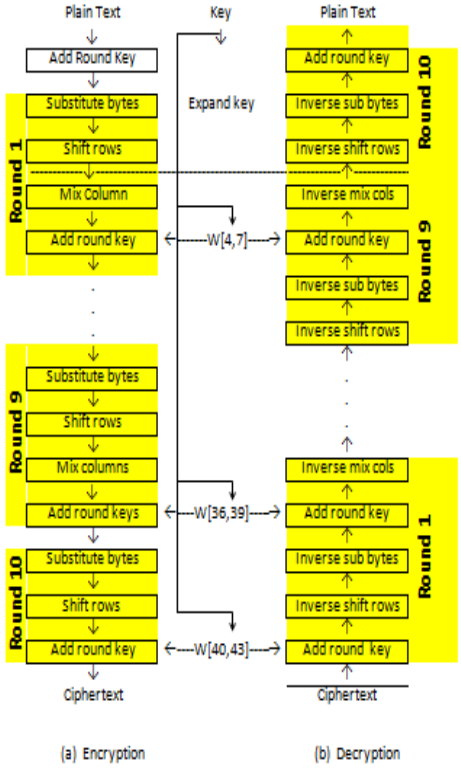


Fig. 1 Working of AES

B. Procedure for Encryption and Decryption Using AES

Encryption and Decryption is performed using AES as explained above.

Encryption using AES:

For each Round (except final round) with State and Key as Input, Repeat the following steps:

Substitute_State_Bytes ()
Shift_State_Rows ()
Mix_State_Columns ()
Add_Round_key ()
For Final Round, Repeat the following steps:
Substitute_State_Bytes ()
Shift_Satte_Rows ()
Add_Round_key ()

Step 1: Substitute_State_Bytes (State)

Each byte of the block is replaced with its substituent in the S Box.

Each byte is taken independent.

Single S Box is used for all of the states as shown in Figure 2.

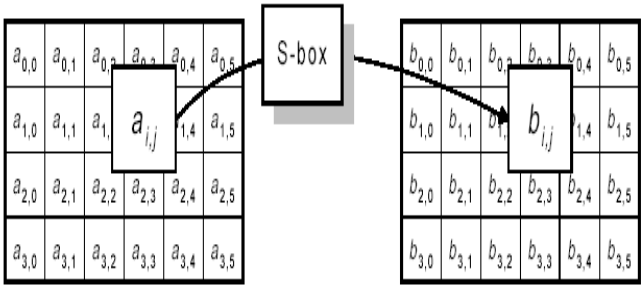
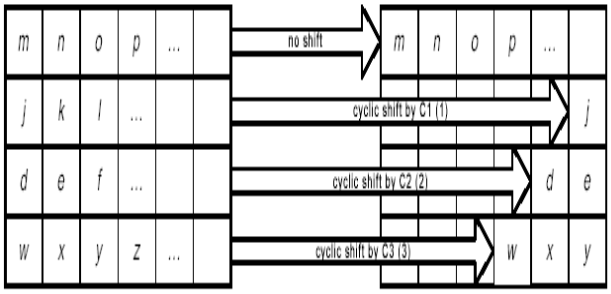


Fig. 2 Substitute Bytes

Step 2: Shift_State_Rows (State)

E ach row of the state is moved certain number of steps in cycle manner.

Number of shifts a row undergoes is kept different for different rows as shown in Figure 3.



-

Fig. 3 Shift Rows

Step 3: Mix_State_Columns (State)

State columns are considered as polynomials over Galois Field (2^8).

Each and every state column is modulo multiply of a pair of polynomials.

Step 4: Add_Round_Key (State, Key[i])

XOR round key with state as shown in Figure 4.

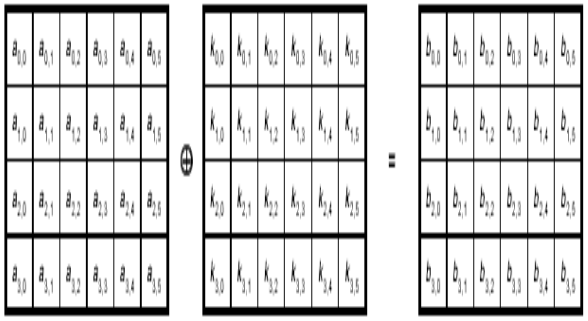


Fig. .4 Add Round Key

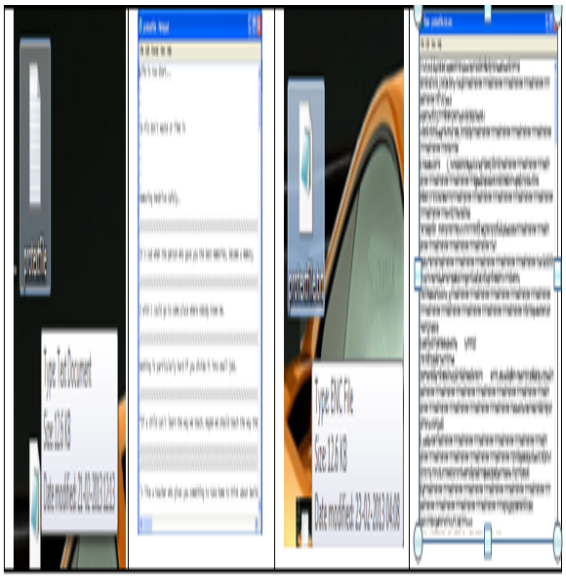
Decryption using AES

For each Round (except final round) with State and Key as Input, Repeat the following steps:

Inverse_ Substitute_State_Bytes ()
Inverse_Shift_State_Rows ()
Inverse_Mix_State_Columns ()
Inverse_Add_Round_key ()
For Final Round, Repeat the following steps:
Inverse_ Substitute_State_Bytes ()
Inverse_Shift_State_Rows ()
Inverse_Add_Round_key ()

All above steps of decryption are same as during encryption except work in reverse.

The above mentioned technique was applied on various test images for carrying enryption.Encrypted files were then transmitted across internet so that could not be understood by any intuder.These files were then successfully decrypted at receiver end for retrieveing the required information.The result of application this AES algorithm is shown below in Figure 5.



(a) (b) (c) (d)

Fig. 5 (a,b) Text File and (c,d) Encrypted File

III. CONCLUSION

This paper provides the review of various cryptography techniques like DES, RC4, Blowfish and AES for images. Comparison analysis of these techniques proves AES to be better than other existing techniques. So, this work is focused on implementation of AES for encrypting text files, image files and messages. AES has been successful to encrypt given text file and transmit it across internet which was further decrypted at receiver end without been cracked by any intruder. The AES technique has been successfully tested for all types of image or text files for transferring information across networks in secured manner and results are satisfactory.

REFERENCES

[1] Kahn, D. (1983). Kahn on Codes: Secrets of the New Cryptology. New York: Macmillan.
[2] Man, Y. R., (2003), "Internet Security: Cryptographic Principles, Algorithms and Protocols", John Wiley and Sons Ltd, England, Copyright.
[3] Stallings, W., (2004) "Network Security Essentials (Applications and Standards)", Pearson Education.
[4] Kessler, G.C., (January 25, 2013), "An Overview of Cryptography", Auerbach.
[5] DES Encryption Standard, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springer Field, VA, April 1977.
[6] Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 2001.
[7] Ferguson, N., and Schneier, B., (2003), "Practical Cryptography", John Wiley
[8] Ferguson, N., Schneier, B., and Kohno, T., (2010), "Cryptography Engineering: Design Principles and Practical Applications", New York: John Wiley and Sons.
[9] Dawson, E., and Gustafson, (2002), "Evaluation of RC4 Stream Cipher", Information Security Research Center.
[10] Young, A., and Yung, M., (2004), "Malicious Cryptography: Exposing Crypto virology", New York: John Wiley and Sons.

Ms. Mamta Juneja is an Assistant Professor in University Institute of Engineering and Technology, Panjab University, Chandigarh, India.. She did masters in Computer Science from Punjab Technical University, India and currently pursuing Doctorate in the same. Her interest areas include Image Processing, Steganography, Information Hiding and Information Security.
Email:er_mamta@yahoo.com

Prof. Dr. Parvinder S. Sandhu is Doctorate in Computer Science and Engineering and working as Professor in Computer Science & Engineering department at Rayat & Bahra Institute of Engineering and Bio-Technology, Mohali, Punjab, INDIA. He is editorial committee member of various International Journals and conferences. He has published more than 150 research papers in various referred International journals and conferences. He chaired more than 100 renowned International Conferences and also acted as keynote speaker in different countries. His current research interests are Software Reusability, Software Maintenance, Machine Learning and Image Processing. Email: parvinder.sandhu@gmail.com