International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

Implementation of Enhancing Security of Data using AES Cryptography

Vikas Goyal[1], Geeta Arora[2]
[1]Assistant Professor, CSE Department, MIMIT-Malout, India
[2]Assistant Professor, ECE Department, MIMIT-Malout, India

***Abstract*—** *There is a considerable that Data may contain confidential information that needs to be secured from any third party access. Encryption algorithms play a main role for securing these types of data. The encryption algorithms are varied in their performance. This paper evaluate the performance the AES encryption algorithms. The performance of encryption algorithms for all type of data.*

***Keywords*—** *Cryptography, AES, DES, encryption, decryption.*

I. INTRODUCTION

[1] It is the practice and study of techniques for secure communication. More generally, they are related to various areas in information security such as data confidentiality, data integrity, authentication, and non-repudiation. It deals with the conversion of a plain intelligible data into an unintelligible data and again modifying that message into its original form. Cryptography prior to the modern age was effectively synonymous with encryption and converts information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique required to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. It provides Confidentiality, Integrity, and Accuracy. [4] Cryptography algorithms play an important part in information security. Its division is done into Symmetric and Asymmetric key cryptography.

1.1. Symmetric Key Cryptography

In Symmetric key encryption single key is used to encrypt and decrypt data. The distribution of keys should be done before transmission to happen between two parties. This Key plays an important role in encryption and decryption. Use of weak key in the algorithm can easily lead data to be decrypted. The size of the key determines the strength of such type of key encryption. Symmetric algorithms are of two types: block ciphers and stream ciphers. The first type of symmetric algorithms i.e., block ciphers are operating on data in groups or blocks. Examples included are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. The second types of symmetric algorithms are Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. Encryption algorithms consume such 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.

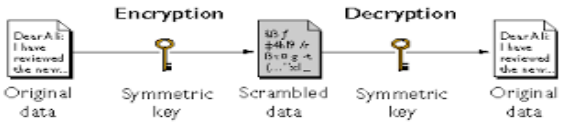

Fig. 1.1. Symmetric key cryptography.

1.2. Asymmetric Key Cryptography

In Asymmetric key encryption, double keys are used; private keys and public keys. Public key is used for encryption while private key is used for decryption (e.g. Digital Signatures). Public key is meant to the public and private key to the user. There is no distribution required before transmission. Asymmetric encryption techniques comparatively 1000 times slower than Symmetric techniques, since they require more computational processing power.

II. AES

[4] Advanced Encryption Standard (AES) also termed as the Rijndael algorithm is a symmetric block cipher. It was believed that security of DES was hindered due to advancement in computer processing power. NIST serves the purpose to define a substitution for DES that can be applied in non-military information security applications by US government agencies. [6] AES is a block cipher with 128 bits of a block length. AES allows for three different key lengths: 128, 192, or 256 bits. Processing for encryption consists of 10 rounds for 128- bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256- bit keys. Processing for each round includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and in addition the round key. The order in which these four steps are executed is different for encryption and decryption. AES encryption is fast and flexible. It can be implemented on different platforms especially in small devices. AES has been tested for many security applications.

2.1. AES Encryption

[3] In encryption mode, the initial key is added to the input value at the very beginning, which is called an initial round. This is followed by 9 utterance of a normal round and ends with a slightly modified final round, as one can see in Figure 2.2 During one normal round the following operations are performed in the following order: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The final round is a normal round without the Mix Columns stage.

Vikas Goyal and Geeta Arora, "Implementation of enhancing security of data using AES cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 123-126, 2016.

International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

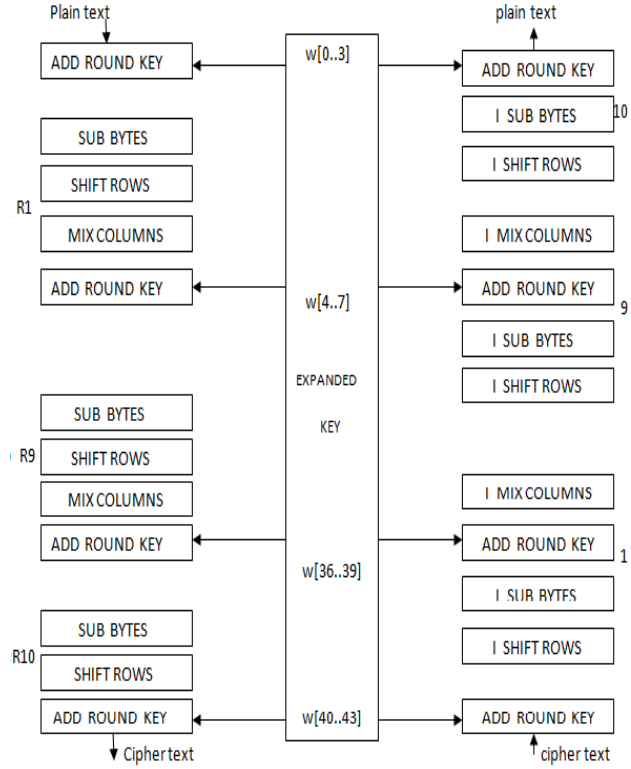

Fig. 2.1. Encryption and decryption of AES.

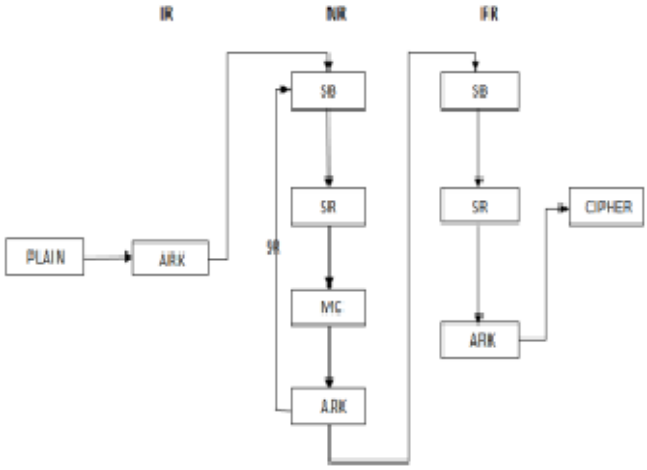

Fig. 2.2. General structure of encryption.

2.1.1. Steps in AES encryption

- Sub Bytes—a non-linear replacement step where each byte is substituted with another according to a lookup table.
- Shift Rows—a transposition step where each row of the state is moved cyclically a certain number of steps.
- Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
- Add Round Key—each byte of the state is combined with the round key; each round key is obtained from the cipher key using a key schedule

2.1.2. Code for AES encryption

```
FileInputStream fis = new FileInputStream (file_path.getText());
FileOutputStream fos = new FileOutputStream(p);
byte k [ ] = "KESHAVKUMARSINHA".get bytes();
SecretKeySpec key = new SecretKeySpec(k, "AES");
Cipher cienc = Cipher.getInstance("AES");
cienc.init(Cipher.ENCRYPT_MODE, key);
CipherOutputStream cos = new CipherOutputStream(fos, cienc);
byte [ ] buf = new byte [4096];
int read;
```

2.2. AES Decryption

[3] In decryption mode, the operations are in reverse order compared to their order in encryption mode. Thus it starts with an initial round, followed by 9 utterance of an inverse normal round and ends with an AddRoundKey. An inverse normal round consists of the following operations in this order: AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes. The starting round is an inverse normal round without the InvMixColumns.

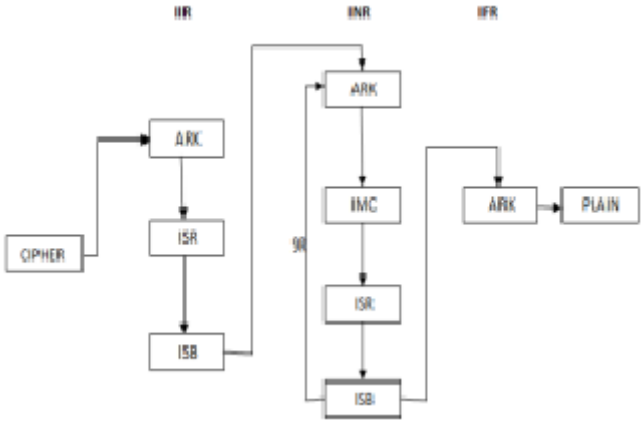

Fig. 2.3. General structure of decryption.

2.2.1. Steps in AES decryption

- InvShiftRows—is the inverse of the ShiftRows transformation. The bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets).
- InvSubBytes—is the inverse of the byte substitution transformation, in which the inverse Sbox is applied to each byte of the State.
- InvMixColumns—is the inverse of the MixColumns transformation. InvMixColumns operates on the State column-by-column, treating each column as a four term polynomial.
- AddRoundKey—is its own inverse, since it only involves an application of the XOR operation. Equivalent Inverse Cipher transformations differ from that of the Cipher, while the form of the key schedules for encryption and decryption remains the same.

2.2.2. Code for AES decryption

```
FileInputStream fis = new FileInputStream (file_path.getText());
FileOutputStream fos = new FileOutputStream("d"+p);
byte k [ ] = "KESHAVKUMARSINHA".get bytes();
```


Vikas Goyal and Geeta Arora, "Implementation of enhancing security of data using AES cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 123-126, 2016.

International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

```
SecretKeySpec key = new SecretKeySpec(k, "AES");
Cipher cidec = Cipher.getInstance("AES");
cidec.init(Cipher.DECRYPT_MODE, key);
CipherOutputStream cos = new CipherOutputStream(fos, cidec);
byte [ ] buf = new byte [4096];
int read;
```

III. TRIPLE DES

Triple DES was developed to address the clear flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by using the algorithm three times in succession with three different keys. The integrated key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker. It has always been regarded with some suspicion, since the original algorithm was never designed to be applied in this way, but no serious deficiency have been uncovered in its design, and it is today available cryptosystem used in a number of Internet protocols.

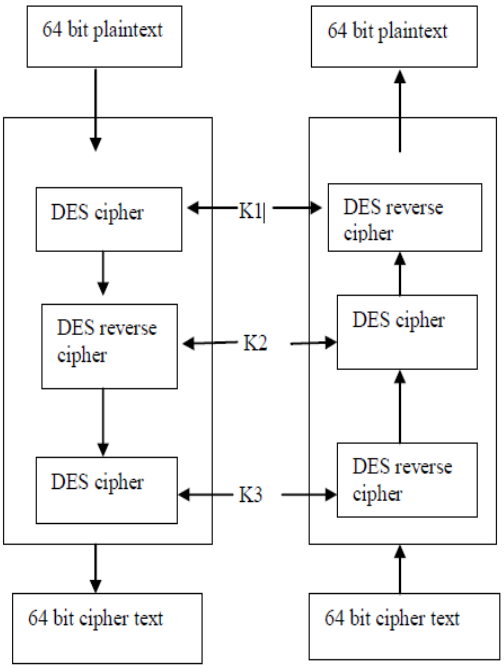

Fig. 3.1. Encryption and decryption of DES.

[2] Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion. The following Figure 3.4 and figure 3.5 is the block diagram of 3DES as shown in below.

IV. EXPERIMENT AND RESULT

This paper was successfully completed with the implementation of Encryption and decryption for AES algorithm. Implementation of AES algorithm was done in NetBeans for providing security to any type of data like text data, image data, video data, and audio data. This implementation will be useful in providing security to any data from third part access.

V. COMPARISONS BETWEEN AES AND DES

In the table below a comparative study between Triple DES and AES is presented into nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key.

TABLE 4.1 Comparison between AES and DES.

Factors	AES	Triple DES
Key Length	128,192 or 256 bits	(k1,k2andk3) 168 bits (k1 and k2 is same) 112bits
Block Size	128,192 or 256 bits	64 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	2000	1978
Security	Considered secure	Proven inadequate
Cryptanalysis Resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential Brute force attacker could be analyze plain text using different cryptanalysis
Possible Keys	2^{128}, 2^{192} and 2^{256}	2^{112} or 2^{168}
Possible ASCII Printable Character Key	95^{16}, 95^{24} or 95^{32}	95^{14} or 95^{21}
Time required to checking all possible key at 50 billion key per seconds.	For a 128- bit key :$5*10^{21}$ years	Foe a 112–bit key :800 Days

VI. CONCLUSIONS

Encryption algorithm plays a very crucial role in Data security. Our research evaluates the performance of the two encryption algorithms AES and Triple DES. With the theoretical comparisons, experimental analysis and comparison is done for Triple DES and AES algorithms. Based on the text files used and the experimental result it was concluded that AES algorithm ingest least encryption and decryption time as compared to Triple DES algorithm. AES has high throughput than Triple DES.

REFERENCE

[1] V. Agrawal, S. Agrawal, and R. Deshmukh, "Analysis and review of encryption and decryption for secure communication," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, issue 2, pp. 1-3, 2014.

[2] S. Karthik and A. Muruganandam, "Data encryption and decryption by using triple DES and performance analysis of crypto system," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, issue 11, pp. 24-31, 2014.

[3] M. Pitchaiah, P. Daniel, and Praveen, "Implementation of advanced encryption standard algorithm," *International Journal of Scientific & Engineering Research*, vol. 3, issue 3, pp. 1-6, 2012.

[4] P. C. Mandal, "Evaluation of performance of the symmetric key algorithms: DES, 3DES, AES and Blowfish," *Journal of Global Research in Computer Science*, vol. 3, issue 8, 2012.
[5] S. Soni, H. Agrawal, and M. Sharma, "Analysis and comparison between AES and DES cryptographic algorithm," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, issue 6, pp. 362-365, 2012.
[6] S. D. Rihan, A. Khalid, and S. E. F. Osman, "A performance comparison of encryption algorithms AES and DES," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, issue 12, pp. 151-154, 2015.