ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Combined Cryptographic Standards for Minimizing the Decryption Time of Encrypted Data using E-AES and D-AES

Ravikant K[1], Umesh Kumar Lilhore[2]

M.Tech Scholar, Dept. of CSE, NRI Institute of Information Science & Technology, Bhopal (MP), India[1]

Assistant Professor, Dept. of CSE, NRI Institute of Information Science & Technology, Bhopal (MP), India[2]

ABSTRACT: Due to the excessive use of cloud storage by users, security becomes the major factor, another major aspect is the time to access the stored data. It has been observed that the data can be stored in different patterns, such as original plain text and the encrypted cipher text. Due to the security of user's data, the encrypted data is stored in to the cloud. Now with this method of encryption, we require different cryptographic algorithms used to encrypt the users data. In our survey [1], it has been analyzed that different algorithms had been implemented and found different time duration is required to decrypt the encrypted cipher data downloaded from the cloud. In [1] some of the key exchange algorithm is used to for user authentication. In this paper, we have proposed some advanced cryptographic algorithms and key exchange algorithms which will help to enhance the security and also reduce the decryption time.

KEYWORDS: Cryptography, DES, TDES, AES, Diffie-Hellman, Elgamal.

I. INTRODUCTION

In communication networks the security of data transmission is a vital problem. A communication is said to be reliable only when it provides a high security to data. The science of keeping users data secure in the form of cipher text is known as cryptography. The encryption process is applied before sending the data into the cloud and decryption is applied after downloading the data from the cloud.

Encryption is one of the main principles which guarantees security of sensitive information. Algorithm performs substitutions and transformation techniques on the plain text and changes it into cipher text, which cannot be read by the users. The encryption algorithm are classified into two groups

1. Symmetric key (also known as secret key)
2. Asymmetric key (also known as public key)

The method used in symmetric key encryption are performed using the same key. It is also called as conventional encryption. Asymmetric encryption method are performed using different keys-one public and one private. It is also called as public key encryption. In our survey paper [1], we had studied about decryption time of different algorithms with different data input size. This paper aims to find the decryption time of other advanced algorithms such as AES and Elgamal.

In this paper we'll analyze different algorithms and try to combine algorithms for making the cryptosystem more secure. Alanazi et al [2] done a comparative analysis of three algorithms (DES, TDES and AES) with nine different factors like key length, cipher type, security etc. In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits. A block cipher may take 128-bit plain text and encrypts it to 128-bit cipher text [3].

II. ALGORITHMS USED

A. *DES (DATA ENCRYPTION STANDARDS)*

DES is a fiestel-type substitution-permutation network (SPN) cipher. The DES is uses a56-bit key which can be broken using brute-force method. A 16 cycle is used with an overall 56-bit key into 16 48-bit subkey. To decrypt identical keys

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

are used in reversed order. The L and R blocks are in size of 32-bits each, combining the overall block size of 64-bits. The hash function 'f' specifies by standard using the other given name as "S-boxes", takes 32-bit data block as input and produces 32-bit output.

B. ***TDES (TRIPLE DES)***

TDES was developed to overcome the flaws of DES, without designing the whole new cryptosystem. TDES simply run the DES three times with three different keys. The combined key size becomes 168-bits (3*56). The TDEA involves 3 64-bit keys (k1,k2,k3) in encrypt-decrypt-encrypt (EDE) modes. The plain text is encrypted with k1, then decrypted with k2 and again encrypted with k3. The following are the three key options

Option1: the preferred option, employs three mutually independent keys (k1≠k2≠k3), keyspace is 3*56=168.
Option2: employs two mutually independent keys and a third key is same as the first key (k1≠k2=k3), keyspace is 2*56=112.
Option3: employs three identical keys (k1=k2=k3). This option is similar to DES.

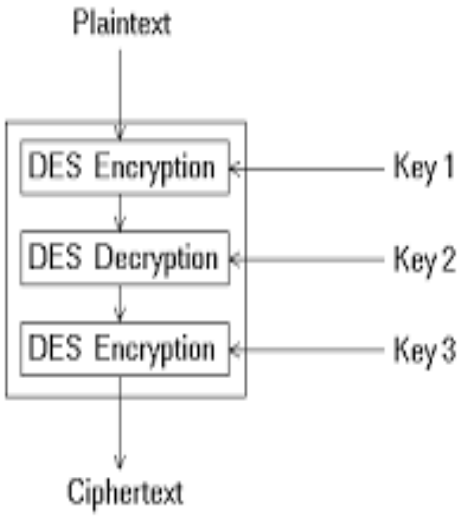


Figure1: TDES

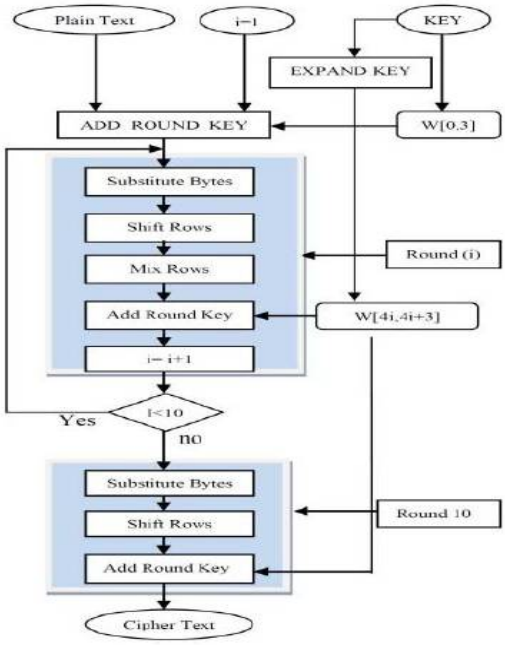


Figure2: AES

C. ***AES (ADVANCE ENCRYPTION STANDARDS)***

AES is the advance encryption standard started to replace DES. AES supports any combination of data and key-length of 128, 192 and 256 bits. The algorithm is also called as AES-128, AES-192, AES-256 depending on the key length. AES executes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys [5]. AES allows the data length which can be divided into four basic blocks and form a 4*4 matrix. The cipher begins with the AddRoundKey. Before reaching nine rounds, during each round the transformation of data is performed.

1. Sub-keys
2. Shift-rows
3. Mix-cloumns
4. Add round key

Each round of AES is observed by the following transformations.

- Substitution Byte Transformation: in sub-byte transformation, each byte of data block is transformed into another block using substitution box of 8-bits.
- Shift Rows Transformations: it is byte transposition the bytes of the last three rows are cyclically shifted.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

- MixColumns transformations: this round is equivalent to a matrix multiplication of each column of the states. A fix matrix is multiplied to each column vector.
- AddRound transformation: it is a bitwise XOR between the 128-bit of present states and 128 bits of the round key. The transformation is its own inverse.

D. ***ELGAMAL***

Elgamal is a cryptosystem which is based on the discrete logarithm problem. It relies on the assumption that DL cannot be found in feasible time. The original public key system is Diffie-Hellman, it requires calculation of common private key. This poses problems if the sryptosystem should be applied to communication system. The Elgamal simplifies the Diffie-Hellman key exchange 'k'. This exponent is a replacement for private component.

Key Generation

The basic requirement for a cryptographic system is atleast one key for symmetric algorithm and two keys for asymmetric.

- Prime number and group generation (p,q,g^b).
- Private key selection (b) $1<=b<=p-2$
- Public key assembling
  Public key=g^b mod p, triplet (p,g,g^b) and private key is b.
- Public key publishing

Table 1: Comparison of DES, TDES and AES

Factors	DES	TDES	AES
Key Length	56 bits	(k1,k2,k3) 168 bits (k1 & k2 same) 112 bits	128, 192, 256 bits
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Block Size	64 bits	64 bits	128, 192, 256 bits
Security	Inadequate	One only week which is exit in DES	Secure
Possible Keys	2^{56}	2^{112} or 2^{168}	2^{128}, 2^{192} or 2^{256}

III. METHODS USED IN PRESENT SYSTEM

We have analysed different methods in the system and also analysed the decryption time for each algorithms.

Method 1:

When the cryptographic algorithms are used for encryption and decryption such as RSA, DES and TDES.

Table 2

Decryption Time of single algorithms (without combining with other key exchange algorithms)

Data Size (byte)	RSA (Av) in ms	DES (Av) in ms	TDES (Av) in ms	No. of Iterations
643	38.2	12.8	36.8	5
2342	34.0	7.8	53.6	5
4921	34.6	9.0	53.8	5
14763	42.2	15.6	86.6	5
29526	34.6	41.2	138.2	5

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Method 2:
For enhancing the security, the key exchange algorithms are used for data access security. User enters the private key and proves the identity for authentication. Now in this method Diffie-Hellman is implemented with cryptographic algorithms for increasing the security and user authenticity.

Table 3
Decryption Time of algorithms combined with Diffie-Hellman Key Exchange algorithm

Data Size (byte)	Diffie-Hellman (Av) in ms	Diffie-Hellman+ RSA (Av) in ms	Diffie-Hellman+ DES (Av) in ms	Diffie-Hellman+ TDES (Av) in ms	No. of Iterations
643	15	53.2	27.8	51.8	5
2342	15	49.2	22.8	68.6	5
4921	15	49.6	24.0	68.8	5
14763	15	57.2	30.6	101.6	5
29526	15	49.6	56.2	153.2	5

IV. PROPOSED ALGORITHM

Present system has some loopholes and security issues with the cryptographic algorithms. It has been observed by analysing the hybrid algorithm, the time of decryption is also increased. In this paper we have taken the advanced cryptographic algorithm and combined with Diffie-Hellman and ElGamal key-exchange algorithm to form a more secure system with less amount of decryption time.
In this we have used AES (Advanced Encryption Standards) for encryption and decryption and ElGamal, Diffie-Hellman algorithm for key-exchange user authentication. With this combination we have introduced two new hybrid algorithms as E-AES (ElGamal- AES) and D-AES (Diffie-Hellman- AES).
First lets find out the decryption time of AES before combining with other key exchange algorithms and also the average time of ElGamal key exchange.

Table 4
Decryption Time of AES and Elgamal key-exchange time

Data Size (byte)	ElGamal (Av) in ms	AES (Av) in ms	No. of Iterations
643	16.2	13.6	5
2342	16.2	14.2	5
4921	16.2	13.2	5
14763	16.2	15.0	5
29526	16.2	21.0	5

Now lets combine the AES algorithm with ElGamal and Diffie-Hellman to introduce our proposed algorithm.

Table 5
Decryption Time of hybrid algorithms E-AES and D-AES

Data Size (byte)	E-AES (Av) in ms	D-AES (Av) in ms	No. of Iterations
643	29.8	28.6	5
2342	30.4	29.2	5
4921	29.4	28.2	5
14763	31.2	30.0	5
29526	37.2	36.0	5

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Now let's analyse all the hybrid algorithms together.

Table 6
Decryption time comparison of all hybrid algorithms

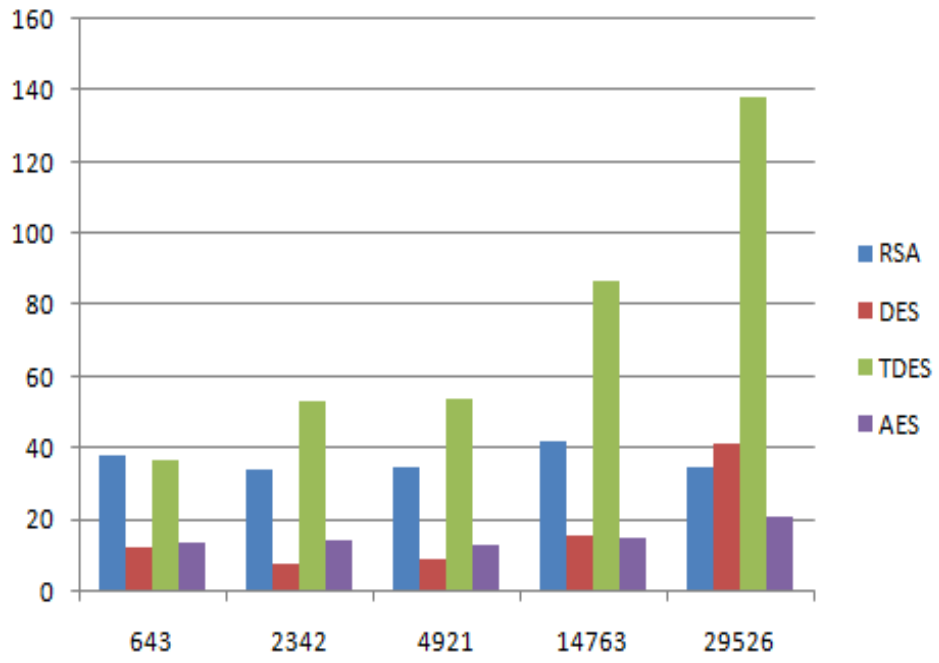
Data Size (in bytes)	No. Of Iterations	Diffie-Hellman (Av) in ms	ElGamal (Av) in ms	Diffie-Hellman+RSA (Av) in ms	Diffie-Hellman+DES (Av) in ms	Diffie-Hellman+ TDES (Av) in ms	D-AES (Av) in ms	E-AES (Av) in ms
643	5	15.0	16.2	53.2	27.8	51.8	28.6	29.8
2342	5	15.0	16.2	49.0	22.8	68.8	29.2	30.4
4921	5	15.0	16.2	49.6	24.0	68.9	28.2	29.4
14763	5	15.0	16.2	57.2	30.6	101.6	30.0	31.2
29526	5	15.0	16.2	49.6	56.2	153.2	36.0	37.2

In the above table we have implemented the combination of Diffie-Hellman and Elgamal with the most secure cryptography algorithm (AES) and we have found the decryption time is less as compared to the Diffie-Hellman+TDES hybrid algorithm which was proposed in our survey paper.

V. RESULTS

The D-AES and E-AES is implemented and found the following results.

Graph 1
Decryption Time of different algorithms.



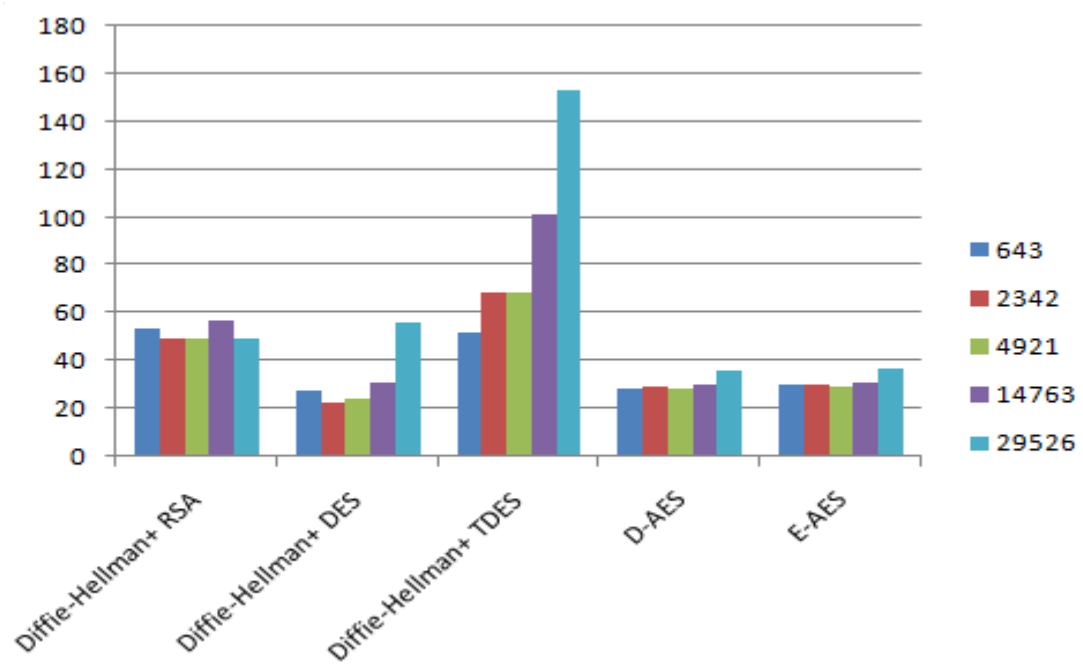
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Graph 2
Decryption Time of different hybrid algorithms.



VI. CONCLUSION AND FUTURE WORK

By the above graphs it has been shown that the hybrid algorithm D-AES and E-AES are more efficient than other hybrid algorithm. The D-AES and E-AES decryption time is less than other Diffie-Hellman+ TDES and it is more efficient with respect to security and key management. With this approach we conclude our work and in future this method can be implemented in other cloud softwares, so that a system can be developed for users.

REFERENCES

1. Anjum Asma and Gihan Nagib,'Energy Efficient Routing Algorithms for Mobile Ad Hoc Networks–A Survey', International Journal of Emerging Trends & Technology in computer Science, Vol.3, Issue 1, pp. 218-223, 2012.
2. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, Volume 2, ISSUE 3, pp. 152-157, MARCH 2010.
3. A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji, and S.M.Mohammed," Implementation Stage for High Securing Cover- File of Hidden Data Using Computation Between Cryptography and Steganography", International Conference on Computer Engineering and Applications (ICCEA09), Telecom Technology and Applications (TTA), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Vol.19, Session 6, p.p 482-489.
4. Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.
5. 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, pp. 386-391, July 2012.
6. Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 211-216, 2010.
7. Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, "AES and Confidentiality from the Inside Out", the 12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591, 2010.
8. Rashmi Singh and Shiv Kumar, "Elgamals Algorithm in Cryptography",International Journal of Scientific and Engineering Research, Vol 3, Issue 12, December 2012.