2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-7281-7741-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICACITE51222.2021.9404734

# Comparative Study on Different Encryption and Decryption Algorithm

1st Jatin Dutt Gaur
*Student, Department of Computer Engineering*
*Galgotias University*
*Greater Noida, India*
jatin_dutt.scsebtech@galgotiasuniversity.edu.in

2nd Adarsh Kumar Singh
*Student, Department of Computer Engineering*
*Galgotias University*
*Greater Noida, India*
adarsh_kumar1.scsebtech@galgotiasuniversity.edu.in

3rd Nipun Pratap Singh
*Student, Department of Computer Engineering*
*Galgotias University*
*Greater Noida, India*
nipun_pratap.scsebtech@galgotiasuniversity.edu.in

4th Gokul Rajan V
Assistant Professor,
School of Computing Science and Engineering,
Galgotias University, UP, India
gokulranjan@galgotiasuniversity.edu.i n

*Abstract*- **With the advancement in digitalization, the security of data/file has become a major point of concern. With this digitalization the Encoding and decoding of information have recently been widely developed and investigated, because there is a demand for an inviolable encoding and decoding algorithm which is hard to crack. To fulfill all the demands Cryptography plays major roles. Nowadays, many researchers have proposed many encryption and decryption algorithms such as HMAC, DES, RSA, TWOFISH, BLOWFISH, AES, IDEA and others. But most of the proposed algo's/systems have encountered some problems such as lack of noun muscular and a large amount of time applied to the packet delay to preserve the protection between the terminals on the communication channel. The comparison has been made and the final analysis results are briefed in the result.**

***Keyword: Cryptography, Symmetric, Asymmetric, Encryption, Decryption, Data.***

## I. Introduction

Cryptography has played a vital role in securing a network for a long period of time but gives an approach to store touchy data or communicate it across uncertain organizations so it can't be pursued by anybody aside from the expected beneficiary. Cryptography involves a lot of calculations joined with keys to convert the first message (Plain-text) to scrambled message (Cipher-text), harking back to the proposed beneficiary side to the first message (Plain-text)[1].

In cryptography, encryption is the way toward encoding data. This cycle changes over the first portrayal of the data, known as plaintext, into an elective structure known as ciphertext. In a perfect world, just approved gatherings can decode a ciphertext back to plaintext and get to the first data. Encryption hides your data from curious eyes.

Decryption /Decoding means that you or the PC will inspect and understand encoded or scrambled material or other information and change it back into text. This word may be used to define a technique for physically decoding the data or decoding the information using the correct codes or keys [2].

In the present situation the value of a personal data becomes more valuable than any precious metal or anything. Encrypting and decrypting a file/documents provides security for data all time. It maintains integrity of data. It provides a complete compliance of data with comprehensive security. Encryption and decryption work when the data is transferred from one device to another device it provides a complete authentication from any unknown user.

Working of Encryption and Decryption,

1) *Plaintext* –This is the text message that an algorithm is used to apply to.
2) *Encryption Algorithm* – Performs mathematical operations in order to make the plaintext replacements and transformations.
3) *Secret Key* –This is the input for the algorithm as the key decides the encrypted output.
4) *Cipher text* -This is the encrypted or scrambled message created by the secret key by applying the plaintext message to the algorithm.
5) *Decryption Algorithm* –For encryption, this is the opposite algorithm. It uses the ciphertext and the secret key to derive the plaintext code.

Now comparing 9 different Encryption and decryption algorithms on the basis of different factors. Also, the working of those is shown in this paper [3].

## II. Cryptographic Algorithms

### A. Triple DES

The Triple Des encryption algorithmic program (Triple DES), that applies the DES cipher algorithmic program 3 times to each information block, may be a symmetric-key block cipher. The information cryptography Standard's (DES) 56-bit key now not enough within the face of contemporary cryptological techniques and supercomputing ability. However, to make an additional stable coding, the changed version of DES, Triple DES (3DES), uses a

constant algorithmic program. Meanwhile now there is no requirement to develop a very new square code (block cipher) algorithmic program, Triple DES offers a fairly convenient technique of raising the key size of DES to defend against such attacks [4].

Triple DES uses a "key bundle" that consists of 3 of DES keys, K1, K2, K3. Every key is fifty six bits. The encryption algorithm coding rule is:

$$\text{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext}))).$$

That is, DES encrypt with $K1$, DES *decrypt* with $K2$, then DES encrypt with $K3$.

Decryption is the reverse:

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext}))).$$

That is, decrypt with $K3$, *encrypt* with $K2$, then decrypt with $K1$.

Each triple encryption encrypts one block of 64 bits of data.

The middle operation in every case is the reverse of the primary and last. This improves the strength of the algorithmic program by using a pair of keys and provides backward friendly DES with keying option three. Three DES operations take place in the sequence of encrypt-decrypt-encrypt with three different keys. Triple DES using Cipher Block Chaining (CBC) provides more protection by creating it tough to arrange ciphertext blocks again.

The whole contact interface will be split into two groups of users. The first type of user is the administrator, who monitors the entire correspondence and is alerted if any malicious mail is found. The second form is the general user, who will be an employee of the company and connect via emails with all other users. When the administrator sends the mail to any general user, the message will be encrypted using any particular key of his choosing. The key is sent by mail to the individual person who receives the encrypted mail. Then the general user can then use the key for the purpose of decryption [5].

The implementation offers a communication protection strategy which essentially deals with the theft of an organization's information and protected data. By finding the damaging emails, this technique solves the problem description.

### *B. Twofish encryption algorithm*

Twofish algorithmic program is a regular block cipher. For secret writing and decipherment, only a single secret key is used. Twofish comprises a 128-bit block size, and accepts a key of up to 256 bits of any key length. On each 32-bit and 8-bit CPUs, and on hardware, Twofish is quick. And it may be used flexibly in any network applications wherever keys are perpetually changed and in applications wherever there's very little or no RAM and fixed storage accessible [6].

On high-end CPUs, Twofish yells, and it is versatile enough for small CPUs with modern cards. It fits well on hardware in addition. And between key-setup time and encoding speed, there square measure several performance trade-offs that create it special among the AES candidates. Twofish is far quicker; its key configurations are often as fast as one.5 ciphers.

Because of its distinctive combination of pace, skillfulness, and conservative nature, we tend to feel that Twofish is the most suitable choice among all the AES candidates. forward that it's secure. Across all CPUs, Twofish is the quickest AES candidate. Twofish is compatible with sensible cards, together with those with simply a number of registers, a number of bytes of RAM, and a little memory. and therefore the hardware fits into a number of gates.

The ability to trade off key-setup time for secret writing speed, and read-only memory and RAM for secret writing speed, and no alternative algorithmic rule has a similar skillfulness in implementation. On 32-bit CPUs, 8-bit CPUs and hardware, these selections exist.

### *C. Blowfish encryption algorithm*

Blowfish is a type of encryption that is an alternative to the DES Encryption Technique. It is substantially faster than DES and with no successful cryptanalysis technique found to date, provides a strong encryption rate. It is one of the first safe block cyphers not subject to patents and is thus freely open for use by anyone. In terms of encryption time, decryption time & throughput, Blowfish offers better performance than AES, DES and 3DES [7].

#### *a) Encryption with Blowfish*

There are two key stages of Encryption with Blowfish: sixteen iterations of the round function and an output operation.

#### *b) Decryption with Blowfish*

It is necessary to remember that the structure of the encryption must be used in the same order i.e. the final exclusive-or should not be used before the round functions are started. This exclusive-or from encryption would be undone by the first exclusive-or from the round feature of decryption.

#### *c) Advantages of Blowfish*

Blowfish is a relatively quick block cipher following the completion of the key schedule due to the limited number of rounds (sixteen) and the simplicity of the round operation.

#### *d) Disadvantages of Blowfish*

In Blowfish, the main schedule is very time consuming (equivalent to encryption of about 4 KB of data). However, as defense against brute-force attacks, this can be an advantage in certain situations.

The results indicate that Blowfish's decryption time and decryption time output are better than all four algorithms studied, and it provides better efficiency, followed by AES, DES and 3DES, Because of its minimum time for decryption and overall throughput.

### *D. Advanced Encryption Standard (AES)*

One of the most popular and frequently used symmetric block cipher algorithms worldwide is the Advanced Encryption Standard (AES) algorithm. In order to encrypt and decrypt sensitive data, this algorithm has its own special structure and is applied worldwide in hardware and software. When encrypted by the AES algorithm, it is incredibly hard for hackers to get the real data. To date, there is no evidence to crack this algorithm [8].

It is based on a "substitution-permutation network". It involves a variety of similar operations, some of which include replacing inputs with unique outputs and others

involve shuffling bits around. Interestingly, rather than bits, AES performs all of its computations on bytes. The 16 bytes of the 128 bits of a plaintext block are thus handled by AES.

These 16 bytes are arranged for processing as a matrix in four columns and four rows. Unlike DES, the number of rounds in AES is variable and depends on the key duration. For 128-bit keys, it uses 10 rounds, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds, calculated from the original AES key, uses a different 128-bit round key.

One of the efficient algorithms is the advanced encryption standard (AES) algorithm and it is commonly supported and implemented on hardware and software. This algorithm enables various key sizes such as 128, 192, and 256 bits with 128-bit block cipher to be dealt with. According to the research findings, AES has the potential to provide much more protection compared to other algorithms such as DES, Twofish, 3 Des Etc [9].

*E. IDEA encryption algorithm*

Via five steps, MD5 generates the message digest, i.e. padding, appending span, dividing input into 512-bit blocks, initializing chaining variables, processing blocks and four rounds, and using various constants in each iteration. The Regular Block Size is 16 bytes of 128 bits. In round blocks, where part of the key is applied to the round and then other operations are carried out on it, a block cipher would normally operate. After a given number of rounds, say between ten and 16, we end up with our cipher text for that block [10].

The 64-bit plain text block input is divided into 4 parts (16 bits each declaring q1 to q4), so q1 to q4 will be the inputs for the initial round algorithm.

- Here are eight rounds.
- Composed of 128 bits, the secret is.
- 6 sub-keys will be generated in each round.
- For each subkey 16 bits are used.
- On the four q1 to q4 input blocks, all these subkeys will be placed
- Output Transformation is the last action that normally benefits only Four subkeys.
- The final result produced is four ciphertext blocks from B1 to B4 (Every sixteen bits).
- They are blended to produce the final 64-bit ciphertext blocks.

IDEA may be a known cipher that many experts have examined for the last ten subkey formations for the round, using 6 sub-keys for each of the 8 rounds (therefore 8 x 6 = 48 subkeys are necessary for the rounds). Four subkeys (i.e. 48 + 4 = 52 subkey total) gain from the last performance transformation. All these 52 subkeys will be created for years from an input key of 128 bits, and no strike was found against five or higher of its 8.5 rounds, however.

IDEA can be trusted due to its greater intensity against cryptanalytic attacks because of its more efficiency or higher security. Basically, the aim of the algorithm is to encourage learners to get familiar with this algorithm by providing a basic version that allows a situation to function well and equate the IDEA methodology with the methods of DES and AES.

*F. MD5 encryption algorithm*

The fifth variant of the Message Digest Algorithm is the message digest algorithm It creates a review of a 128-bit message. MD5 is a much better choice than implementations of the message review and get 512-bits of blocks, that are split into 16 blocks, each 32-bit, which generates a 128-bit information review, a collection of four 32-bit blocks. Via five phases, MD5 produces the information review, appending size, splits input message into 512-bit blocks, initializing chain variables, and using various constants in each iteration.

It was designed for the primary purpose of protection because it takes data of any size and shows a 128-bit hash value output.

*1: Including Bits of Padding*

Padding means swapping additional bits with the initial post. Then the initial message is padded into MD5 so that 448 modulo 512 is congruent with its bit length. In such a way that the cumulative bits are 64 fewer than the length of 512 bits, padding is done. And initial message size is already consistent with 448 modulo 512, the padding will be ended [11].

*2: Including size to size*

After padding at the end, which is used to record the duration of the original information, 64 bits are inserted. Modulo 2^64. At this point, the resulting message has a size multiple of 512 bits.

*3: Initialize the buffer with MD*

To compute the values for the message digest, a four-word buffer is used to (X, Y Z, W). Here X, Y, Z, W are 32-bit records which are initialized.

*4: Message processing in a 16-word block*

MD5 uses supplement features that input the data as 3 32-bit numbers and produce 32-bit information. These use logical operators like OR, XOR, NOR. The contents of 4 buffers are merged with data using this auxiliary buffer and sixteen rounds are achieved sixteen basic operations.

It is actually very important for the storage of the information on the clouds and internet has to keep the security and privacy of the data at its highest priority. The reliable algorithm should be implemented to encrypt private data. Recent studies suggest that SHA algorithms have been given priority over MD5, MD5 is more vulnerable to internet attacks [12].

*G. HMAC encryption algorithm*

HMAC is a digital signature designed to reuse the digest algorithms for MD5 and SHA-1 messages and to provide an efficient data integrity protocol function. This algorithm is used to safely encrypt plain text, is used in the SSL certificate

and Secure Socket Layer protocol, and has been chosen as the appropriate security implementation for the internet protocol, i.e. IP.

*Step1: To Make symmetric key's length equal to several bits in each block.*

We need to act in order to equal the length of the key to the number of bits depending on each one. Three theories exist. In each block, less than the number of bits is the length of a key. In this example, to compare the length of a key to several bits, we need to expand the length of the key by adding many 0 bits [13].

*Step2: Symmetric XOR with a pad.*

In this step, to produce a variable called S1, we XOR the symmetric to the pad.

*Step3: Including S1, the initial message.*

In this step, at the end of S1, we add the original message.

*Step4: Apply the algorithm to the message - digest.*

In this step, some of the selected message digest algorithms (MD5, SHA-1, SHA-512, etc.) are added to the output of step three. Let's assume that the performance of this phase four is H

*Step5: Symmetrical key XOR with paper.*

In this step, the symmetric key with pad XOR is used for generating the variable named S2.

*Step6: Append S2 to H.*

We take the digest of the message determined in step 4 in this step and add it to the end of the S2 extracted from the preceding step, i.e. step 5.

*Step7: Algorithm for message digest.*

We will apply the chosen message-digest algorithm to the performance of step 6 in this step. This step's produced message digest is the final MAC. We've seen the fundamental principle of the Hash-based Message Authentication Code in this article and it's working. In the case of more than one recipient, we cannot use the Hash-based Message Authentication Code. This is because the symmetric key is used by HMAC to create the MAC. Only two parties, i.e. the sender and recipient, must share the symmetrical key [14].

*H. RSA security*

The RSA algorithm is an algorithm for asymmetric cryptography. Asymmetric simply implies that it acts on two distinct keys, i.e. Private Key and Public Key. The public key is given to everyone as the name describes, and the private key is kept private. The cryptography of the public key is primarily used for authentication, non-repudiation, and exchanging of keys [15].

One of the reasons RSA has been most commonly used is that it enables a message to be encrypted by either of the two keys and the opposite key to decrypt it, promising data and electronic communications confidentiality, transparency, authenticity and non-reputability. It is important to remember that RSA will be very vulnerable to attacks by a poor key generation, so care must be taken to ensure that two large random prime numbers are used to measure the module, which will become the public key, and those two primes themselves will consist of the private key.

Although RSA is today's most used cryptography algorithm, there are some drawbacks that need to be taken into account in order for RSA to remain the best and research needs to be done to make RSA quantum resistant. Studies in the field of quantum encryption methods immune to quantum computers are now more than ever needed, as they will soon replace the existing encryption systems.

*I. DES*

DES is a block cipher; the information is encrypted in a 64-bit block. The key length is 56 bits, and the key consists of 64 bits initially. From the key length, the bit positions 8, 16, 24, 32,40,48,56, 64 are discarded. DES is based on two fundamental cryptographic attributes: substitution and transposition. DES involves 16 steps, each of which is referred to as a Round Algorithm [16].

*A. Working of DES*

i. In DES, using a 56 bit key, data is encrypted in 64 blocks. This algorithm converts the 64 bit input into a 64 bit output using a 56 bit key in a sequence of steps.
ii. In order to reverse encryption using the same key, the same steps are used. The adjacent figure shows the overall DES encryption scheme.
iii. The encryption feature has two inputs, the 64-bit plain text (to be encrypted). The 64-bit key (actually 56 bits + 8 parity bits).
iv. The processing of the above figure's plaintext (LHS) occurs in three stages. First, the 64 bit plaintext passes through an initial permutation that rearranges the bits to generate the permissible output.
v. The output of the last round consists of 64 bits that are a function of plain text and key input. To generate pre-output, the left and right input halves are swapped.
vi. Finally, to create 64 bit cipher text, the pre-output is transferred by inverse permutation (initially used). The figure's R.H.S indicates the way in which the 56 bit key is used.
vii. A subkey Ri is then generated for each round by combining left circular shift and permutation. For each round, the permutation function is the same, but due to repeated shifts of key bits, a different subkey is produced.

For certain applications, such as banking systems, DES is now considered to be an unreliable encryption process. There are some empirical outcomes in the cipher that indicate theoretical limitations. Increasing this algorithm, by adding a new level of protection to it is therefore quite necessary. We may change this algorithm in the future by changing the implementation of the function, the configuration of the S-box and replacing the old XOR with a new operation.

## III. RESULTS AND DISCUSSION

Now we are going to compare all the 9 algorithms on different basis/factors. Some of the basic/factor on which we are going to compare are listed below. Developer, Made in Year, Symmetric/Asymmetric, Key used, Key size, Block size, Rounds Used, Flexibility and Power consumption.

Both cryptographic algorithms have points of weakness and points of power. Based on the demands of the program

that will be used, we choose the cryptographic algorithm. The blowfish algorithm is the perfect choice in the case of time and memory according to the parameters of guessing attacks and the necessary characteristics from the results of the experiment and the comparison, since it records the shortest time among all algorithms.

Even the minimum memory capacity is consumed. AES algorithms may be chosen if confidentiality and fairness are major considerations. If the application's demand is for network bandwidth, the best choice is DES. We can consider that blowfish and AES algorithms are used to prevent attacks from being guessed by the application and can be implemented on top of all internet protocols based on IPv4 and IPv6 and the examinations reported in this paper show that all algorithms and classes work well with different execution times and memory consumption. RSA is today's most used cryptography algorithm. RSA to remain the best and some more research needs to be done to make RSA quantum resistant.

***Table 1: Comparison of various algorithms on key factors***

| ***Factors*** | ***Tripledes*** | ***TwoFish*** | ***Blowfish*** | ***AES*** | ***IDEA*** | ***MD5*** | ***HMAC*** | ***RSA*** | ***DES*** |
|---|---|---|---|---|---|---|---|---|---|
| ***Developer*** | IBM | Bruce Schneier | Bruce Schneier | Vincent Rijmen, Joan Daemen | Xuejia Lai and James Massey | Ronald Rivest | Bellare et al. | Ron Rivest, | Horst Feistel |
| ***Made in Year*** | 1978 | 1998 | 1993 | 1998 | 1991 | 1992 | 1996 | 1977 | 1970 |
| ***Symmetric/Asymmetric*** | Symmetric | Symmetric | Symmetric | Symmetric | Symmetric | Message Digest (secure hash) | symmetric | Symmetric | symmetric |
| ***Key used*** | Same key is used for Encryption and Decryption purposes. | A single key is used for encryption and decryption | Same key is used for Encryption and Decryption purposes. | Same key is used for Encryption and Decryption purposes. | Decryption is same as encryption only the key is reversed | It is an unkeyed hash function | Same key is used for Encryption and Decryption purposes. | It involves both public and private keys | Same key is used for Encryption and Decryption purposes. |
| ***Key size*** | 168, 112 or 56 bits | 128, 192 or 256 bits | 32–448 bits | 128, 192 or 256 bits | 128 bits | 28 bits | any | 1,024 to 4,096 bit | 56-bit |
| ***Block size*** | 64 bits | 128 bits | 64 bits | 128 bits | 64 | 512 bit | 512-bit | variable-length | 64 bits |
| ***Rounds Used*** | 48 DES - equivalent rounds | 16 | 16 | 10, 12 or 14 | 8.5 | 4 | 2 | 1 | 16 |
| ***Flexibility*** | Yes | Yes | Yes | Yes | No | No | Yes | Yes | Yes |
| ***Power consumption*** | Low | High | High | Low | High | Low | High | Low | Low |

## IV CONCLUSION

In the upcoming future there will be more advancement in technology. With advancement in technology or Digitalization the security of the personal data becomes a major point of concern. By adopting proper securing techniques like encrypting and decrypting, the security of data becomes more feasible. The conversion of data at the starting point into an unrecognizable form and at the end makes it readable. This makes it difficult for an unknown/ unauthorized user to view it. With this comprehensive security of data leads to complete privacy. Upon comparing all these 9 algorithms, we can come to a conclusion that the RSA algorithm remains one the best algorithms that can be used for securing data with at most security.

## V REFERENCE

[1]. Khalid Ali, Faheem Akhtar, Suhail Ahmed Memon, Anum Shakeel, Asif Ali, Abdul Raheem, "Performance of Cryptographic Algorithms based on Time Complexity", Computing Mathematics and Engineering Technologies (iCoMET) 2020 3rd International Conference on, pp. 1- 5, 2020.

[2]. Yuxiang Li, Yan Li, Jihong Liu, "Discussion on Privacy Issues and Information Security in the Internet of Things", Chinese Control And Decision Conference (CCDC) 2020, pp. 4968-4972, 2020.

[3]. Bhoopal Rao Gangadari, Shaik Rafi Ahamed, "FPGA implementation of compact S-Box for AES algorithm using composite field arithmetic", India Conference (INDICON) 2015 Annual IEEE, pp. 1- 5, 2015.

[4]. Bhoopal Rao Gangadari, Shaik Rafi Ahamed, "Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications", , vol. 3, no. 3, pp. 177-183, 2016.

[5]. Vaishnavi S. Shetty, R. Anusha, Dileep Kumar M.J., Prajwal Hegde N., "A Survey on Performance Analysis of Block Cipher Algorithms", Inventive Computation Technologies (ICICT) 2020 International Conference on, pp. 167-174, 2020.

[6]. Ashraf A.M. Khalaf, Mona S. Abd El-karim, Hesham F.A. Hamed, "A triple hill cipher algorithm proposed to increase the security of encrypted binary data and its implementation using FPGA", Advanced Communication Technology (ICACT) 2016 18th International Conference on, pp. 752-759, 2016.

[7]. Ashraf A. M. Khalaf, Mona S. Abd El-Karim, Hesham F. A. Hamed, "Proposed triple hill cipher algorithm for increasing the security level of encrypted binary data and its implementation using FPGA", Advanced Communication Technology (ICACT) 2015 17th International Conference on, pp. 454-459, 2015.

[8]. Sandeep Kolli, Maciej Zawodniok, "Energy-efficient multi-key security scheme for wireless sensor network", Local Computer

[9]. Networks 2009. LCN 2009. IEEE 34th Conference on, pp. 937-944, 2009.

[10]. Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.

[11]. Z. Yong-Xia and Z. Ge, "MD5 Research," 2010 Second International Conference on Multimedia and Information Technology, Kaifeng, 2010, pp. 271-273, doi: 10.1109/MMIT.2010.186.

[12]. https://www.researchgate.net/publication/234781510_The_Twofish_Encryption Algorithm

[13]. T. Nie and T. Zhang, "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Conference,

[14]. Singapore, 2009, pp. 1-4, doi: 10.1109/TENCON.2009.53961

[15]. S. J. Samuel and S. J. Jenitha, "Enhanced security and authentication mechanism in cloud transactions using HMAC," 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-4, doi: 10.1109/ICCIC.2014.7238548.

[16]. https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data