**PROJECT PHASE-I SYNOPSIS (IB302/IB322/IB333)**

**ON**

**Secure Communication**

*A report submitted in partial fulfilment of the requirement for the award of*

*The degree of*

**BACHELOR OF TECHNOLOGY**

**In**

**COMPUTER SCIENCE AND ENGINEERING/INFORMATION TECHNOLOGY**

A picture containing drawing

Description automatically generated

**Submitted to:**

Guide Name

Designation

**Submitted by:**

Chiraag Singh Dhapola - 180111024 - CSF

Harshit Nayal - 180111045 - CSF

Ashutosh Gautam- 180111039 - CSF

Ritik Mamgai – 180111046 - CSF

**SCHOOL OF COMPUTING**

**DIT UNIVERSITY, DEHRADUN**

(State Private University through State Legislature Act No. 10 of 2013 of Uttarakhand and approved by UGC)

**Mussoorie Diversion Road, Dehradun, Uttarakhand - 248009, India**

**ABSTRACT:**

Securing the information from attackers is very important key aspect in today's life. Many cryptographies algorithms are used in data transmission security. Many encryption algorithm like AES, DES, and RSA etc. have been proposed by researchers.

Encryption is the process of encoding information or data in order to prevent unauthorized access. These days we need to secure the information that is stored in our computer or is transmitted via internet against attacks. There are different types of cryptographic methods that can be used. Basically, the selecting cryptographic method depends on the application demands such as the response time, bandwidth, confidentiality and integrity. However, each of cryptographic algorithms has its own weak and strong points. In this paper, we will present the result of the implementation and analysis that applied on several cryptographic algorithms such as DES, AES and MD5.

**INTRODUCTION:**

**1.Advanced Encryption Standard (AES):**

The **Advanced Encryption Standard** (**AES**), also known by its original name **Rijndael** is a specification for the [encryption](https://en.wikipedia.org/wiki/Encryption) of electronic data established by the U.S. [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST) in 2001.

AES is a subset of the Rijndael [block cipher](https://en.wikipedia.org/wiki/Block_cipher) developed by two [Belgian](https://en.wikipedia.org/wiki/Belgium) cryptographers, [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen) and [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen), who submitted a proposal to NIST during the [AES selection process](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process). Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the [U.S. government](https://en.wikipedia.org/wiki/Federal_government_of_the_United_States) and is now used worldwide. It supersedes the [Data Encryption Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES), which was published in 1977. The algorithm described by AES is a [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm), meaning the same key is used for both encrypting and decrypting the data. In the United States, AES was announced by the NIST as U.S. [FIPS](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard) PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see [Advanced Encryption Standard process](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process) for more details).

AES is included in the [ISO](https://en.wikipedia.org/wiki/International_Organization_for_Standardization)/[IEC](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission) [18033-3](https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_standards,_18000-19999) standard. AES became effective as a U.S. federal government standard on May 26, 2002, after approval by the U.S. [Secretary of Commerce](https://en.wikipedia.org/wiki/United_States_Secretary_of_Commerce). AES is available in many different encryption packages, and is the first (and only) publicly accessible [cipher](https://en.wikipedia.org/wiki/Cipher) approved by the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) for [top secret](https://en.wikipedia.org/wiki/Classified_information) information when used in an NSA approved cryptographic module.

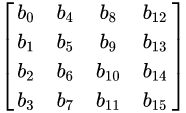
## Description of the ciphers:

AES is based on a design principle known as a [substitution–permutation network](https://en.wikipedia.org/wiki/Substitution–permutation_network), and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a [Feistel network](https://en.wikipedia.org/wiki/Feistel_network). AES is a variant of Rijndael, with a fixed [block size](https://en.wikipedia.org/wiki/Block_size_(cryptography)) of 128 [bits](https://en.wikipedia.org/wiki/Bit), and a [key size](https://en.wikipedia.org/wiki/Key_size) of 128, 192, or 256 bits. By contrast, Rijndael *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 [column-major order](https://en.wikipedia.org/wiki/Column-major_order) array of bytes, termed the *state*. Most AES calculations are done in a particular [finite field](https://en.wikipedia.org/wiki/Finite_field_arithmetic).

For instance, 16 bytes,

are represented as this two-dimensional array:



The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the [plaintext](https://en.wikipedia.org/wiki/Plaintext), into the final output, called the [ciphertext](https://en.wikipedia.org/wiki/Ciphertext). The number of rounds are as follows:

* 10 rounds for 128-bit keys.
* 12 rounds for 192-bit keys.
* 14 rounds for 256-bit keys.

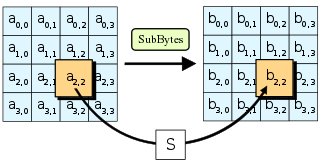
Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

### High-level description of the algorithm

1. KeyExpansion – round keys are derived from the cipher key using the [AES key schedule](https://en.wikipedia.org/wiki/AES_key_schedule). AES requires a separate 128-bit round key block for each round plus one more.
2. Initial round key addition:
   1. AddRoundKey – each byte of the state is combined with a byte of the round key using [bitwise xor](https://en.wikipedia.org/wiki/Bitwise_xor).
3. 9, 11 or 13 rounds:
   1. SubBytes – a [non-linear](https://en.wikipedia.org/wiki/Linear_map) substitution step where each byte is replaced with another according to a [lookup table](https://en.wikipedia.org/wiki/Rijndael_S-box).
   2. ShiftRows – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   3. MixColumns – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
   4. AddRoundKey
4. Final round (making 10, 12 or 14 rounds in total):
   1. SubBytes
   2. ShiftRows
   3. AddRoundKey

### The SubBytes step:

Main article: [Rijndael S-box](https://en.wikipedia.org/wiki/Rijndael_S-box)

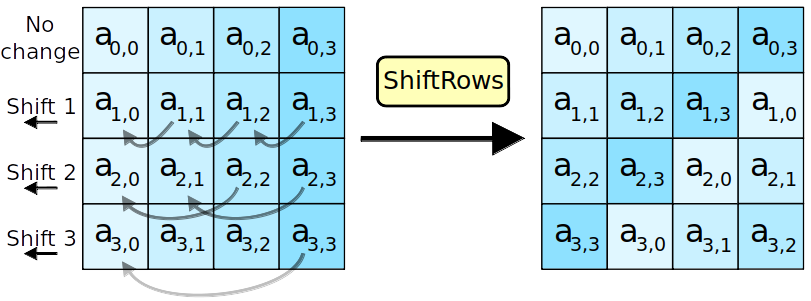
[](https://en.wikipedia.org/wiki/File:AES-SubBytes.svg)

In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, *S*; *bij* = *S(aij)*.

In the SubBytes step, each byte  in the *state* array is replaced with a SubByte using an 8-bit [substitution box](https://en.wikipedia.org/wiki/Substitution_box). This operation provides the non-linearity in the [cipher](https://en.wikipedia.org/wiki/Cipher). The S-box used is derived from the [multiplicative inverse](https://en.wikipedia.org/wiki/Multiplicative_inverse) over [GF](https://en.wikipedia.org/wiki/Finite_field)(28), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible [affine transformation](https://en.wikipedia.org/wiki/Affine_transformation). The S-box is also chosen to avoid any fixed points (and so is a [derangement](https://en.wikipedia.org/wiki/Derangement)), i.e.,  , and also any opposite fixed points, i.e.,  . While performing the decryption, the InvSubBytes step (the inverse of SubBytes) is used, which requires first taking the inverse of the affine transformation and then finding the multiplicative inverse.

### The ShiftRows step:

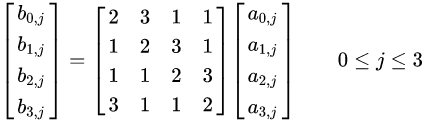
The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain [offset](https://en.wikipedia.org/wiki/Offset_(computer_science)). For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. The importance of this step is to avoid the columns being encrypted independently, in which case AES would degenerate into four independent block ciphers.



### The MixColumns step:

In the MixColumns step, the four bytes of each column of the state are combined using an invertible [linear transformation](https://en.wikipedia.org/wiki/Linear_transformation). The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides [diffusion](https://en.wikipedia.org/wiki/Diffusion_(cryptography)) in the cipher.

During this operation, each column is transformed using a fixed matrix



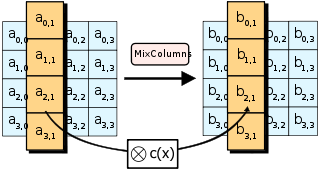
(matrix left-multiplied by column gives new value of column in the state):

Matrix multiplication is composed of multiplication and addition of the entries. Entries are bytes treated as coefficients of polynomial of order .Addition is simply XOR. Multiplication is modulo irreducible polynomial  . If processed bit by bit, then, after shifting, a conditional [XOR](https://en.wikipedia.org/wiki/Exclusive_or) with 1B16 should be performed if the shifted value is larger than FF16 (overflow must be corrected by subtraction of generating polynomial). These are special cases of the usual multiplication in  .

In more general sense, each column is treated as a polynomial over  and is then multiplied modulo with a fixed polynomial

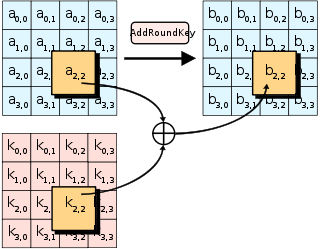
.The coefficients are displayed in their [hexadecimal](https://en.wikipedia.org/wiki/Hexadecimal) equivalent of the binary representation of bit polynomials from

. The MixColumns step can also be viewed as a multiplication by the shown particular [MDS matrix](https://en.wikipedia.org/wiki/MDS_matrix) in the [finite field](https://en.wikipedia.org/wiki/Finite_field) . This process is described further in the article [Rijndael MixColumns](https://en.wikipedia.org/wiki/Rijndael_MixColumns) .



### The AddRoundKey step:

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main [key](https://en.wikipedia.org/wiki/Key_(cryptography)) using [Rijndael's key schedule](https://en.wikipedia.org/wiki/Rijndael_key_schedule); each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise [XOR](https://en.wikipedia.org/wiki/Exclusive_or).



### Optimization of the cipher:

On systems with 32-bit or larger words, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups. This requires four 256-entry 32-bit tables (together occupying 4096 bytes). A round can then be performed with 16 table lookup operations and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the AddRoundKey step. Alternatively, the table lookup operation can be performed with a single 256-entry 32-bit table (occupying 1024 bytes) followed by circular rotation operations.

Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows, and MixColumns steps into a single round operation.

## Security:

The [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data. In June 2003, the U.S. Government announced that AES could be used to protect [classified information](https://en.wikipedia.org/wiki/Classified_information):

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

By 2006, the best known attacks were on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys.

# 2. DES(Data Encryption Standard):

The **Data Encryption Standard (DES )** is a [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) for the [encryption](https://en.wikipedia.org/wiki/Encryption) of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of [cryptography](https://en.wikipedia.org/wiki/Cryptography).

Developed in the early 1970s at [IBM](https://en.wikipedia.org/wiki/IBM) and based on an earlier design by [Horst Feistel](https://en.wikipedia.org/wiki/Horst_Feistel), the algorithm was submitted to the [National Bureau of Standards](https://en.wikipedia.org/wiki/National_Bureau_of_Standards) (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA), the NBS selected a slightly modified version (strengthened against [differential cryptanalysis](https://en.wikipedia.org/wiki/Differential_cryptanalysis), but weakened against [brute-force attacks](https://en.wikipedia.org/wiki/Brute-force_attack)), which was published as an official [Federal Information Processing Standard](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard) (FIPS) for the United States in 1977.

The publication of an NSA-approved encryption standard led to its quick international adoption and widespread academic scrutiny. Controversies arose from [classified](https://en.wikipedia.org/wiki/Classified_information) design elements, a relatively short [key length](https://en.wikipedia.org/wiki/Key_length) of the [symmetric-key](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) [block cipher](https://en.wikipedia.org/wiki/Block_cipher) design, and the involvement of the NSA, raising suspicions about a [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)). The [S-boxes](https://en.wikipedia.org/wiki/S-box) that had prompted those suspicions were designed by the NSA to remove a backdoor they secretly knew ([differential cryptanalysis](https://en.wikipedia.org/wiki/Differential_cryptanalysis)). However, the NSA also ensured that the key size was drastically reduced so that they could break the cipher by brute force attack. The intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their [cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis).

DES is insecure due to the relatively short [56-bit key size](https://en.wikipedia.org/wiki/56-bit_encryption). In January 1999, [distributed.net](https://en.wikipedia.org/wiki/Distributed.net) and the [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) collaborated to publicly break a DES key in 22 hours and 15 minutes (see [chronology](https://en.wikipedia.org/wiki/Data_Encryption_Standard" \l "Chronology)). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible in practice. The algorithm is believed to be practically secure in the form of [Triple DES](https://en.wikipedia.org/wiki/Triple_DES), although there are theoretical attacks. This cipher has been superseded by the [Advanced Encryption Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) (AES). DES has been withdrawn as a standard by the [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology).

## Description:

DES is the archetypal [block cipher](https://en.wikipedia.org/wiki/Block_cipher)—an [algorithm](https://en.wikipedia.org/wiki/Algorithm) that takes a fixed-length string of [plaintext](https://en.wikipedia.org/wiki/Plaintext) bits and transforms it through a series of complicated operations into another [ciphertext](https://en.wikipedia.org/wiki/Ciphertext) bitstring of the same length. In the case of DES, the [block size](https://en.wikipedia.org/wiki/Block_size_(cryptography)) is 64 bits. DES also uses a [key](https://en.wikipedia.org/wiki/Key_(cryptography)) to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking [parity](https://en.wikipedia.org/wiki/Parity_bit), and are thereafter discarded. Hence the effective [key length](https://en.wikipedia.org/wiki/Key_length) is 56 bits.

The key is nominally stored or transmitted as 8 [bytes](https://en.wikipedia.org/wiki/Byte), each with odd parity. According to ANSI X3.92-1981 (Now, known as ANSI [INCITS](https://en.wikipedia.org/wiki/INCITS) 92-1981), section 3.5:

One bit in each 8-bit byte of the *KEY* may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16,..., 64 are for use in ensuring that each byte is of odd parity.

Like other block ciphers, DES by itself is not a secure means of encryption, but must instead be used in a [mode of operation](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation). FIPS-81 specifies several modes for use with DES. Further comments on the usage of DES are contained in FIPS-74.

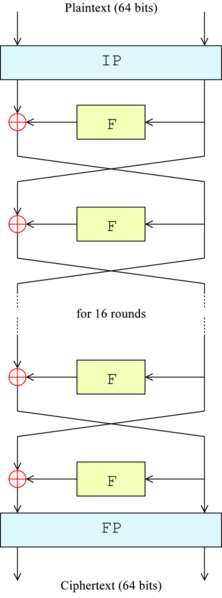
Decryption uses the same structure as encryption, but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions.)

**Overall structure:**

The algorithm's overall structure is shown in Figure 1: there are 16 identical stages of processing, termed *rounds*. There is also an initial and final [permutation](https://en.wikipedia.org/wiki/Permutation), termed *IP* and *FP*, which are [inverses](https://en.wikipedia.org/wiki/Inverse_function) (IP "undoes" the action of FP, and vice versa). IP and FP have no cryptographic significance, but were included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware.

Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the [Feistel scheme](https://en.wikipedia.org/wiki/Feistel_scheme). The Feistel structure ensures that decryption and encryption are very similar processes—the only difference is that the subkeys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

The ⊕ symbol denotes the [exclusive-OR](https://en.wikipedia.org/wiki/XOR) (XOR) operation. The *F-function* scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.



The overall Feistel structure of DES

**3.MD5(message-digest algorithm)**:

The **MD5 message-digest algorithm** is a widely used [hash function](https://en.wikipedia.org/wiki/Hash_function) producing a 128-[bit](https://en.wikipedia.org/wiki/Bit) hash value. Although MD5 was initially designed to be used as a [cryptographic hash function](https://en.wikipedia.org/wiki/Cryptographic_hash_function), it has been found to suffer from extensive vulnerabilities. It can still be used as a [checksum](https://en.wikipedia.org/wiki/Checksum) to verify [data integrity](https://en.wikipedia.org/wiki/Data_integrity), but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

MD5 was designed by [Ronald Rivest](https://en.wikipedia.org/wiki/Ronald_Rivest) in 1991 to replace an earlier hash function [MD4](https://en.wikipedia.org/wiki/MD4), and was specified in 1992 as [RFC 1321](https://tools.ietf.org/html/rfc1321).

One basic requirement of any cryptographic hash function is that it should be [computationally infeasible](https://en.wikipedia.org/wiki/Computational_complexity_theory" \l "Intractability) to find two distinct messages that hash to the same value. MD5 fails this requirement catastrophically; such [collisions](https://en.wikipedia.org/wiki/Collision_resistance) can be found in seconds on an ordinary home computer.

The weaknesses of MD5 have been exploited in the field, most infamously by the [Flame malware](https://en.wikipedia.org/wiki/Flame_malware) in 2012. The [CMU Software Engineering Institute](https://en.wikipedia.org/wiki/CMU_Software_Engineering_Institute) considers MD5 essentially "cryptographically broken and unsuitable for further use".

As of 2019, MD5 continues to be widely used, in spite of its well-documented weaknesses and deprecation by security experts.

MD5 is one in a series of [message digest](https://en.wikipedia.org/wiki/Message_digest) algorithms designed by Professor [Ronald Rivest](https://en.wikipedia.org/wiki/Ronald_Rivest) of [MIT](https://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology) (Rivest, 1992). When analytic work indicated that MD5's predecessor [MD4](https://en.wikipedia.org/wiki/MD4) was likely to be insecure, Rivest designed MD5 in 1991 as a secure replacement. ([Hans Dobbertin](https://en.wikipedia.org/wiki/Hans_Dobbertin) did indeed later find weaknesses in MD4.)

## MD5 hashes:

The 128-bit (16-byte) MD5 hashes (also termed *message digests*) are typically represented as a sequence of 32 [hexadecimal](https://en.wikipedia.org/wiki/Hexadecimal) digits. The following demonstrates a 43-byte [ASCII](https://en.wikipedia.org/wiki/ASCII) input and the corresponding MD5 hash:

MD5("[The quick brown fox jumps over the lazy dog](https://en.wikipedia.org/wiki/The_quick_brown_fox_jumps_over_the_lazy_dog)") =

9e107d9d372bb6826bd81d3542a419d6

Even a small change in the message will (with overwhelming probability) result in a mostly different hash, due to the [avalanche effect](https://en.wikipedia.org/wiki/Avalanche_effect). For example, adding a period to the end of the sentence:

MD5("[The quick brown fox jumps over the lazy dog](https://en.wikipedia.org/wiki/The_quick_brown_fox_jumps_over_the_lazy_dog)**.**") =

e4d909c290d0fb1ca068ffaddf22cbd0

The hash of the zero-length string is:

MD5("") =

d41d8cd98f00b204e9800998ecf8427e

The MD5 algorithm is specified for messages consisting of any number of bits; it is not limited to multiples of eight bits ([octets](https://en.wikipedia.org/wiki/Octet_(computing)), [bytes](https://en.wikipedia.org/wiki/Byte)). Some MD5 implementations such as [md5sum](https://en.wikipedia.org/wiki/Md5sum) might be limited to octets, or they might not support *streaming* for messages of an initially undetermined length.

**SPECIAL FEATURES:**

1. User interface for login and signup.

**SYSTEM REQUIREMENTS:**

**METHODOLOGY:**

1. User(sender) inputs the message.

2. Using AES algorithm(symmetric) to encrypt the message using 128 bits key.

3. Trasmmit the data to the receiver.

4. Decrypt the encrypted message at the receiver’s end using the same key.

**REFERENCES:**

1.<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

2.<https://en.wikipedia.org/wiki/Data_Encryption_Standard>

3. <https://en.wikipedia.org/wiki/MD5>

**TEAM DETAILS :**

1. Chiraag Singh Dhapola - 180111024 - CSF

2. Harshit Nayal - 180111045 – CSF

3. Ashutosh Gautam- 180111039 – CSF

4. Ritik Mamgai – 180111046- CSF

**GUIDE DETAILS:**