AES Encryption Technique:-

The word AES signifies Advanced Encryption Standard. It is an encryption and decryption technique. The AES came after the DES (Data Encryption Standard). It is a powerful successor which overcomes almost every muddle and mess of DES. The AES is also k/as Rijndael. It was designed by Vincent Rijmen & Joan Daemon in 1998. And it was approved by NIST(*National Institute of Standards and Technology*) in 2001 as AES. The AES is an *symmetric key block cipher* – same key is used for encryption and decryption. It is a encryption technique where *plain text* is of 128 bit and an 128 bit *key* is applied over it and finally we get out 128 bit *cipher text*. The method takes an 128 bit *information*(data) as an input and applies an algorithm that converts that 128 bit input into a unreadable or un-meaningful information. This method have three basic defined types and the first one is as the 128 bit key will be used for 10 number of rounds , second one says that 192 bit key will be used for 12 number of rounds and similarly the third one says that 256 bit key will be used for 14 number of rounds of encryption. And for encryption every round contains , firstly Pre-Round Transformation then round phases. In a Pre-Round Transformation the 128 bit information is converted in 16 bit small blocks with the help of an 128 bit key. Then after in the round phase the info is processed as firstly the Sub-Bytes process takes place where the 16 bit blocks are arranged in a 4X4 matrix , after the Shift-Rows method is applied where the rows are left shifted as shifting information will be shifted by one next position i.e. the 1^{st} row will be shifted zero times and 2^{nd} row will be shifted one time similarly the 3^{rd} row will be shifted two times and the 4^{th} row will be shifted three times, the third stage contains Mix-Columns where the columns will be redistributed by an special mathematics function i.e. a series of mathematical operations that is designed for that particular encryption , lastly the Add-Round-Key is performed where key is *XORED*(re-aligned),then goes for next round processing and if the round is final round then it is the *cipher text*. And for the decryption , It also haves 4 rounds , firstly the Sub-Bytes process takes place where the cipher text is divided into 4X4 matrix such that it contains a block of 16 bit information , afterwards the Shift-Rows operation is performed where the rows of matrix are right shifted in such a way that 1^{st} row will be shift zero times , 2^{nd} row will be shifted one times , 3^{rd} row is shifted two times , similarly 4^{th} row will be shifted three times , afterwards the Mix-Columns process takes place where the matrix is redistributed by an special mathematics function which is designed for the decryption , the last process is Add-round-key where the key is *XORED* , then the information goes to the next round and if that round is final round then it is the decrypted plain text. Since the AES encryption is an symmetric block cipher algorithm the special math function for rearranging i.e. mixing columns of encryption and the special mathematics function for rearranging i.e. mixing columns of decryption will be opposite or vice-versa of each other. While talking about the advantages of AES encryption technique , it is the most robust security protocol , it is open source and used world wide , for 128 bit one must attempt 2^{128} times to break the encryption that's why it is an very safe protocol but it is very complex to be implemented. If we talk about the attacks which are able to break the AES algorithm i.e. that the attacks which are used to crack the AES algorithm are firstly the quantum computing or the traditional computing having advance speedup powers, secondly any new generated algorithm that was unknown at that time when AES was generated that is having a very huge amount of factorizing power. But as the conclusion AES is a very powerful and efficient encryption technique.

~Ritik Patle(0533CS171056)