Advanced Encryption Standard (AES) is an encryption standard that surpassed DES in terms of usefulness and safety. It was established by the U.S Institute of Standards and Technology in 2001. It is a symmetric key block cypher that is about 6 times as fast as triple DES. AES is very standard in regular day encryption that would take billions of years to crack using a brute force attack, making it an incredibly secure option for encryption.

As computation power increased, DES was being seen more and more as a vulnerability to an exhaustive key search. This is partially since DES was coined back in the 70’s when computational power was much weaker than when AES was made in 2001. In June of 2003 the U.S government declared that AES could protect classified information causing it to become an instant standard for encryption. The selection process for AES was between 15 different algorithms. AES chose and algorithm made by two Belgian cryptographers, Joan Daemen and Vincent Rijndael.

AES works by having its data broken into chunks of 128-bits and by using keys of either 128, 192, or 256-bits. Since it is a symmetric based encryption system, both the sender and the receiver needs to know what the secret key is. All of the lengths are secure, but 192-bit keys and 256-bit keys are used for top secret information. The inputted 128-bit chunk is broken up into 16-bytes and put into a 4x4 matrix. Depending on what key size is used, the amount of rounds run through the algorithm changes. 128 bit keys use 10 rounds, 192-bit keys use 12 rounds, and 256-bit keys use 14 rounds. Each key is just a randomly generated string is just a random bit string. Like DES, a round does substitution and transposition to create the ciphertext. Each round consists of 4 sub-processes. These processes in each round are SubBytes, ShiftRows, MixColumns, and AddRoundKey.

The SubBytes section is where the 16 inputted bytes (128-bits) are substituted by looking at an included table and replacing the each inputted byte with a corresponding lookup byte. This creates a new 4x4 matrix which is far different than the original 16-bytes that were placed into the original matrix.

The ShiftRows section is where each row in the matrix is shifted left according to the algorithm. The first row remains unchanged, the second row shifts once to the left, the third shifts twice, and the forth row shifts three times to the left. Any entries that would be shifted off of the matrix are reinserted on the right side of the matrix so it remains a 4x4 matrix.

The MixColumn section is where each 4 byte column is transformed using an invertible mathematical function. The function takes each 4 byte column and changes it to 4 completely new bytes and replaces the old 4 bytes with the new 4 bytes. This results in a completely new matrix and along with the previous 2 steps causes enough diffusion. This process is not used in the last round however.

Finally, the last sub-process is AddRoundKey. A 128-bit round key is generated using the original secret key and is used each round to XOR with the 16-byte matrix. Therefore, the 16-byte matrix is treated as 128-bits and is XORed with the round key to give another brand new 128-bit result. If it is the last round, the resulting 128-bit string is the ciphertext. If it is not, the 128-bit result is made into 16 bytes again and the next round begins.

To decrypt, all of the sub-processes are simply done in reverse. However, the decryption algorithm must be implemented separately from the encryption algorithm.

AES is very secure and it has only been successfully attacked through side-channel attacks. Side-channel attacks don’t directly attack the cipher, but attack vulnerabilities of the systems or hardware that use the algorithm. For example, the exploit against TLS v1.0 protocol. TLS uses AES but TLS displays certain information allowing for attackers to predict the initialization vector. There is also many papers published on attacks on AES on lower rounds, but none successful on the standard rounds. A 2011 paper was published that outlined a biclique attack that is faster than a brute force attack. It is still not fast or powerful enough to crack AES in any amount of reasonable time.

AES is a powerful encryption cipher that is the only one publicly approved by the NSA for top level security encryption. It still has yet to have an efficient crack meaning that information is guaranteed to be secure for the time being. It has far superseded previous algorithms such as DES and 3-DES which have been found to be far weaker than AES.

*Advanced Encryption Standard*. TechTarget.com. <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

*Advanced Encryption Standard*. TutorialsPoint.

<https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm>

*How Secure is AES Against Brute Force Attacks?.* EE|Times.

<http://www.eetimes.com/document.asp?doc_id=1279619>