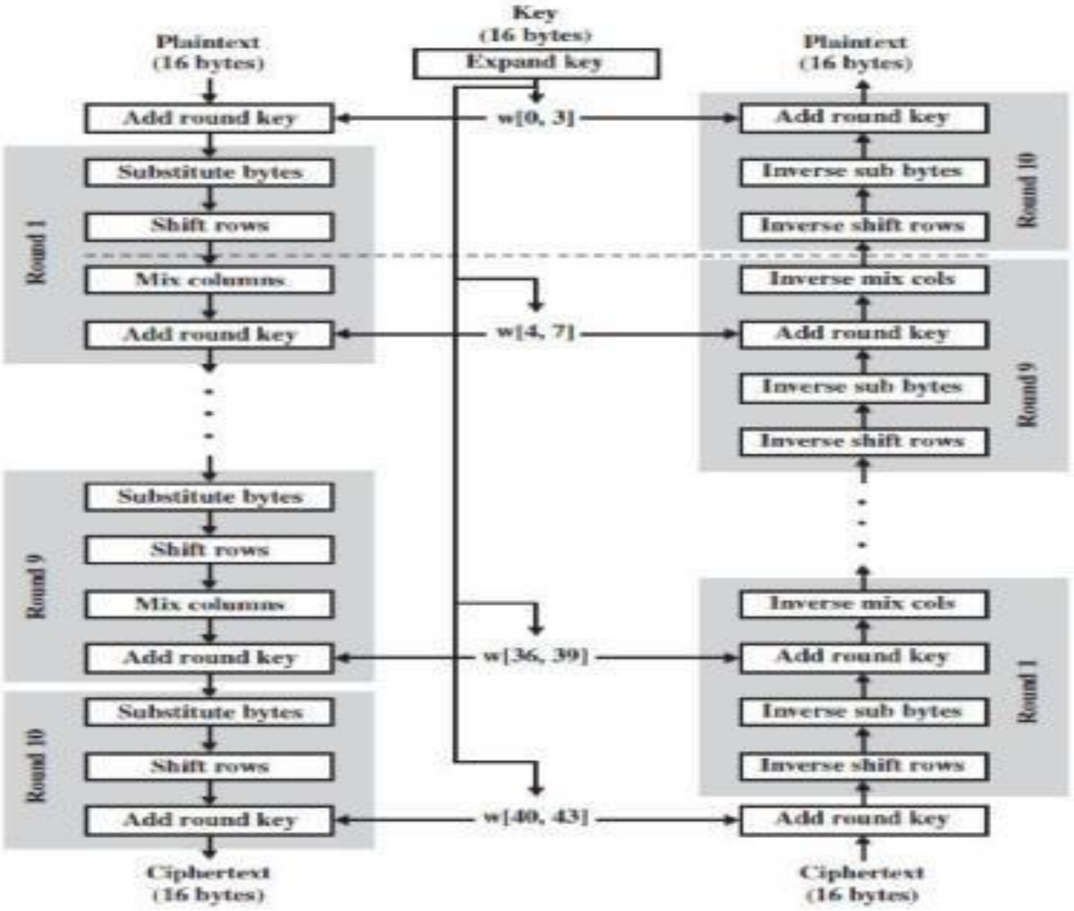
SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Advanced Data Encryption Standard (AES)

- The principal drawback of 3DES is that the algorithm is relatively slow in software.
- The original DEA was designed for mid-1970s hardware implementation and does not produce efficient software code.
- 3DES, which has three times as many rounds as DEA, is correspondingly slower.
- A secondary drawback is that both DEA and 3DES use a 64-bit block size.
- For reasons of both efficiency and security, a larger block size is desirable.
- As a replacement, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have a security strength equal to or better than 3DES and significantly improved efficiency.
- In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits.
- Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.
- The two researchers who developed AES are both cryptographers from Belgium:

  Dr. JoanDaemen and Dr.Vincent Rijmen.



(a) Encryption (b) Decryption

Figure 2.5 AES Encryption and Decryption

The following comments give some insight into AES.

One noteworthy feature of this structure is that it is not a Feistel structure, but processes the entire data block in parallel during each roundusing substitutions and permutation.

The key that is provided as input is expanded into an array of forty- four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round.

Four different stages are used, one of permutation and three of substitution:

substitution of the block.

- **Shift rows:**A simple permutation that is performed row by row.
- **Mix columns:**A substitution that alters each byte in a column as afunction of all of the bytes in the column.

Add round key:A simple bitwise XOR of the current block with a portion ofthe expanded key.

The structure is quite simple. For both encryption and decryption, the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.

Only the **Add Round Key** stage makes use of the key. For this reason, the cipherbegins and ends with an Add Round Key stage.

The Add Round Key stage by itself would not be tough. The other three stages together scramble the bits, but by themselves, they would provide no security because they do not use the key.

Each stage is easily reversible. For the Substitute Byte, Shift Row, and Mix Columns stages, an inverse function is used in the decryption algorithm.

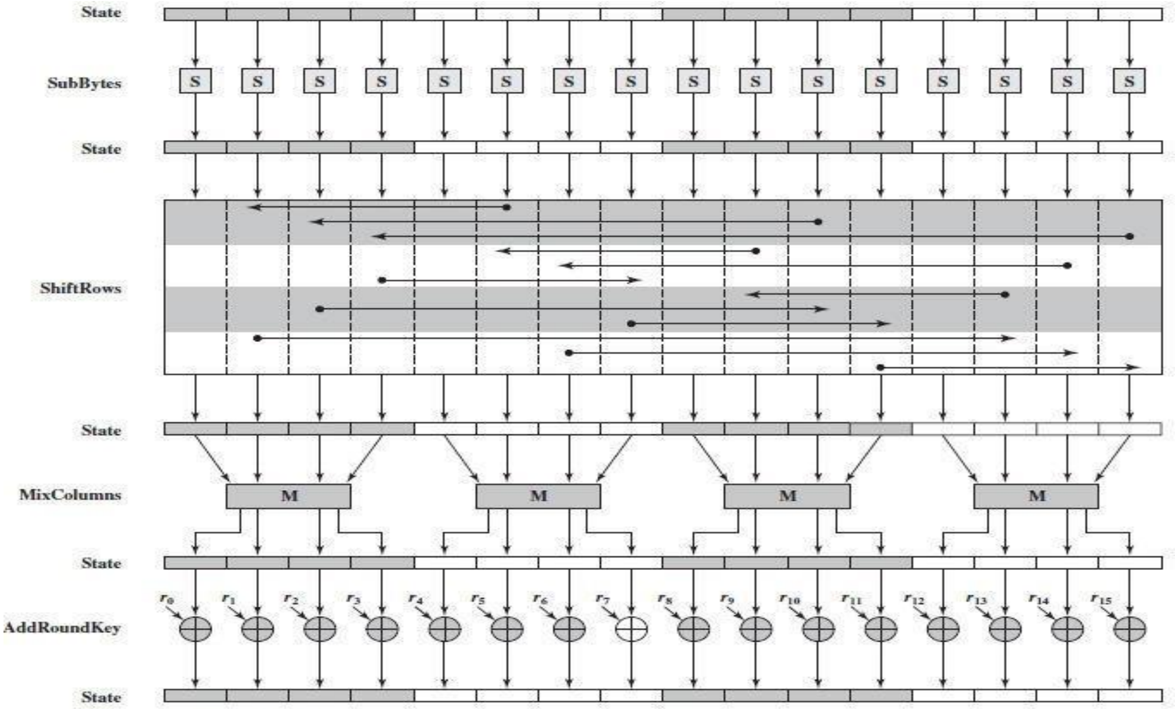


Figure 2.6 AES Encryption Round