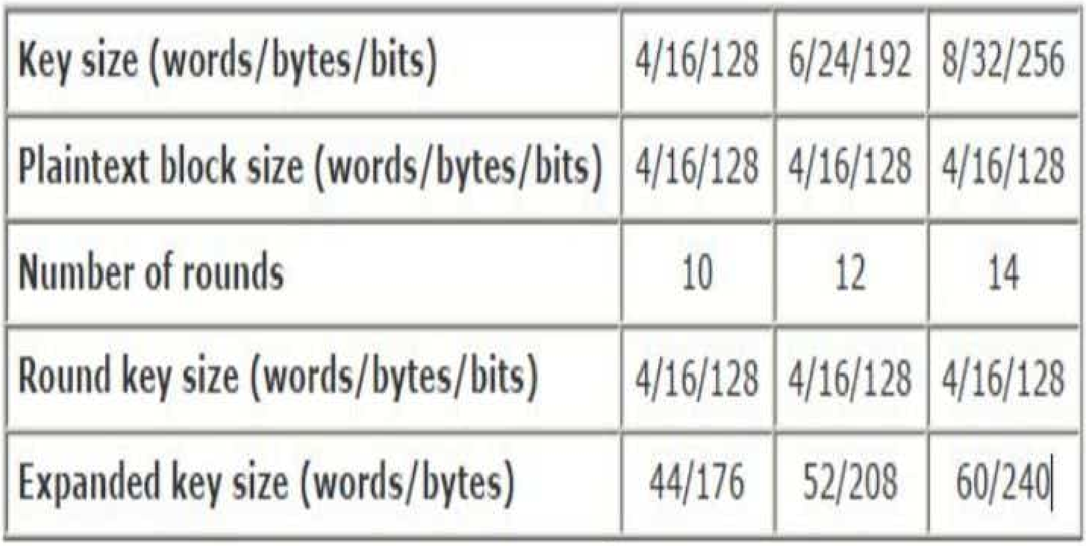
Advanced Encryption Standard

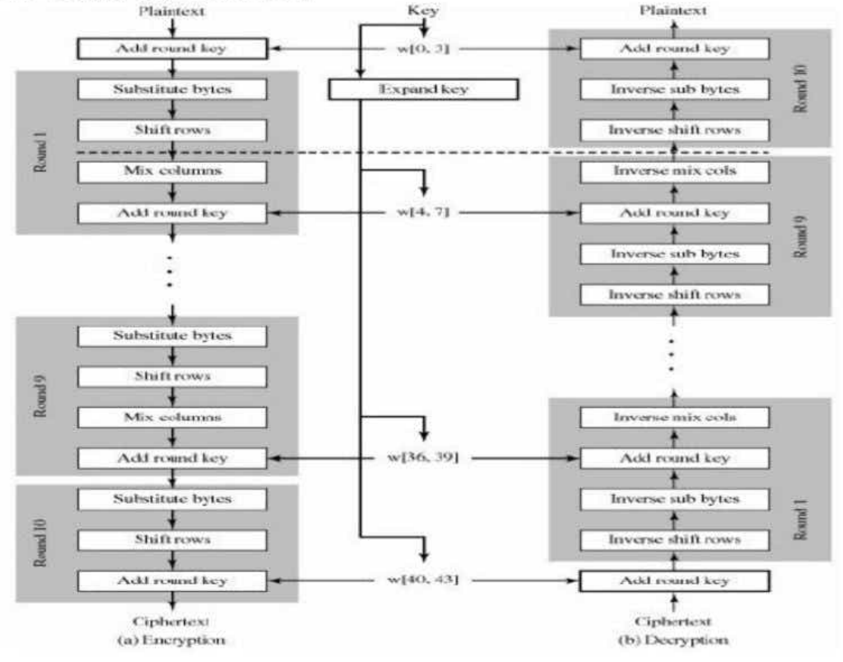
- The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192, or 256 bits
- The AES specification uses the same three key size alternatives but limits the block length to 128 bits
- A number of AES parameters depend on the key length (Table)
- Assume a key length of **128 bits**, which is likely to be the one most commonly implemented

Table. AES Parameters



Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

AES Data Structures



Overall AES structure

- AES structure is not a **Feistel structure.**
- Two of the AES finalists, including Rijndael, do not use a
- Feistel structure but process the entire data block in parallel during each round using
- substitutions and permutation.

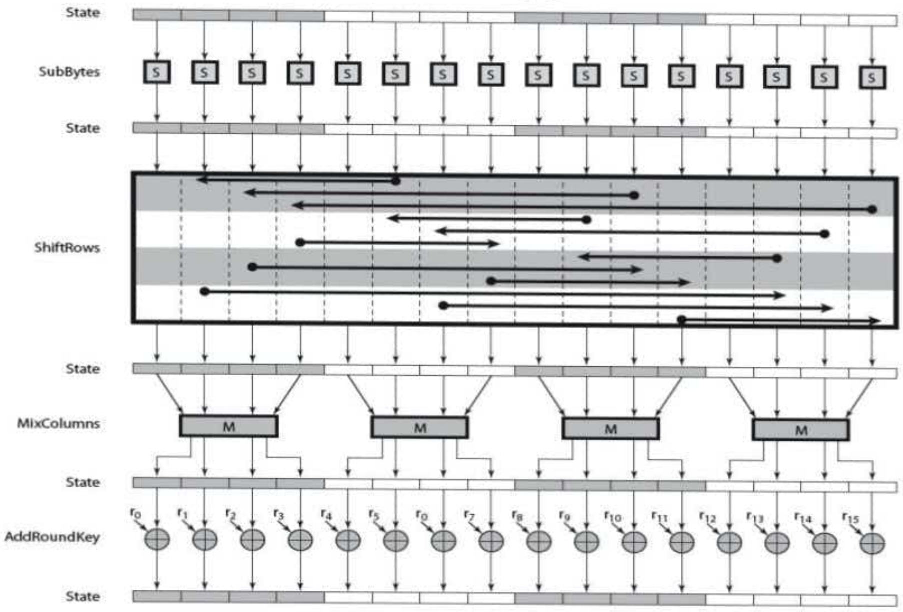
Four different stages are used, one of permutation and three of substitution:

- **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
- **ShiftRows:** A simple permutation
- **MixColumns:** A substitution that makes use of arithmetic over GF(2^8)
- **AddRoundKey:** A simple bitwise XOR of the current block with a portion of the expanded key

For both encryption and decryption, the cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages

- The Figure shows the overall structure of AES. The input to the encryption and decryption algorithms is a single 128-bit block. In FIPS PUB 197, this block is depicted as a square matrix of bytes.
- This block is copied into the **State array, which is modified at each stage of encryption or decryption.**
- **After the final** stage, **State is copied to an output matrix.**
- **These operations are depicted in Figure a. Similarly, the** 128-bit key is depicted as a square matrix of bytes.
- This key is then expanded into an array of key schedule words; each word is four bytes and the total key schedule is 44 words for the 128-bit key (Figure 5.2b). Note that the ordering of bytes within a matrix is by column.
- So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the **in matrix,** the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the **w matrix.**

AES Encryption Round



- Only the AddRoundKey stage makes use of the key
- For this reason, the cipher begins and ends with an AddRoundKey stage
- Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security
- The AddRoundKey stage is, in effect, a form of Vernam cipher and by itself would not be formidable
- The other three stages together provide confusion, diffusion, and nonlinearity, but by themselves would provide no security because they do not use the key
- We can view the cipher as alternating operations of XOR encryption (AddRoundKey) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on
- This scheme is both efficient and highly secure, each stage is easily reversible

- For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm
- For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block, using the result that $A \oplus A \oplus B = B.$
- As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order
- However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular structure of AES
- Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. Figure lays out encryption and decryption going in opposite vertical directions
- At each horizontal point (e.g., the dashed line in the figure), **State is the same for** both encryption and decryption
- The **final round of both encryption and decryption** consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible