For the following AES questions give a brief high level description. Your answers should not be more than 5 lines.

1) What is the purpose of state array?
Ans:
The State array holds the intermediate results on the 128-bit block at each stage in the processing.

2) Briefly describe ShiftRows?
Ans:
The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed.

3) How many bytes are altered in shift rows?
Ans:
12 bytes

4) Briefly describe MixColumns?
Ans:
MixColumns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

5) Briefly describe AddRound key
Ans:
The 128 bits of State are bitwise XORed with the 128 bits of the round key.

6) What is the difference between Rijndael and AES?
Ans:
Rijndael allows for block lengths of 128, 192, or 256 bits. AES allows only a block length of 128 bits.