1. **AddRound Key**
   - Input (state và key expansion dưới dạng mã hex):
   - State: 32 88 31 E0 43 5A 31 37 F6 30 98 07 A8 8D A2 34
   - Key Expansion: 2B 28 AB 09 7E AE F7 CF 15 D2 15 4F 16 A6 88 3C
   - ➔ Output (kết quả của phép XOR 128 bit giữa state và key expansion dưới dạng mã hex):
   - ➔ Output: 19 A0 9A E9 3D F4 C6 F8 E3 E2 8D 48 BE 2B 2A 08
2. **SubBytes**
   - Thay thế mỗi byte state bằng 1 byte trong bảng S-box
     EA 04 65 85 83 45 5D 96 5C 33 98 B0 FO 2D AD C5
   - ➔ 87 F2 4D 97 EC 6E 4C 90 4A C3 46 E7 8C D8 95 A6
3. **ShiftRows**
   - Hàng đầu không thay đổi
   - Hàng 2 dịch vòng trái 1 byte
   - Hàng 3 dịch vòng trái 2 byte
   - Hàng 4 dịch vòng trái 3 byte

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

➔

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

4. **MixColumns**

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

X

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

=

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC