Ví dụ:

K = A2E7F3E9F4EC8BB93217B94C5FD982CD

Chia các word, chia K làm 4 word, mỗi word 4 byte

w0= A2E7F3E9

w1= F4EC8BB9

w2= 3217B94C

w3= 5FD982CD

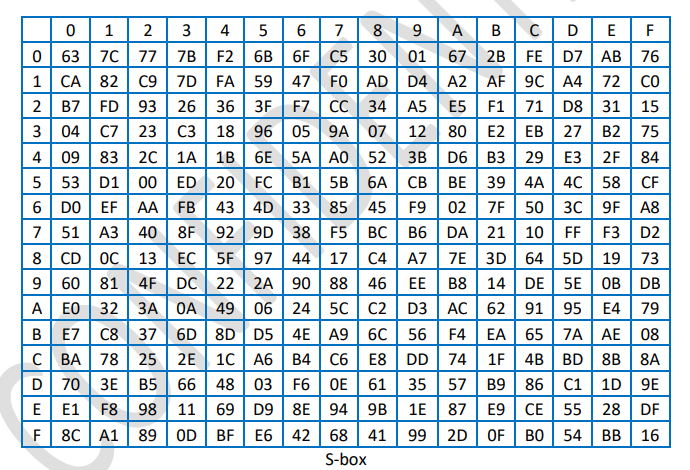
**2. Trong hệ mật mã AES, xét sơ đồ sinh khóa con, tại vòng lặp thứ 1, biết khóa input K0. Hãy cho biết thực hiện các bước tính cần thiết và cho biết khóa con tiếp theo được sinh ra là gì? Cụ thể cho biết:**

**1) Kết quả dịch vòng trái với word cuối, kí hiệu r**

r = RotWord(w3) = D982CD5F

**2) Kết quả phép thế S-box đối với r, kí hiệu s**

Thay thế từng byte trong r bằng bảng Sbox Subword



s= subword(r) = 3513BDCF

**3) Kết quả phép XOR với Rcon[i], kí hiệu xrc**

xrc= XOR (Rcon [1], s)

Rcon [1] = (RC [1], 0, 0, 0) = (01, 0, 0, 0)

Rcon [1] = 01000000

Xor S= 3513BDCF

xrc = 3413BDCF

**4) Tính khóa tiếp theo, kí hiệu Ki**

K1 = (w4, w5, w6, w7)

w4 = XOR (xrc, w0)

w5 = XOR (w4, w1)

w6 = XOR (w5, w2)

w7 = XOR (w6, w3)

**3. Trong hệ mật mã AES, xét thuật toán mã hóa, tại vòng lặp thứ 1, biết giá trị input là state(128 bit), state = 9BA7F9DA2F6AFCA6659999C5C7143569. Hãy cho biết kết quả sau khi thực hiện các phép SubByte, ShiftRows, và MixColumns? Cụ thể cho biết**

|  |  |  |  |
| --- | --- | --- | --- |
| 9B | 2F | 65 | C7 |
| A7 | 6A | 99 | 14 |
| F9 | FC | 99 | 35 |
| DA | A6 | C5 | 69 |

**1) Kết quả thay thế từng byte trong state bằng bảng S-box, kí hiệu**

**state = SubByte(state) =**

|  |  |  |  |
| --- | --- | --- | --- |
| 14 | 15 | 4D | C6 |
| 5C | 02 | EE | FA |
| 99 | B0 | EE | 80 |
| 57 | 24 | A6 | F9 |

**2) Kết quả dịch vòng trái, ký hiệu state = ShiftRows(state)**

|  |  |  |  |
| --- | --- | --- | --- |
| 14 | 15 | 4D | C6 |
| 02 | EE | FA | 5C |
| EE | 80 | 99 | B0 |
| F9 | 57 | 24 | A6 |

**3) Thực hiện phép MixColumns, ký hiệu state = MixColumns(state), hãy cho biết giá trị byte thứ 50 của state , biết giá trị được tính bắt đầu từ chỉ số 0 và tính từ trái sang phải**

MixColumn: 