BÀI TẬP NHÓM 1
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 18DC9095F9149EDB7323F20E4E462D92 là input bài 6
K = CFD61D489E7C48BC46C9F875C1F04E1B là input bài 1, 6
output C = CFC0A43275DE34CBA24990C7D827D8B7

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = CFD61D489E7C48BC46C9F875C1F04E1B,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 18DC9095F9149EDB7323F20E4E462D92,
   K (input) = CFD61D489E7C48BC46C9F875C1F04E1B
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 2
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = B104AADD3AC293DF787EFD2CF8065925 là input bài 6
K = C281B1763B140EF7AB12EB2745F1F59F là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = C281B1763B140EF7AB12EB2745F1F59F,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = B104AADD3AC293DF787EFD2CF8065925,
   K (input) = C281B1763B140EF7AB12EB2745F1F59F
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 3
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 4AEB5D62EC3B55DBF5D5A87708E2FF1E là input bài 6
K = 6704C20E086B3F537AE5721F486DC559 là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = 6704C20E086B3F537AE5721F486DC559,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 4AEB5D62EC3B55DBF5D5A87708E2FF1E,
   K (input) = 6704C20E086B3F537AE5721F486DC559
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 4
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = AB5BFF34115C963B835CAF027EBE0B53 là input bài 6
K = CDAB0FC51CACBCF9A8A348C3D2D0247A là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = CDAB0FC51CACBCF9A8A348C3D2D0247A,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = AB5BFF34115C963B835CAF027EBE0B53,
   K (input) = CDAB0FC51CACBCF9A8A348C3D2D0247A
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 5
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 7BB88955B6E87E91095C2A880F983F46 là input bài 6
K = 021D3D04A490B5A4C91A4F85112A5B55 là input bài 1, 6
output C = 96829D7366AEECFD2E72BBAD37DFE5F0

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = 021D3D04A490B5A4C91A4F85112A5B55,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 7BB88955B6E87E91095C2A880F983F46,
   K (input) = 021D3D04A490B5A4C91A4F85112A5B55
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state Mix Columns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 6
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 58A89BB7073DAA060FF436751C46674C là input bài 6
K = 344E74129CD8D1D127FC62A01EF147B7 là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = 344E74129CD8D1D127FC62A01EF147B7,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 58A89BB7073DAA060FF436751C46674C,
   K (input) = 344E74129CD8D1D127FC62A01EF147B7
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 7
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = BC3034B5D3677672E290C28DC16922FB là input bài 6
K = AADE12F39F579A5A49845A7797FE9146 là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = AADE12F39F579A5A49845A7797FE9146,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = BC3034B5D3677672E290C28DC16922FB,
   K (input) = AADE12F39F579A5A49845A7797FE9146
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 8
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 5D4D42B8363CF3A3B9ADDBB21FABB5AE là input bài 6
K = FEE7CE5F5EA2FB126868CDCD3CFAE8DB là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = FEE7CE5F5EA2FB126868CDCD3CFAE8DB,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 5D4D42B8363CF3A3B9ADDBB21FABB5AE,
   K (input) = FEE7CE5F5EA2FB126868CDCD3CFAE8DB
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 9
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = 39400A33DB86771F578E208998CDB8A4 là input bài 6
K = A2E7F3E9F4EC8BB93217B94C5FD982CD là input bài 1, 6
output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = A2E7F3E9F4EC8BB93217B94C5FD982CD,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = 39400A33DB86771F578E208998CDB8A4,
   K (input) = A2E7F3E9F4EC8BB93217B94C5FD982CD
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**

BÀI TẬP NHÓM 10
NỘI DUNG MÃ HÓA BÀI TẬP AES-128
THAM KHẢO NỘI DUNG THỰC HÀNH

Input M = C53DC29057B08FDC5B72FFA0111A7F2A là input bài 6
K = 2C501FC7D58E1D56EFFB2FF87D497189 là input bài 1, 6
output C = 2B2187E46DCE23B83C603FADBB6A2B50

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. **Chia khóa K (128 bit) thành 4 word (32 bit)**
   Input: K (input) = 2C501FC7D58E1D56EFFB2FF87D497189,
   Output: w_0 = , w_1 = , w_2 = , w_3 = ,

2. **Dịch vòng trái 1 byte đối với w_3 (32 bit)**
   Input: w_3 (kết quả bài 1) =
   Output: rw = RotWord(w_3) =

3. **Thay thế từng byte trong rw bằng bảng S-box** SubWord
   Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: sw = SubWord(rw) =

4. **sw XORbit với Rcon[j]**
   Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)
   Output: xcsw = XorRcon(sw, RC[i]) =

5. **Tính khóa K1 = (**w_4, w_5, w_6, w_7)
   Input: xcsw (kết quả bài 4) = ; w_0, w_1, w_2, w_3 (kết quả bài 1);
   Output: w_4 = **XORbit(**xcsw, w_0**) =**
   w_5 = **XORbit(**w_4, w_1**)** =
   w_6 = **XORbit(**w_5, w_2**)** =
   w_7 = **XORbit(**w_6, w_3**) =**

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. **Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)**
   Input: M (input) = C53DC29057B08FDC5B72FFA0111A7F2A,
   K (input) = 2C501FC7D58E1D56EFFB2FF87D497189
   Output: state = **AddRoundKey(M, K)**
   ========== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ==========
7. **Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)**
   Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,
   Sbox (tài liệu mục 5.3, Table 5.2, trang 157)
   Output: state = **SubByte (state)**

8. **Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)**
   Input: state (kết quả bài 7) = ,
   Output: state = **ShiftRows (state)**

9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)**
   Input: state (kết quả bài 8) = ,
   Output: state = **MixColumns (state)**

10. **Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 9) = ,
    Ki (kết quả bài 5) =
    Output: state = **AddRoundKey (state, Ki)**
    ========== VÒNG LẶP THỨ 10 ==========
11. **Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)**
    Input: state (kết quả bài 10) = ,
    K10 (kết quả bài 5) =
    Output: C = state = **AddRoundKey (ShiftRows(SubByte (state)), Ki)**