**1) Tổng quan AES-128**

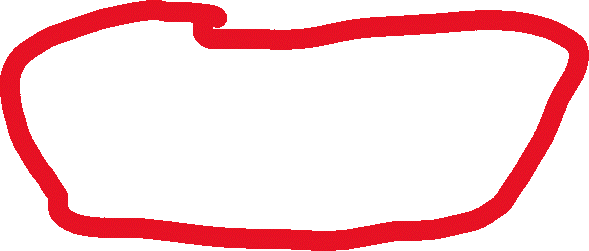
Các vấn đề liên quan đến chuẩn mã hóa AES được mô tả trong tài liệu "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", công bố ngày 26/11/2001, của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST). Mục này chỉ trình bày ngắn gọn về mã hóa AES 128 bit, gọi tắt là AES-128 theo hướng dễ thực hiện bằng mạch số.

Mã hóa AES được thực hiện thông qua 5 chức năng chính là AddRoundKey, SubBytes, ShiftRows, MixColumns và KeyExpansion. Năm chức năng này được sắp xếp để thực hiện ba bước cơ bản.

* Bước 1. Bước khởi tạo: dữ liệu cần được mã hóa plain\_text[127:0] kết hợp với key[127:0] bằng chức năng AddRoundKey
* Bước 2. Bước lặp mã hóa: kết quả bước 1 được sử dụng để thực hiện tuần tự các chức năng SubBytes, ShiftRows, MixColumns và AddRoundKey. Bước này được lặp lại 9 lần. Chú ý, KeyExpansion thực hiện song song với bước AddRoundKey để tạo khóa vòng cho chức năng này.
* Bước 3. Bước tạo ngõ ra: Sau 9 lần lặp ở bước 2, kết quả được sử dụng để thực hiện tuần tự các chức năng SubBytes, ShiftRows và AddRoundKey để tạo ngõ ra cipher\_text[127:0].

|  |
| --- |
| [https://1.bp.blogspot.com/-tfXma_t6SL4/XY9qWVx5tqI/AAAAAAAAJ90/kfAXnRta7ogQeXc9rX-JkA2b3E-f-9hCQCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-tfXma_t6SL4/XY9qWVx5tqI/AAAAAAAAJ90/kfAXnRta7ogQeXc9rX-JkA2b3E-f-9hCQCKgBGAsYHg/s1600/image.png) |
| Hình 1: Quá trình mã hóa AES-128 |

Quá trình mã hóa AES-128 sẽ được giải thích trên một ví dụ cụ thể. Giả sử chuỗi dữ liệu cần mã hóa plain\_text[127:0] và khóa mã key[127:0] có giá trị như sau:



* plain\_text[127:0] = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
* key[127:0] = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

Dữ liệu và khóa mã được sắp xếp dưới dạng ma trận với mỗi phần tử là một byte.

|  |
| --- |
| [https://1.bp.blogspot.com/-drYPbl5B91c/XY9rKCHAYeI/AAAAAAAAJ98/55YIAx6JvzsyTbSRkqk3Vx9bGNXoNsQ0gCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-drYPbl5B91c/XY9rKCHAYeI/AAAAAAAAJ98/55YIAx6JvzsyTbSRkqk3Vx9bGNXoNsQ0gCKgBGAsYHg/s1600/image.png) |
| Hình 2: Dữ liệu và khóa mã được sắp xếp dưới dạng ma trận |

Trong quá trình mã hóa, ma trận dữ liệu ban đầu sẽ bị biến đổi bởi các chức năng AddRoundKey, SubBytes, ShiftRows hoặc MixColumns để tạo ra các dữ liệu trung gian gọi là ma trận trạng thái. Ma trận khóa mã sẽ bị biến đổi bởi chức năng KeyExpansion để tạo ra các khóa mã trung gian gọi là khóa vòng.  
**2)Chức năng AddRoundKey**Chức năng AddRoundKey thực hiện ở:

1. Bước khởi tạo: XOR khóa mã với ma trận dữ liệu
2. Bước lặp mã hóa và bước tạo ngõ ra: XOR khóa vòng (round key) với ma trận trạng thái.

|  |
| --- |
| [https://1.bp.blogspot.com/-vRjv-zOL9L8/XY9snv93zdI/AAAAAAAAJ-I/AR15FMTy9KomK5jB7HyBI85HuRTf3IsMACKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-vRjv-zOL9L8/XY9snv93zdI/AAAAAAAAJ-I/AR15FMTy9KomK5jB7HyBI85HuRTf3IsMACKgBGAsYHg/s1600/image.png) |
| Hình 3:  Chức năng AddRoundKey cho bước khởi tạo |

Đối với bước lặp mã hóa và bước tạo ngõ ra, vị trí "khóa mã" là các "khóa vòng" còn dữ liệu là của lần tính trước đó.  
**3)ChứcnăngSubBytes**  
Chức năng SubBytes là thực hiện thay thế từng byte của ma trận trạng thái, ngõ ra của AddRoundKey, bằng một giá trị đã quy định trong chuẩn AES. Bảng quy định giá trị thay thế gọi là S-box.

|  |
| --- |
| [https://1.bp.blogspot.com/-ocF0DHnd76I/XY9tRJMGxvI/AAAAAAAAJ-Q/vHw8t8jmSFwaeXtyVDRI0ZbeAkggLFNnACKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-ocF0DHnd76I/XY9tRJMGxvI/AAAAAAAAJ-Q/vHw8t8jmSFwaeXtyVDRI0ZbeAkggLFNnACKgBGAsYHg/s1600/image.png) |
| Hình 4:  S-box của mã hóa AES |

Ví dụ, byte cần thay thế là H08 thì dò ở hàng số 0 và cột số 8 trong bảng S-box sẽ được kết quả là 30.

|  |
| --- |
| [https://1.bp.blogspot.com/-9NMeiih9bvI/XY9tbXh0eOI/AAAAAAAAJ-U/fFw0u8UXSU0P3jf15fKlTR9ozf09O8bpgCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-9NMeiih9bvI/XY9tbXh0eOI/AAAAAAAAJ-U/fFw0u8UXSU0P3jf15fKlTR9ozf09O8bpgCKgBGAsYHg/s1600/image.png) |
| Hình 5:  Chức năng SubBytes |

**4)ChứcnăngShiftRows**  
Chức năng ShiftRows thực hiện quay trái từng hàng của ma trận trạng thái, ngõ ra của SubBytes, theo byte với hệ số quay tăng dần từ 0 đến 3. Hàng đầu tiên có hệ số quay là 0 thì các byte được giữ nguyên vị trí. Hàng thứ hai có hệ số quay là 1 thì các byte được quay một byte. Hàng thứ ba quay hai byte và hàng thứ tư quay ba byte.

|  |
| --- |
| [https://1.bp.blogspot.com/-4T2A2aKJKwA/XY9t39J72EI/AAAAAAAAJ-c/JXiqzQCc0JEfXjvr5ZGSm6D6xeDUy5asACKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-4T2A2aKJKwA/XY9t39J72EI/AAAAAAAAJ-c/JXiqzQCc0JEfXjvr5ZGSm6D6xeDUy5asACKgBGAsYHg/s1600/image.png) |
| Hình 6:  Chức năng ShiftRows |

**5)ChứcnăngMixColumns**  
Chức năng MixColumns thực hiện nhân từng cột của ma trận trạng thái, ngõ ra của ShiftRows, với một ma trận chuyển đổi quy định bởi chuẩn AES.



|  |
| --- |
| [https://1.bp.blogspot.com/-uCXm3fz21fo/XY9udiS7hsI/AAAAAAAAJ-o/zgA6mMfukzkyBc_99phrWSY5ZYdHaIY2ACKgBGAsYHg/s320/image.png](https://1.bp.blogspot.com/-uCXm3fz21fo/XY9udiS7hsI/AAAAAAAAJ-o/zgA6mMfukzkyBc_99phrWSY5ZYdHaIY2ACKgBGAsYHg/s1600/image.png) |
| Hình 7:  Ma trận chuyển đổi sử dụng trong chức năng  MixColumns |

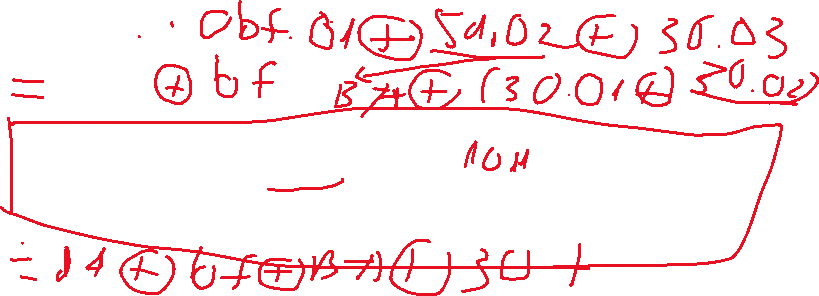
Việc biến đổi một cột của ma trận trạng thái được thực hiện bởi hai phép toán là nhân (.) và XOR (+).  
Biểu thức sau tạo ra phần tử *H04,* H là ký hiệu của số Hex, ở cột 1 trong hình minh họa "chức năng MixColumns".

**H04 =Hd4.H02 + Hbf.H03 + H5d.H01 + H30.H01=Hd4.H02 + (Hbf.H02 + Hbf.H01) + H5d.H01 + H30.H01**

|  |
| --- |
| [https://1.bp.blogspot.com/-ycQcABB_tr8/XY9vJ3bZqWI/AAAAAAAAJ-w/sOtFCU9yFnUg1NmORH82L4Ei8LbbwrbdACKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-ycQcABB_tr8/XY9vJ3bZqWI/AAAAAAAAJ-w/sOtFCU9yFnUg1NmORH82L4Ei8LbbwrbdACKgBGAsYHg/s1600/image.png) |
| Hình 8:  Chức năng MixColumns |

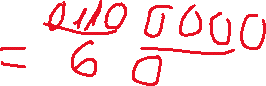
Phép nhân với H01 thì giữ nguyên giá trị. Phép nhân với H02 tương đương với việc dịch trái một bit và XOR có điều kiện như sau:

* Nếu bit MSB của giá trị được dịch bằng 1 thì giá trị sau khi dịch được XOR với H1b
* Nếu bit MSB của giá trị được dịch bằng 0 thì giữ giá trị saukhi dịch.



|  |
| --- |
| [https://1.bp.blogspot.com/-MZ0e8mFKWA8/XY9wAkEm32I/AAAAAAAAJ_I/91bKUqN_2wgAG-ClgiXd3JFZs0_o1lJOwCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-MZ0e8mFKWA8/XY9wAkEm32I/AAAAAAAAJ_I/91bKUqN_2wgAG-ClgiXd3JFZs0_o1lJOwCKgBGAsYHg/s1600/image.png) |
| Hình 9: Chi tiết về cách tính MixColumns tạo ra phần tử *H04*từ cột 1 |

Bạn đọc có thể thực hành biến đổi với các phần tử còn lại của cột 1 và các cột khác để so sánh với kết quả hình 8.



**6)Chức năng KeyExpansion**

* Chức năng KeyExpansion thực hiện tính toán khóa vòng cho bước lặp mã hóa và bước tạo ngõ ra. Kết quả của một lần thực thi KeyExpansion là một khóa vòng sử dụng cho chức năng AddRoundKey. Với mã hóa AES-128, số khóa vòng là 10 tương ứng với 9 lần AddRoundKey ở bước lặp mã hóa và 1 lần AddRoundKey ở bước tạo ngõ ra.  
  Chức năng KeyExpansion được thực hiện thông qua 4 chức năng là **RotWord, SubWord, AddRcon và AddW.**

|  |
| --- |
| [https://1.bp.blogspot.com/-64RMlbYGIXI/XY9w680HrjI/AAAAAAAAJ_U/gmyV7LoGRoYrVbydvxmWGPTtjJ6u243cQCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-64RMlbYGIXI/XY9w680HrjI/AAAAAAAAJ_U/gmyV7LoGRoYrVbydvxmWGPTtjJ6u243cQCKgBGAsYHg/s1600/image.png) |
| Hình 10:  Chức năng KeyExpansion |

* Mỗi khóa vòng có 128 bit được chia làm 4 word, mỗi word là 4 byte và ký hiệu là w[j] với j là số nguyên. Mã hóa AES-128 có 1 khóa mã và 10 khóa vòng nên tổng số từ là 44 và được đánh số từ 0 đến 43.
* **Khóa mã có 4 từ là w[0], w[1], w[2] và w[3].**
* **Khóa vòng 1 có 4 từ là w[4], w[5], w[6] và w[7]. Tương tự, khóa vòng 10 có 4 từ là w[40], w[41], w[42] và w[43].**
* Từ w[j] tính theo công thức sau, với 3 < j < 44.
* **w[j] = AddW[j - 4] = w[j - 1] + w[j - 4]**
* **w[j = 4∗ n] = AddW[j - 4] = trans(w[j - 1]) + w[j - 4]**



**Chú :** khi tính các từ ở vị trí j là bội số của 4, như w[4], w[8],... và w[40], thì

w[j-1] phải được biến đổi qua 3 chức năng RotWord, SubWord và AddRcon, gọi là trans(w[j-1]), trước khi XOR với w[j-4].

* Khóa mã key ở mục 1 được sử dụng để minh họa việc tính toán khóa vòng. Khóa mã key[127:0] được chia làm 4 từ như biểu thức sau:

**w[0] = 2b 7e 15 16  w[1] = 28 ae d2 a6**

**w[2] = ab f7 15 88  w[3] = 09 cf 4f 3c**

Việc tính toán khóa vòng 1 là thực hiện tính 4 từ w[4], w[5], w[6] và w[7]. Để tính khóa vòng 1, trans(w[3]) phải được tính trước thông qua 3 chức năng RotWord, SubWord và AddRcon.

**w[4] = AddW[0] = trans(w[3]) + w[0];**

**w[5] = AddW[1] = w[4]+ w[1];**

**w[6] = AddW[2] = w[5]+ w[2];**

**w[7] = AddW[3] = w[6]+ w[3];**

**w[8]=trans(w[7]) + w[4];**

**w[9]=w[8]+w[5]....**

**Chức năng RotWord**: Chức năng RotWord thực hiện quay trái từ w[j] một byte.

|  |
| --- |
| [https://1.bp.blogspot.com/-w4Hwq9Uvi98/XY9yH9kuJPI/AAAAAAAAJ_k/Nf8kJJbu3sYt6AWlT0oXw7CnQWazN5X4wCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-w4Hwq9Uvi98/XY9yH9kuJPI/AAAAAAAAJ_k/Nf8kJJbu3sYt6AWlT0oXw7CnQWazN5X4wCKgBGAsYHg/s1600/image.png) |
| Hình 11:  Thực thi RotWord cho từ w[3] |

**Chức năng SubWord:** thực hiện thay thế các phi tuyến từng byte của kết quả RotWord theo bảng S-box.

|  |
| --- |
| [https://1.bp.blogspot.com/-mZEVED6EO-o/XY9yU6ECE2I/AAAAAAAAJ_o/IJH7Gvk9Oss_u0LiOzArEMazYBZDMZY2wCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-mZEVED6EO-o/XY9yU6ECE2I/AAAAAAAAJ_o/IJH7Gvk9Oss_u0LiOzArEMazYBZDMZY2wCKgBGAsYHg/s1600/image.png) |
| Hình 12:  Thực thi SubWord khi chuyển đổi từ w[3] |

Chức năng AddRcon thực hiện XOR kết quả SubWord và giá trị Rcon[j/4] với j là bội số của 4. Số lượng giá trị Rcon[j/4] là 10 tương ứng với 10 lần tính khóa vòng. Chức năng AddRcon sẽ tạo ra kết quả cuối cùng của biến đổi trans(w[j-1]).  
  
**Rcon[j/4] Giátrị HEX  Vị trí sử dụng**Rcon[1]    01000000    sử dụng cho trans(w[3]) khi tính w[4]  
Rcon[2]    02000000        sử dụng cho trans(w[7]) khi tính w[8]  
Rcon[3]    04000000        sử dụng cho trans(w[11]) khi tính w[12]  
Rcon[4]    08000000        sử dụng cho trans(w[15]) khi tính w[16]  
Rcon[5]    10000000        sử dụng cho trans(w[19]) khi tính w[20]  
Rcon[6]    20000000      sử dụng cho trans(w[23]) khi tính w[24]  
Rcon[7]    40000000        sử dụng cho trans(w[27]) khi tính w[28]  
Rcon[8]  80000000        sử dụng cho trans(w[31]) khi tính w[32]  
Rcon[9]  1b000000        sử dụng cho trans(w[35]) khi tính w[36]  
Rcon[10]  36000000      sử dụng cho trans(w[39]) khi tính w[40]

|  |
| --- |
| [https://1.bp.blogspot.com/-yTCITLH547Q/XY9y6Zr_tAI/AAAAAAAAJ_w/Z8u5HKP_LXkDucO-cEP3RanAMf3G2H6XACKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-yTCITLH547Q/XY9y6Zr_tAI/AAAAAAAAJ_w/Z8u5HKP_LXkDucO-cEP3RanAMf3G2H6XACKgBGAsYHg/s1600/image.png) |
| Hình 13:  Thực thi AddRcon khi chuyển đổi từ w[3] |

Chức năng AddW thực hiện XOR w[j-4] với w[j-1] hoặc trans(w[j-1]) như công thức 4.8 để tạo ra khóa vòng.

|  |
| --- |
| [https://1.bp.blogspot.com/-nqTfUnO1d4k/XY9zHys2T4I/AAAAAAAAJ_0/Fg-dC42Il1U_Y_k3E4rXvYZTtC77JWyBgCKgBGAsYHg/s640/image.png](https://1.bp.blogspot.com/-nqTfUnO1d4k/XY9zHys2T4I/AAAAAAAAJ_0/Fg-dC42Il1U_Y_k3E4rXvYZTtC77JWyBgCKgBGAsYHg/s1600/image.png) |
| Hình 14:  Thực thi AddW để tạo khóa vòng 1 |

Như vậy, bài viết đã trình bày các bước tính toán cần thiết để mã hóa một chuỗi dữ liệu 128 bit với key 128 bit theo giải thuật AES.