Bài tập phần AES

Bài 1: Tính trong $GF(2^8)$:

$$(x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2),$$

với đa thức bất khả quy là đa thức được dùng bởi AES, tức là

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

Gợi ý: Bạn có thể sử dụng bảng tính nghịch đảo như trong Slides để tính phần tử nghịch đảo.

Đáp án: Trước hết ta tính nghịch đảo của

$$x^7 + x^6 + x^3 + x^2 = (1100\ 1100) = (CC)_{\text{hex}}$$

Tra bảng trong Slide trang 16/48, ta được

$$\begin{aligned}(x^7 + x^6 + x^3 + x^2)^{-1} = (1B)_{\text{hex}} &= (0001\ 1011) \\ &= x^4 + x^3 + x + 1\end{aligned}$$

Vậy, ta được

$$\begin{aligned}x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2) &= (x^4 + x + 1) \cdot (x^4 + x^3 + x + 1) \\ &= x^7 + x^2 + x\end{aligned}$$

Bài 2: Phép biến đổi MixColumn dựa trên phép nhân ma trận trên trường hữu hạn AES. Đặt $b = b_7x^7 + b_6x^6 + \cdots + b_0$ là một trong bốn input của phép nhân ma trận. Mỗi input này sẽ được nhân với các đa thức hằng số biểu diễn bởi byte $01, 02$ hoặc 03. Nhiệm vụ của bạn trong bài này là tìm ra các phương trình để tính ba phép nhân này. Ta ký hiệu kết quả bởi đa thức $d = d_7x^7 + d_6x^6 + \cdots + d_0$.

1. Phương trình để tính 8 bit của $d = 01 \cdot b$;
2. Phương trình để tính 8 bit của $d = 02 \cdot b$;
3. Phương trình để tính 8 bit của $d = 03 \cdot b$.

Chú ý: AES xác định "01" biểu diễn đa thức 1, "02" biểu diễn đa thức x, và "03" biểu diễn đa thức $1 + x$.

Bài 3: Bây giờ ta sẽ tính độ phức tạp theo các cổng logic của hàm MixColumn, dùng kết quả

của **Bài 2**. Ta cũng biết rằng cổng XOR với 2 input biểu diễn một phép cộng trong $GF(2)$.

1. Cần bao nhiêu cổng XOR để thực hiện một phép nhân với hằng số 01, 02 và 03, tương ứng, trong $GF(2^8)$.
2. Hãy tính độ phức tạp theo cổng trong cài đặt phần cứng của phép toán nhân ma trận với vector.
3. Độ phức tạp theo cổng logic trong cài đặt phần cứng của toàn bộ tầng Diffusion là gì? Ta giả sử rằng phép hoán vị không mất cổng nào.

Bài 4: Nhiệm vụ của bạn là tính hàm S-box (chính là ByteSub) cho các input 29, $F3$ và 01.

1. Đầu tiên dùng bảng nghịch đảo (trong Slide 16/48) để tính giá trị B' . Sau đó thực hiện ánh xạ affine bằng cách tính phép nhân ma trận với vector và cộng vector.
2. Kiểm tra lại kết quả dùng bảng S-box trong Slide số 25/48.
3. Giá trị của $S(0)$ là gì?

Bài 5: Hãy đưa ra biểu diễn bit của các hằng số vòng trong Key schedule:

- $RC[7]$
- $RC[8]$
- $RC[9]$