Lista de exercícios: AES

1. A história de desenvolvimento do AES é diferente do DES. Descreva as diferenças entre elas.

2. Apresente brevemente os eventos fundamentais do processo de desenvolvimento do AES.

3. Qual é o nome original escolhido para ser o AES?

4. Quem desenvolveu o AES?

5. Quais são os tamanhos de bloco e de chave aceitos pelo AES?

6. Compute as tabelas de multiplicação e adição para o campo primal $GF(7)$.

7. Compute a tabela de multiplicação do campo de extensão $GF(2^3)$ para o caso em que o polinômio irredutível é $P(x) = x^3 + x + 1$.

8. Escreva um programa em C ou Python para fazer o exercício anterior.

9. Compute $A(x) + B(x) \mod P(x)$ em $GF(2^4)$ usando o polinômio irredutível $P(x) = x^4 + x + 1$.
Qual é a influência da escolha do polinômio irredutível na computação para os seguintes casos?

- $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$
- $A(x) = x^2 + 1$, $B(x) = x + 1$

10. Compute $A(x) \times B(x) \mod P(x)$ em $GF(2^4)$ usando o polinômio irredutível $P(x) = x^4 + x + 1$.
Qual é a influência da escolha do polinômio irredutível na computação para os seguintes casos?

- $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$
- $A(x) = x^2 + 1$, $B(x) = x + 1$

11. Faça em $GF(2^8)$

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

,
onde o polinômio irredutível é aquele usado pelo AES $P(x) = x^8 + x^4 + x^3 + x + 1$.

12. Considere o corpo $GF(2^4)$, com $P(x) = x^4 + x + 1$ sendo o polinômio irredutível. Ache as inversas de $A(x) = x$ e $B(x) = x^2 + x$. Verifique sua resposta multiplicando as inversas que você encontrou por A e B.

13. Encontre todos os polinômios irredutíveis de grau 3 e 4 em $GF(2^n)$. Considere apenas polinômios com coeficiente do termo de maior grau igual a um.

14. Consider AES com bloco e chave de 128 bits. Qual é a saída do primeiro turno do AES se a entrada e a chave consistem de 128 valores iguais a 1?

15. Seja $W = (w_0, w_1, w_2, w_3) =$ (`0x01000000`, `0x00000000`, `0x00000000`, `0x00000000`) a entrada em partes de 32 bits para AES com bloco de 128 bits. As subchaves para a computação do resultado do primeito turno do AES é $W_0, \ldots, W_7$ com 32 bits cada são:

- $W_0 =$`(0x2B7E1516)`
- $W_1 =$`(0x28AED2A6)`
- $W_2 =$`(0xABF71588)`

- W_3 =(0x09CF4F3C)
- W_4 =(0xA0FAFE17)
- W_5 =(0x88542CB1)
- W_6 =(0x23A33939)
- W_7 =(0x2A6C7605)

Descreva como a entrada é processada no primeiro turno (elementos S-Box). Para este exercício, pode ser útil escrever um código que apresenta a computação dos passos intermediários para computação de `ShiftRows`, `SubBytes` e `MixColumns`.

Além disso, 1) compute a saída do primeiro turno do AES para a entrada W e as subchaves $W_0, \ldots, W_7$. 2) compute a saída do primeiro turno do AES para o caso que todos os bits de entrada são zeros. Quantos bits mudaram?

16. Compute o elemento S-Box (ByteSub) para bytes de entrada `0x29`, `0xF3`, `0x01` e `0x00`. Para isso, primeiro procure pela tabela das inversas em $GF(2^8)$ e depois faça a multiplicação e adição entre matrix e vetor da S-Box. Compare com a S-Box em `https://en.wikipedia.org/wiki/Rijndael_S-box`.

17. O tamanho mínimo de chave do AES é 128 bits. Assuma que um hardware especial com múltiplos processadores pode testar uma chave em 10 nanosegundos por 1 processador. Considere que cada processador custa R\$30. Considere que o desempenho do processador duplica a cada 18 meses, mas o preço mantém constante. Quanto tempo é necessário esperar para construir uma máquina de busca de chaves baseado em força bruta que quebra o AES em uma semana e custa até 3 milhões de reais?

18. Assuma o uso do AES com chave de 192 bits e também que existe um hardware capaz de testar $3 \cdot 10^7$ chaves por segundo.

- Se usamos 100 mil cópias desse hardware em paralelo, quanto tempo em média a busca por uma chave leva? Compare esse tempo com a idade do universo (10^10 anos)
- Considerando que o hardware dobra sua capacidade a cada 18 meses, quanto tempo em média temos que esperar para fazer uma busca de chave no AES-192 em 24 horas usando 100 mil cópias em paralelo?

19. O que é criptanálise diferencial? O DES e o AES são resistentes a isso?

20. O que é criptanálise linear? O DES e o AES são resistentes a isso?