Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 05 - AES

Para 20/11/2023.

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. Qual foi o conjunto original de critérios usados pelo NIST para avaliar as cifras AES candidatas?
2. Qual foi o conjunto final de critérios usados pelo NIST para avaliar as cifras AES candidatas?
3. Qual é a diferença entre Rijndael e AES?
4. Responda:
   (a) Qual é a finalidade do array Estado?
   (b) Como é construída a S-box?
   (c) Descreva rapidamente o estágio SubBytes, ShiftRows, MixColumns, AddRoundKey, e o algoritmo de expansão de chave.
5. Quantos bytes em Estado são afetados por ShiftRows?
6. Use a chave `1010 0111 0011 1011` para encriptar o texto claro `"ok"`conforme expresso em ASCII, ou seja, `0110 1111 0110 1011`. Os projetistas do S-AES obtiveram o texto cifrado `0000 0111 0011 1000`. E você?
7. Compare AES com DES. Para cada um dos seguintes elementos do DES, indique o elemento comparável no AES ou explique por que ele não é necessário no AES.
   (a) XOR do material da subchave com a entrada da função f.
   (b) XOR da saída da função f com a metade esquerda do bloco.
   (c) função f.
   (d) permutação P.
   (e) troca de metades do bloco.

8. (1 ponto-extra) Calcule a saída da transformação **MixColumns** para a seguinte sequência de bytes de entrada `"67 89 AB CD"`. Aplique a transformação **InvMixColumns** ao resultado obtido para verificar seus cálculos. Altere o primeiro byte da entrada de `"67"`para `"77"`, realize a transformação **MixColumns** novamente para a nova entrada e determine quantos bits mudaram na saída.

   Nota: você pode realizar todos os cálculos à mão ou escrever um programa que dê suporte a eles. Se escolher escrever um programa, ele deverá ser feito inteiramente por você; nesta tarefa, não use bibliotecas ou código fonte de domínio público (você pode se guiar pelos exemplos Sage disponibilizados).

9. (2 pontos-extra) Crie um software que possa encriptar e decriptar usando S-AES. Dados de teste: um texto claro binário de `0110 1111 0110 1011` encriptado com uma chave binária de `1010 0111 0011 1011` deverá dar o texto cifrado binário `0000 0111 0011 1000`. A decriptação deverá funcionar da mesma forma.

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.