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. 08

Para 11/12/2023

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. Por que mdc(n, n + 1) = 1 é para dois inteiros consecutivos n e n + 1?
2. Usando o teorema de Fermat, encontre 3^{201} mod 11.
3. Use o teorema de Fermat para encontrar um número a entre O e 72, com a congruente a 9794 módulo 73.
4. Use o teorema de Euler para encontrar um número a entre 0 e 9, tal que a seja congruente a 7^{1000} módulo 10. (Observe que isso é o mesmo que o último dígito da expansão decimal de 7^{1000}.)
5. Use o teorema de Euler para encontrar um número x entre 0 e 28, com x^{85} congruente a 6 módulo 35 (Você não precisará usar qualquer pesquisa por força bruta).
6. Observe, na Tabela 8.2, que $\phi(n)$ é par para $n > 2$. Isso é verdadeiro para todo $n > 2$. Dê um argumento conciso para explicar por que isso acontece.
7. Se n é composto e passa no teste de Miller-Rabin para a base a, então n é chamado de pseudoprimo forte à base a. Mostre que 2047 é um pseudoprimo à base 2.
8. O exemplo usado por Sun-Tsu para ilustrar o CRT foi

   $$x = 2 \pmod 3); \quad x = 3 \pmod 5; \quad x = 2 \pmod 7$$

   Solucione para x.

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