UNIVERSIDADE
FEDERAL DO CEARÁ

Segurança - 2023.1 Prof. Marcos Dantas Ortiz - mdo@ufc.br

Aluno:_____

RSA - Geração de Chaves

1. Escolha dois números primos grandes p, q.
2. Calcule n = pq, z = (p-1)(q-1)
3. Escolha e (com e < n) que não tenha fatores comuns com z. (e, z são "relativamente primos").
4. Escolha d tal que ed - 1 seja divisível exatamente por z.

(em outras palavras: ed mod z = 1).

5. Chave pública é (n,e).
6. Chave privada é (n,d).

RSA - Cifragem e Decifragem

1. Para criptografar a mensagem m (<n), calcule $\mathbf{c = m^e \bmod n}$
2. Para descriptografar o padrão de bits recebido, c, calcule $\mathbf{m = c^d \bmod n}$

Questão 1) Usando o algoritmo de chave pública RSA, faça:

a) Se $p = 7$ e $q = 11$, liste 5 valores válidos para e.
b) Se $p = 13$, $q = 31$, e $e = 7$, encontre d.
c) Usando $p = 5$, $q = 11$, e $e = 27$, encontre d e criptografe "RSA". Utilize A = 1, B = 2, C = 3... , Z = 26

Questão 2) Em um sistema de chave pública usando RSA, você intercepta o texto cifrado C = 10 enviado a um usuário cuja chave pública é (e = 5, n=35). Qual é o texto claro M?

Questão 3) Quais são os requisitos que devem ser atendidos pelos algoritmos de chave pública?

Questão 4 (FCC-2009-TJ-PI-Analista Judiciário-Análise de Sistemas) - O usuário torna a sua chave **I** disponível para todos os que podem eventualmente enviar-lhe informações criptografadas. Essa chave pode apenas codificar os dados, mas não pode descodificá-los, ou seja, não pode abrir as informações criptografadas, mas é capaz de criptografar um arquivo. No envio da informação criptografada, a chave **II** é utilizada, e quem recebe o texto cifrado, descodifica-o com a chave **III** . O algoritmo de criptografia **IV** rata o texto como se fosse um número muito grande, eleva-o à potência de outro número também enorme e, então, calcula o restante depois de dividido por um terceiro número igualmente gigantesco. Por fim, o número resultante de todo este processo é convertido de novo em texto. Na criptografia V o algoritmo divide os dados em pequenos pedaços chamados de blocos, depois coloca letras em volta, muda a informação presente em cada bloco para números, comprime e expande esses dados e coloca esses números em fórmulas matemáticas que incluem a chave. Então o algoritmo repete todo o processo, até mesmo dúzias de vezes, se necessário.

Completam correta e respectivamente as lacunas I a V:

a) pública; privada; privada; simétrica; assimétrica.
b) pública; privada; pública; assimétrica; simétrica.
c) privada; privada; pública; assimétrica; simétrica.
d) pública; privada; pública; simétrica; assimétrica.
e) pública; pública; privada; assimétrica; simétrica.

Bom Trabalho!