TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE

CARGO 5: INSPETOR DE CONTROLE EXTERNO – ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA

APLICAÇÃO: 29/11/2015

PADRÃO DE RESPOSTA DEFINITIVO

Espera-se do candidato a elaboração de texto em que desenvolva os pontos apresentados abaixo.

O algoritmo RSA-4096 é uma cifra assimétrica que utiliza chaves de 4096 *bits*, enquanto que o MD-5 é uma função de resumo criptográfico, *hash*, que gera resumos de 128 *bits*. Enquanto o algoritmo apresenta alto grau de segurança, a função tem conhecidos ataques que a fragilizam para uso como resumo criptográfico.

Apesar desse fato, a combinação dos dois não leva a um uso inseguro, pois, a menos que a chave pública do destinatário seja substituída, o *hash* do arquivo é geralmente obtido antes mesmo do envio, o que força um eventual atacante externo a montar um ataque de segunda pré-imagem. Assim, apesar de haver falhas estruturais já conhecidas do MD-5, ao contrário do que ocorre no caso de sigilo, autenticação e verificação de integridade impõem uma janela de tempo bem mais breve para que os ataques sejam válidos. Assim, a escolha é adequada para a aplicação sugerida.

Outras opções seriam o uso de funções de *hash* como SHA-2 ou SHA-3 junto com RSA-4096, sendo preferida a função SHA-3.