CODIFICANDO E DECODIFICANDO UMA MENSAGEM EM CRIPTOGRAFIA RSA

RUAN EVISLON FERREIRA DA SILVA, JOCEL FAUSTINO NORBERTO DE OLIVEIRA,

O que fazemos para codificar uma mensagem no sistema de criptografia RSA é calcular sua potencia módulo n relativamente a um expoente especialmente escolhido. Entretanto, para que isto seja viável, a mensagem deve ser um número inteiro. Mas não é isto o que ocorre em geral: a maior parte das mensagens é um texto. Dessa forma, a primeira coisa a fazer, se desejarmos usar o método RSA, é inventar uma maneira de converter a mensagem em uma sequência de números. Suponhamos, para simplificar, que a mensagem original é um texto onde não há números, apenas palavras, e no qual todas as letras são maiúsculas. Portanto, em última análise a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre palavras. Chamaremos esta primeira etapa de pré-codificação, para distingui-la do processo de codificação propriamente dito. Aqui ilustraremos resumidamente esse processo. Uma vez feito o processo de codificação faremos adiante o processo para decodificar um bloco da mensagem codificada. Em outras palavras, queremos saber qual é a receita que nos permite, de posse de um bloco codificado e da chave pública, reconstruir o bloco original, antes da codificação. Este trabalho é parte do processo de entendimento da Criptografia RSA, bem como ilustra uma das principais aplicações da Aritmética modular.

PALAVRAS-CHAVE: CRIPTOGRAFIA, MENSAGEM, CONGRUÊNCIA

ÀREA TEMÀTICA: MATEMÁTICA (PESQUISA)

FORMA DE APRESENTAÇÃO: RELATO DE EXPERIÊNCIA