XII SEMANA ACADÊMICA DA
LICENCIATURA EM MATEMÁTICA
DO IFRS, CAMPUS CAXIAS DO SUL
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL
CAMPUS CAXIAS DO SUL, RS - BRASIL
17, 20 E 21 DE OUTUBRO DE 2022

Um estudo da Cifra de Hill

Acadêmico Renan Chilanti Susin, Me. Félix Afonso de Afonso, Me. Nícolas Moro Müller

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - Campus Caxias do Sul, RS, Brasil

Resumo

A palavra Criptografia vem do latim cryptographia, formado de crypto (kryptós oculto, secreto) + graphia (graphía, com o sentido de escrita). A criptografia estuda os métodos para codificar uma mensagem de modo que somente seu destinatário legítimo consiga interpretá-la. Nesse contexto, o objetivo deste estudo é compreender o sistema de criptografia denominado Cifra de Hill. O nome Cifra de Hill é referência a Lester Sanders Hill, que introduziu esse sistema em dois trabalhos na American Mathematical Monthly: “Criptography in an Algebraic Alphabet” (Vol. 36, 1929) e “Concerning Certain Linear Transformation Apparatus of Criptography” (Vol. 38, 1931). A Cifra de Hill é um sistema de criptografia de chave simétrica (privada), ou seja, a chave de codificação deve ser mantida privada entre o remetente e o destinatário da mensagem. Tal método utiliza de vários conceitos relacionados à Álgebra Linear, dentre os principais a eliminação gaussiana, operações com matrizes, independência linear, base e transformações matriciais. Além disso, utiliza fundamentos da Aritmética Modular como congruência e inverso modular. A metodologia utilizada neste estudo foi a pesquisa bibliográfica, visto que os pré-requisitos relacionados a Aritmética, Álgebra Linear e o sistema de criptografia abordado foram baseados em materiais já publicados. Constatou-se que a Cifra de Hill apresenta diversas vantagens na criptografia de dados como disfarçar as frequências das letras do texto comum (mensagem não codificada), além da sua simplicidade devido ao uso de multiplicação e inversão de matrizes para cifrar e decifrar, oferecendo alta velocidade e rendimento na aplicação. No entanto, a principal desvantagem desta cifra é que ela criptografa blocos de texto comum idênticos em blocos de texto cifrado idênticos, resultando em uma baixa segurança a ataques de texto comum conhecido. Tal sistema foi amplamente utilizado durante o período de sua origem até meados da Segunda Guerra Mundial (1939-1945). No contexto da época foi altamente revolucionária por causa do uso de matrizes. Atualmente seu uso prático está obsoleto, devido aos enormes avanços tecnológicos dos computadores, porém a cifra de Hill deixou o seu legado servindo de base e influência para outros métodos de criptografia simétrica. Como resultado do estudo, ficou evidente a importância e dependência de muitas definições e resultados da Aritmética Modular e Álgebra Linear para o funcionamento da Cifra de Hill. Além disso, com a realização deste estudo foi possível aprofundar os conhecimentos nestes tópicos, visto que alguns dos resultados abordados não foram trabalhados durante a graduação. Também, foi possível constatar que a Criptografia pode ser uma excelente ferramenta para o ensino de Matemática, a nível básico e superior.

Palavras-chave: Aritmética Modular. Álgebra Linear. Criptografia. Cifra de Hill. -.

Modalidade: Comunicação Científica.