ENEPEX
ENCONTRO DE ENSINO, PESQUISA E EXTENSÃO
9º ENEPE UFGD • 6º EPEX UEMS

# Um Estudo do Sistema Criptográfico RSA

[1] **SALAZAR. Douglas Correia** (douglassalazar_dcs@hotmail.com); [2] **MOLGORA.** Adriana Betânia de Paula (adrianamolgora@gmail.com);

[1] Aluno do curso de Ciência da Computação-UEMS;
[2] Professora do curso de Ciência da Computação-UEMS;

O projeto de iniciação científica possibilita ao aluno através da pesquisa, aumentar seus conhecimentos teóricos e práticos de determinado assunto, além de ser uma grande experiência para sua vida tanto profissional como pessoal. Juntamente com a Professora Adriana Betânia de Paula Molgora, foi desenvolvido uma pesquisa sobre os fundamentos matemáticos e teóricos da Criptografia RSA além da implementação em meio computacional. Desde os tempos primordiais, a proteção de dados ou informações sempre foi muito importante. Em diversas situações como em assuntos relacionados a guerras, o homem precisou enviar mensagens secretas e, para isso tentou desenvolver maneiras de embaralhar essas mensagens de forma que ficassem protegidas. Dessa forma nasceu a criptografia, que pode ser definida como um conjunto métodos ou técnicas que realizam a codificação e decodificação de dados. A criptografia pode ser classificada em simétrica ou assimétrica. A criptografia simétrica é também denominada de criptografia de chave privada, existindo uma única chave para codificação e decodificação dos dados. A assimétrica é denominada de criptografia de chave pública, onde são necessárias duas chaves, uma para codificação e outra para decodificação dos dados. Na criptografia de chave privada a chave deve ser mantida em segredo tanto pelo emissor quanto pelo receptor da mensagem. Já na criptografia de chave pública a chave usada para codificação dos dados é de domínio público e, por essa razão é denominada de chave pública. Nesse caso, a chave usada para decodificação é denominada de chave privada sendo mantida em segredo apenas pelo destinatário legítimo. O método criptográfico RSA é um dos métodos mais utilizados na atualidade. Esse método é um dos algoritmos de criptografia de chave pública mais seguros da atualidade e é utilizado em softwares como o Netscape, um popular programa de navegação da Internet. Um estudo minucioso desse método depende do entendimento do embasamento teórico matemático e computacional envolvido nos processos de codificação e decodificação dos dados. Este trabalho propõe realizar um estudo desse método criptográfico de forma detalhada a fim de disponibilizar conhecimentos sobre o mesmo e possibilitar pesquisas posteriores mais avançadas.

**Palavra Chave:** Criptografia, RSA, Cifragem, Decifragem