9º FEPEG FÓRUM DE ENSINO, PESQUISA, EXTENSÃO E GESTÃO
TRABALHOS CIENTÍFICOS APRESENTAÇÕES ARTÍSTICAS E CULTURAIS DEBATES MINICURSOS E PALESTRAS
23 A 26 SETEMBRO DE 2015
Campus Universitário Professor Darcy Ribeiro
ISSN 1806-549X
A HUMANIZAÇÃO NA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

DESENVOLVIMENTO DE OBJETO DE APRENDIZAGEM DIGITAL DE MATEMÁTICA COMBINATÓRIA A PARTIR DA CRIPTOGRAFIA CLÁSSICA.

Rosivaldo Antonio Goncalves, Heveraldo Rodrigues de Oliveira

INTRODUÇÃO:

A análise combinatória é um dos temas importantes da matemática básica, e é requisito para o aprendizado de outros conteúdos como matemática discreta e probabilidade, e têm implicações em outros temas como teoria dos números, teoria dos autômatos, e inteligência artificial. Além disso, a combinatória tem uma infinidade de aplicações em outras áreas tais como computação, engenharia, geologia, química, entre outras. Entretanto, ensinar Análise Combinatória tem sido um desafio para os professores nas salas de aula. Porém, alunos que têm contato com algumas atividades simples de contagem e formação de agrupamentos durante o Ensino Fundamental, têm mais facilidade de assimilar o conteúdo de estudos futuros. O uso de fórmulas propõe um trabalho mecânico que não oferece ao aluno a oportunidade de compreensão do conteúdo. Novas abordagens do tema evidencia a necessidade de busca de alternativas de ensino do mesmo. Uma das abordagens recorrentes é o ensino de Análise Combinatória por resolução de problemas, um processo investigativo e experimental, no qual os alunos ao serem expostos a situações-problemas possam fazer inferências, desenvolver soluções pessoais a partir das técnicas de contagem, para que enfim seja feita uma formalização. Um dos desafios dos profissionais que aderem a uma nova abordagem tem sido encontrar material para aplica-la, falta subsídio para as mesmas. Um dos materiais mais dinâmicos e de maior apelo com os alunos são os chamados Objetos de Aprendizagem digitais, que são utilizados como recurso auxiliar de ensino em sua maioria, e são reutilizáveis e disponíveis em repositórios na internet. Por séculos a criptografia usou somente ideias baseadas em combinatória. A formação de agrupamentos por Combinações Arranjos e Permutações é o núcleo dessa fase da Criptografia, conhecida como ‘Criptografia Clássica’. Este trabalho se ancora fortemente na perspectiva de que softwares tornam os conteúdos de matemática mais atrativos, e o que propusemos foi a construção do software.

OBJETIVO:

Aapresentar o processo de desenvolvimento de um objeto de aprendizagem digital, que utilize a criptografia clássica como fonte de elaboração de problemas que necessitem do raciocínio combinatório e do uso de técnicas de contagem em sua resolução.

METODOLOGIA:

Para o desenvolvimento da proposta elaboramos aplicativos baseados em modelos simples de criptografia de alfabetos, seguidos de alfabetos e números, e por fim codificação de textos mais complexos. Assim os níveis de complexidade ficaram suficientes para determinados graus de superação de dificuldades. O primeiro passo foi também elaborar um construto teórico no qual ficou balizada a lógica do algoritmo de programação.

ISSN 1806-549X

RESULTADO:

O software foi desenvolvido, e testes foram realizados, sendo que o aplicativo funciona com desempenho satisfatório. Alguns testes com alunos voluntários do programa de iniciação científica Júnior da Unimontes/ Fapemig, foram realizados.

CONCLUSÃO: Os alunos que testaram o aplicativo mostraram facilidade com o material, bem como tiveram a oportunidade de associar esse aprendizado tanto na inicialização de estratégias de guerra desde períodos antes de Cristo, adormecendo por muito tempo, mas vindo a se manifestar importante na segunda guerra mundial e no surgimento de computadores, chegando na atualidade uma das ferramentas mais importantes na criação de senhas eletrônicas.

REFERÊNCIAS:

COUTINHO, Severino Coullier. Números inteiros e criptografia rsa. Rio de Janeiro, Instituto Nacional de Matemática Pura e Aplicada – IMPA – 2ed. 2005.

SCHNEIER, Bruce – *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Wiley: Springer ebook, 2011.