CriptoMat1: ensinando Matemática utilizando conceitos de Criptografia - cifra de César e César estendida

Moisés Bruno dos Santos Gregório[1], **Carla Adriana Barvinski**[1], **Valguima Odakura**[1], **Lino Sanabria**[1]

[1]Faculdade de Ciências Exatas e Tecnologia (FACET)
Universidade Federal da Grande Dourados (UFGD)
Dourados – MS – Brasil

{brunomoises, carlabarvinski, valguima.odakura, linosanabria}@gmail.com

Resumo. *O ensino de Matemática é desafiador tanto para alunos quanto para professores, de um lado temos alunos reclamando da falta de atratividade e aplicação, da distância entre o ensinado e a vida real, do outro lado, professores buscando instrumentos auxiliares que tenham uma linguagem moderna e atraente. Neste artigo é apresentado o CriptoMat1, um aplicativo que busca trazer respostas a esse desafio, despertando no aluno o interesse pela Matemática através do estudo e aplicação da Criptografia. O CriptoMat1 foi desenvolvido em 5 módulos independentes, podendo ser utilizado por alunos e professores do ensino fundamental e médio, além de universitários.*

1. Introdução

No ensino de Matemática é usual a indagação dos alunos quanto a utilidade do que está sendo ensinado, e na maioria das vezes a resposta é de que isto será usado no futuro. Um exemplo clássico é o do Máximo Divisor Comum, que é ensinado utilizando a fatoração, embora o método de Euclides seja ainda hoje o mais eficiente do ponto de vista computacional. Uma abordagem mais interessante talvez seja criar a necessidade de aprendizado de um conceito antes de introduzí-lo.

Neste artigo é apresentado o aplicativo CriptoMat1[1], em que a Criptografia é o fio condutor que liga os conceitos de Matemática ao processo de cifragem. O CriptoMat1 faz parte de um projeto denominado CriptoMat, o qual visa o desenvolvimento de módulos de Objetos de Aprendizagem (OA) que correlacionam Criptografia e Matemática. O principal objetivo do CriptoMat1 é sua aplicação, como instrumento de apoio em sala de aula, em escolas de ensino fundamental e médio, por alunos do Mestrado Profissional em Matemática (PROFMAT), ofertado pela Universidade Federal da Grande Dourados (UFGD).

O aplicativo Criptomat1 é composto de 5 módulos independentes que conceituam, exemplificam e permitem ao aprendiz, a realização de operações de cifragem-decifragem da Cifra de César e Cifra de César estendida, proporcionando uma reflexão sobre os conceitos matemáticos envolvidos em sua operacionalização.

O aplicativo é compativel com Ambientes Virtuais de Aprendizado (AVA) tais como Moodle[2], e também pode ser executado nos mais diferentes navegadores. O CriptoMat1 tem como público alvo alunos do Ensino Fundamental, Médio e de Graduação.

[1]CriptoMat1 Disponível em: http://ivitu.com.br/criptomat/criptomat1/
[2]Moodle Disponível em: https://moodle.org/

No primeiro e segundo caso serve de material de apoio para professores de Matemática. No terceiro caso, os professores podem utilizá-lo para introdução ao tema Criptografia.

O CriptoMat destina-se ao ensino de conceitos de Matemática tais como: números primos; fatoração; fator comum; divisor; múltiplo divisor comum; máximo divisor comum; mínimo múltiplo comum; operações; operação inversa; função; função injetiva; função sobrejetiva; função invertível; inversa de uma função; matrizes; operações com matrizes e matrizes inversas.

Este artigo está organizado como se segue. Na seção 2 é descrito o processo de desenvolvimento do CriptoMat1. Na seção 3 o aplicativo CriptoMat1 é apresentado. Por fim, na seção 4, as considerações finais são descritas.

2. Processo de desenvolvimento

O processo de desenvolvimento do CriptoMat1 compreendeu as fases de planejamento didático-pedagógico, estudo e definição de tecnologias adequadas ao projeto, seleção de ferramentas para a implementação, prototipação e implementação.

As aplicações foram desenvolvidas para a plataforma Web, para serem visualizadas em um navegador Web ou em um AVA. Os objetos de aprendizagem do CriptoMat1 foram desenvolvidos utilizando HTML5 [W3C a], uma linguagem de marcação de texto para a Web. O HTML é utilizado para fazer a estruturação no navegador de hipermídias como textos, imagens e animações. Para melhorar a apresentação dos conteúdos, foi utilizado *Cascading Style Sheets* (CSS) com o objetivo de tornar a interface mais agradável e interessante. O CSS é uma linguagem de estilo utilizada para descrever a apresentação de um documento escrito em HTML e descreve como o elemento estruturado deve ser renderizado na tela.

Para aumentar a interatividade com o usuário nos objetos de aprendizagem desenvolvidos, foi utilizado Javascript, que é uma linguagem de programação interpretada. Utilizando Javascript pode-se obter animações feitas pelo navegador, que tornam a aplicação mais dinâmica e interessante.

Os módulos do CriptoMat1 foram implementados usando a coleção de padrões para desenvolvimento de objetos de aprendizagem *Sharable Content Object Reference Model* (SCORM), [SCO a], [SCO b] e [SCO c], a qual utiliza padrão de metadados baseados na linguagem de marcação *Extensible Markup Language* (XML) [W3C b]. A aplicação de um padrão na implementação de recursos educacionais de *e-learning* é relevante, pois favorece vários aspectos, tais como, a localização, reuso, compartilhamento e interoperabilidade. O uso do SCORM incorpora um conjunto de padrões que facilita o uso de OAs em ambientes virtuais de ensino, garantindo as propriedades básicas dos objetos de aprendizagem, como: adaptabilidade, durabilidade, reusabilidade, dentre outras. A adoção do SCORM favorece o compartilhamento do objeto de aprendizagem e sua manutenção.

Por ser uma aplicação multimídia cujo desenvolvimento envolve a implementação de diferentes aspectos, tais como a criação de animações, a elaboração de *scripts* para captura de entrada de dados, o desenho de interface com o usuário, etc, foram utilizadas várias ferramentas de softwares, as quais estão listadas abaixo:

- Adobe Flash Professional CS6 [Adobe c] para implementação das animações.

- Adobe Dreamweaver CS6 [Adobe b] para desenvolvimento dos *scripts* que fazem a interação com o usuário.
- Adobe Captivate versão 6.0 [Adobe a] para o desenvolvimento da interface, organização das informações, aplicação dos padrões nos objetos de aprendizado.

3. CriptoMat1

O aplicativo Criptomat1 ao todo é composto de 5 módulos independentes que conceituam, exemplificam e permitem ao aprendiz, a realização de operações de cifragem-decifragem da Cifra de César e Cifra de César estendida, proporcionando uma reflexão sobre os conceitos matemáticos envolvidos em sua operacionalização. Nessa seção são apresentados os cinco módulos do CriptoMat1.

Os modulos do CritpoMat1 podem ser acessados através do endereço `http://ivitu.com.br/criptomat/criptomat1/`

3.1. Módulo 1 – Conceituando Criptografia

Esse módulo apresenta o conceito básico de Criptografia, através da narrativa de fatos históricos relacionados com o tema. A interface construída é simples, de fácil entendimento e interativa, faz uso de animações, textos e sons. Buscou-se fazer a apresentação teórica em formato de aula, em que um personagem animado faz o papel de professor. Foram aplicadas várias imagens e animações a fim de manter a atenção do aluno e favorecer a fixação do conteúdo. O módulo apresenta a conceituação da Criptografia, motivação, tipos de cifra, história da Criptografia, cifra de César e exercícios de cifragem ao final. A Figura 1 exibe o ambiente e uma das falas do personagem:

Figure 1. Módulo 1: Animação que apresenta os conceitos básicos da Criptografia.

São apresentados 6 exercícios de avaliação, que estimulam a fixação do conteúdo aprendido no módulo. A Figura 2 exibe uma tela com um dos exercícios, em que é apresentando um número de deslocamento e uma palavra simples. O aprendiz deve decifrar a palavra aplicando a cifra de César e inserir o texto obtido em uma caixa de texto fornecida.

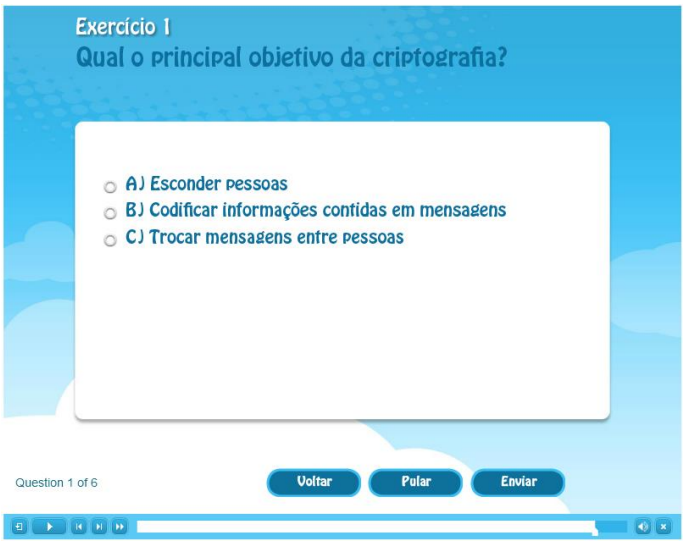

Figure 2. Módulo 1: Exercício do primeiro módulo.

Os testes são resolvidos em sequência e após a resolução dos mesmos, o aprendiz é informado de seu desempenho, conforme ilustrado na Figura 3. Para concluir o módulo, o aproveitamento deve ser igual ou superior a 67% (4 questões de 6). Se o aluno não obtiver a nota mínima, ele deverá assistir novamente o módulo e refazer os exercícios.

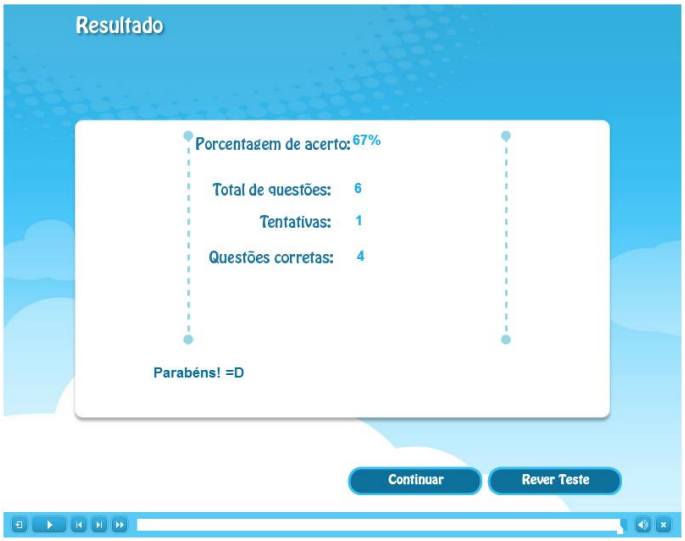

Figure 3. Módulo 1: Apresentação de resultado avaliativo do primeiro módulo.

Ao término do Modulo 1 o aprendiz terá adquirido conhecimento básico sobre a Criptografia, e espera-se também, conseguir despertar seu interesse pelo assunto e a busca por maior conhecimento a respeito do tema.

3.2. Módulo 2 – Aplicação para executar a cifragem de césar

O objetivo deste módulo é exercitar os conceitos aprendidos no Módulo 1, sanando eventuais dúvidas remanescentes, através da execução da cifra de César. Neste módulo o aprendiz testa possibilidades cifrando textos grandes e observando como é calculada a

substituição das letras: o usuário informa o deslocamento e uma mensagem a ser cifrada. Para facilitar o entendimento, pode-se optar pela cifragem rápida, na qual toda a mensagem é cifrada de uma só vez ou pela cifragem lenta, em que cada caractere da mensagem é cifrado um a um. Após executar a codificação da mensagem a aplicação retornará o texto cifrado ao aprendiz que poderá escolher entre realizar a decifragem da mensagem ou executar a aplicação novamente, modificando a mensagem ou o deslocamento. A substituição é ilustrada através de dois círculos circunscritos animados, onde o círculo interno representa o domínio e o externo representa o contradomínio. A Figura 4 ilustra a aplicação.

Figure 4. Módulo 2: Aplicação de cifragem de texto com deslocamento variável.

As interações desse módulo proporcionam um melhor entendimento e fixação do funcionamento da cifragem por substituição, pois o aprendiz tem a possibilidade de executar vários testes. Intenciona-se, com esta aplicação, despertar a curiosidade e interesse do aprendiz pela cifragem, além de já trabalhar, ainda que o aprendiz não perceba, com aritmética modular.

4. Módulo 3 – Cifra de César estendida

O Módulo 3 mostra que a cifra de César é fácil de ser quebrada. Nele é apresentado um melhoramento da cifragem de César, pela modificação da estrutura do cálculo de substituição, chamada cifra de César estendida. A mudança proposta é a adição de dois parâmetros (A e B), que através da equação: $X' = A * X + B$, em que X é a posição do alfabeto onde o caractere a ser cifrado está, e X' é a posição da letra pela qual o caractere a ser cifrado será substituído, após a cifragem. A substituição de apenas um número de deslocamento por A e B proporciona o aumento das possibilidades de combinações, portanto a segurança da cifragem.

Neste módulo o conteúdo é apresentado de forma semelhante ao de uma sala de aula, devido à sua natureza teórica. Pode-se observar o ambiente do Módulo 3 na Figura 5, sendo possível que conceitos da Matemática elementar possam ser explorados pelo professor.

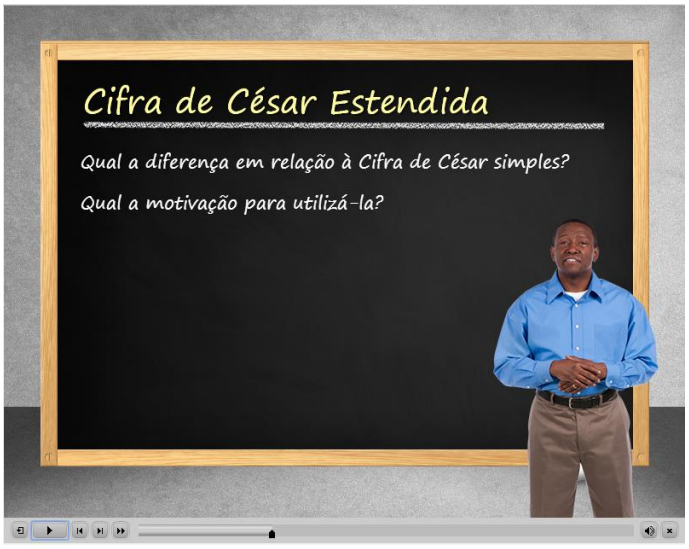

Figure 5. Módulo 3: Ambiente semelhante à uma sala de aula.

5. Módulo 4 – Exercitando a cifragem de César estendida

Este módulo permite ao aprendiz observar o funcionamento do método de cifragem de César estendida, através da realização de testes de cifragem ou decifragem em quaisquer mensagens, conforme ilustra a Figura 6.

Figure 6. Módulo 4: Interface de cifragem utilizando a Cifra de César estendida.

O principal objetivo do módulo é introduzir uma modificação que levará à necessidade de novos conceitos de matemática. Isto é obtido por meio de testes que permitem que o aprendiz, utilizando suas habilidades cognitivas, perceba que para algumas escolhas dos valores de A e B se obtém uma cifragem ideal, ou seja, cifrando e decifrando a mensagem sem perda de informação, enquanto para outras, não é possível realizar o processo inverso (decifragem). Ao constatar isso, o aluno terá a curiosidade de descobrir o que determina o funcionamento ou a falha da cifragem. Através dessa dúvida é introduzido o conteúdo do módulo 5, que através de conceitos matemáticos básicos apresenta o problema e a solução ao aluno.

6. Módulo 5 – Máximo Divisor Comum na Criptografia

Este módulo tem como objetivo esclarecer as dúvidas geradas na execução da unidade anterior, em ocasiões na qual o resultado da decifragem não funcionou conforme o esperado e apontar a causa das dificuldades na recuperação de algumas mensagens. Nele dá-se destaque a operações Matemáticas básicas mostrando que o sucesso ou a falha na cifragem está ligado a conceitos matemáticos simples como, por exemplo, o M.D.C (Máximo Divisor Comum). O módulo consiste em 3 vídeos que abordam o assunto gradativamente. A figura 7 ilustra a interface de apresentação do vídeo.

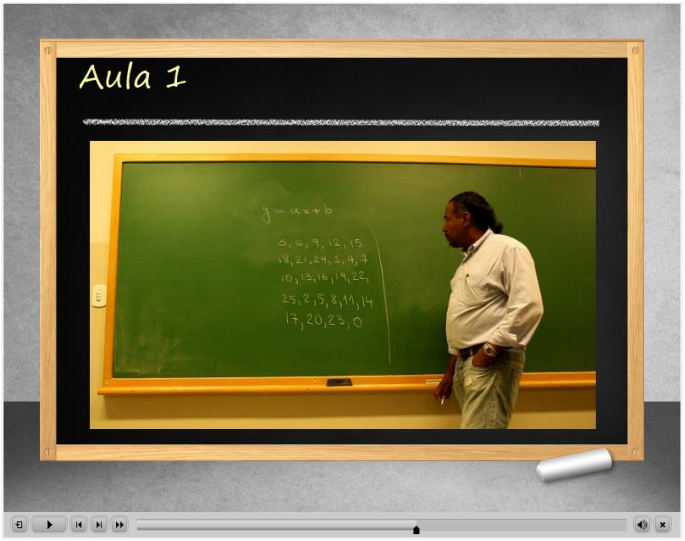

Figure 7. Módulo 5: Interface da exibição da aula em vídeo.

7. Considerações Finais

O CriptoMat1 em sua primeira versão está direcionado para uso pelo professor do ensino Fundamental e Médio como material de apoio, inclusive com roteiro didático com sequência de aulas, de acordo com o conceito matemático a ser abordado. Ainda, esta versão permite que universitários explorem o aplicativo, sem o auxílio do professor, sendo guiado à reflexão sobre Criptografia, algoritmos e Matemática.

O aplicativo ainda não foi testado em sala de aula, sendo esta a próxima atividade do projeto CriptoMat1. O CriptoMat1 será testado em duas fases: primeiramente será avaliado por professores de Matemática, mestrandos do PROFMAT, e em seguida, será testado pelos alunos, com acompanhamento de seus professores.

Para facilitar sua difusão entre os professores prevê-se sua disponibilização em repositórios digitais, para isso serão tomados os procedimentos para licenciamento *Creative Commons*, e sua publicação em um repositório digital de acesso livre como o Banco Internacional de Objetos de Ensino (BIOE)[3].

References

Advanced distributed learning (adl). scorm 2004 4o. edition content aggregation model (cam) version 1.1. `http://www.adlnet.gov`. Acesso em julho de 2014.

[3]http://objetoseducacionais2.mec.gov.br/

Advanced distributed learning (adl). scorm 2004 4o. edition run-time environment (rte) version 1.1. http://www.adlnet.gov. Acesso em julho de 2014.

Advanced distributed learning (adl). scorm 2004 4o. edition sequencing and navigation (sn) version 1.1. http://www.adlnet.gov. Acesso em julho de 2014.

Adobe. Adobe captivate. http://www.adobe.com/br/products/captivate.html. Acesso em julho de 2014.

Adobe. Adobe dreamweaver cs6. http://www.adobe.com/br/products/dreamweaver.html. Acesso em julho de 2014.

Adobe. Adobe flash professional cs6. http://www.adobe.com/br/products/flash.html. Acesso em julho de 2014.

W3C. Html5. http://www.w3.org/TR/html5/. Acesso em julho de 2014.

W3C. Xml. http://www.w3.org/standards/xml/. Acesso em julho de 2014.