CriptoMat2: ensinando Matemática utilizando conceitos de Criptografia - em bloco e RSA

Bruno José da Silva Batista[1], **Paulo Eduardo da Silva Lazari** [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

{brunobatis27, pauloedulazari, carlabarvinski,

valguima.odakura, linosanabria}@gmail.com

Resumo. *A Criptografia é um recurso natural para o ensino da matemática, uma vez que os principais algoritmos criptográficos fazem uso de vários conteúdos de matemática. Sendo um tema que desperta interesse por si, permite que seja utilizado pelo professor como motivador para introdução de conceitos do conteúdo formal, como resposta aos problemas colocados pelos processos de cifragem e decifragem em diferentes técnicas criptográficas. Neste artigo é apresentado o CriptoMat2, um aplicativo que utiliza cifragem em bloco e RSA, o qual foi idealizado como instrumento de apoio para o professor, facilitando a experimentação antes da formalização de conceitos. O CriptoMat2 foi desenvolvido em 4 módulos independentes, para uso por alunos e professores do ensino médio e superior.*

1. Introdução

A Matemática é a ferramenta mais utilizada nas implementações de sistemas criptográficos, logo uma pode se tornar instrumento de aprendizado para a outra: a criptografia pode despertar o interesse do aluno pela matemática, enquanto que ao estudante de computação se faz necessário compreender os problemas e conceitos que são frequentes nos algoritmos de criptografia. Em ambos os casos é preciso estabelecer uma estratégia de abordagem, na qual não se deve apenas apresentar o "como funciona", mas também o "quando não funciona", para que o aprendiz possa discutir o "por que funciona". Com esse propósito em mente o aplicativo CriptoMat2 foi preparado: para que o professor possa guiar os alunos a problemas como solução de sistemas de equações modulares, matrizes invertíveis, funções injetivas, entre outros conceitos matemáticos.

Neste artigo é apresentado o aplicativo CriptoMat2[1], em que a criptografia é o fio condutor que liga os conceitos de matemática ao processo de cifragem. O CriptoMat2 faz parte de um projeto denominado CriptoMat, o qual visa o desenvolvimento de módulos de Objetos de Aprendizagem que correlacionam Criptografia e Matemática. O principal objetivo do CriptoMat2 é sua aplicação, como instrumento de apoio em sala de aula, em escolas de ensino médio e universidades, por alunos do Mestrado Profissional em Matemática (PROFMAT), ofertado pela Universidade Federal da Grande Dourados (UFGD).

[1]CriptoMat2 Disponível em: http://ivitu.com.br/criptomat/criptomat2/

O aplicativo CriptoMat2 é composto de 4 módulos independentes que conceituam, exemplificam e permitem ao aprendiz, a realização de operações com criptografia em bloco e RSA, proporcionando ao aprendiz uma reflexão sobre os conceitos matemáticos envolvidos em sua operacionalização.

O aplicativo é compativel com Ambientes Virtuais de Aprendizado (AVA) tais como Moodle[2], podendo também ser executado nos mais diferentes navegadores. O CriptoMat2 tem como público alvo alunos do Ensino Médio e de Graduação. No primeiro caso serve de material de apoio para professores de matemática. No segundo 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 CriptoMat2. Na seção 3 o aplicativo CriptoMat2 é apresentado. Por fim, na seção 4, as considerações finais são descritas.

2. Processo de desenvolvimento

O processo de desenvolvimento do CriptoMat2 compreendeu as fases de planejamento didático-pedagógico, estudo e definição de tecnologias adequadas ao projeto, seleção de ferramentas para a implementação, prototipação e implementação. Para esse trabalho foram construídas mídias digitais voltadas para o ensino de criptografia aplicando o conceito de objeto de aprendizagem, pois permite o reuso, interoperabilidade, portabilidade, etc.

As aplicações foram desenvolvidas para a plataforma Web, para serem visualizadas em um navegador Web ou em um AVA. Os objetos de aprendizagem do CriptoMat2 foram desenvolvidos utilizando a ferramenta Adobe Captivate versão 7.0 do pacote Adobe eLearning Suite 7.0 [Adobe a], que tem como principal objetivo o desenvolvimento de simulações de aplicações, vídeo-aulas e animações, os quais são recursos frequentemente utilizados na criação de objetos de aprendizagem.

Os objetos de aprendizagem foram desenvolvidos utilizando basicamente HTML5 [W3C a] e Javascript, imagens, e animações utilizando a tecnologia Flash [Adobe c]. Os arquivos de metadados são apresentados através da tecnologia XML [W3C b].

Os módulos do CriptoMat2 foram implementados usando a coleção de padrões para desenvolvimento de objetos de aprendizagem *Sharable Content Object Reference Model* (SCORM) [SCO a], [SCO b], [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 objetos de aprendizagem em ambientes virtuais de ensino, garantindo as propriedades básicas

[2]Moodle Disponível em: https://moodle.org/

dos objetos de aprendizagem, como: adaptabilidade, durabilidade, reusabilidade, dentre outras. A adoção do SCORM favorece o compartilhamento do objeto de aprendizagem, bem como 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 e aplicação dos padrões nos objetos de aprendizado.

3. CriptoMat2

O aplicativo Criptomat2 ao todo é composto de 4 módulos independentes que conceituam, exemplificam e permitem ao aprendiz, a realização de operações de cifragem-decifragem da de criptografia em bloco e RSA, proporcionando uma reflexão sobre os conceitos matemáticos envolvidos em sua operacionalização. Nessa seção são apresentados os quatro módulos do CriptoMat2, nomeados de módulos 6 ao 8.

Os modulos do CritpoMat2 podem ser acessados através do endereço `http://ivitu.com.br/criptomat/criptomat2`

3.1. Módulo 6: Criptografia em bloco

Esse módulo aborda a criptografia em bloco. Nele a multiplicação de matrizes 2×2 é a base para a explanação dos conceitos de cifragem em bloco, a qual é realizada por uma animação conforme ilustra a Figura 1.

3.2. Módulo 7: Praticando criptografia em bloco

Nesse módulo, o aluno aplica os conceitos aprendidos no módulo anterior e realiza atividades práticas de cifragem em bloco. A interação disponibilizada pelo aplicativo permite que aluno compreenda a importância de matrizes em operações de criptografia em bloco. Além disso, o aplicativo permite 456.976 combinações diferentes de matrizes, módulo 26, o que corrresponde a 26^4 (vinte e seis elevado a 4 potência). Desse total, apenas as matrizes cujo determinante não tenham fator comum com 26, isto é, cujo determinante não seja par ou igual a 13, permitem o bom funcionamento do processo de cifragem e decifragem. Quando o aprendiz faz uma boa escolha, o módulo sugere o teste com uma matriz que não tenha a propriedade acima descrita, e reciprocamente, quando o aprendiz faz uma escolha ruim o módulo sugere uma matriz que satisfaça a condição. Assim, o aprendiz pode confrontar as situações investigando as razões do sucesso e do fracasso. Ainda, no caso de uma matriz que não preenche o requisito, o módulo sugere uma frase para que o aprendiz perceba que a encriptação tem falhas.

No roteiro para uso em sala, o professor pode discutir qual o número de elementos da imagem inversa de um bloco, nos casos em que a matriz não é invertível. Para responder, o aprendiz, através da experimentação com o aplicativo, poderá fazer conjecturas que

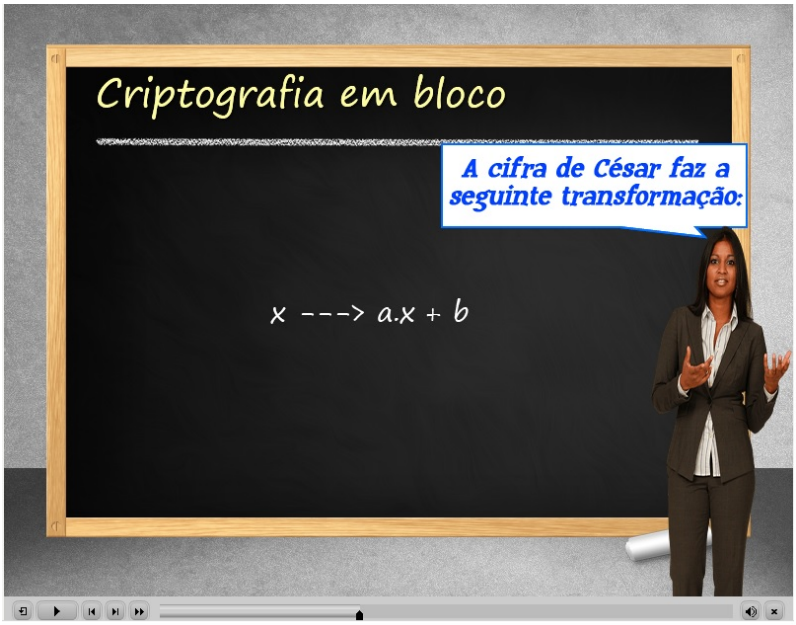

Figure 1. Módulo 6: Conceituando criptografia em bloco.

o professor utilizará como ponto de partida para os conceitos matemáticos envolvidos, motivando o estudante a ampliar o conhecimento sobre o tema.

Após realizar a cifragem e decifragem, ao clicar em "Mostrar" o usuário pode observar a matriz inversa da matriz de entrada, bem como o mapa de substituição. A Figura 2 ilustra a tela inicial do módulo, que tem espaço para o usuário escolher valores para a matriz 2×2 e depois acompanhar a cifragem e a decifragem de mensagens.

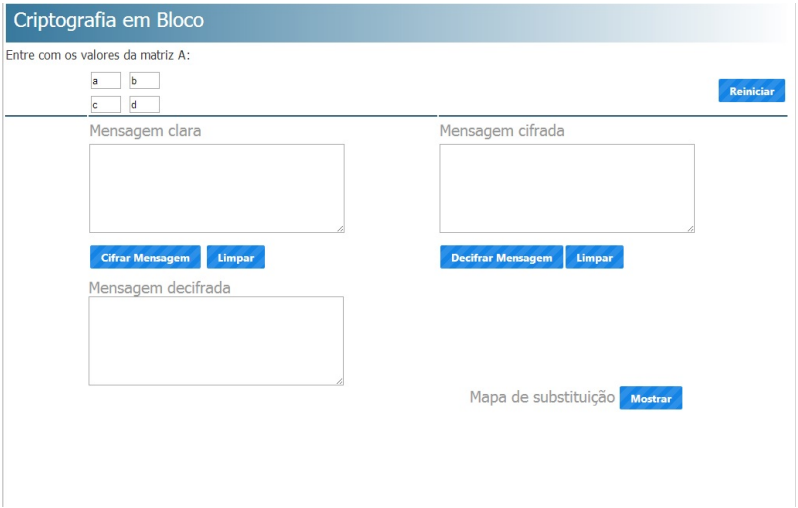

Figure 2. Módulo 7: Praticando criptografia em bloco.

3.3. Módulo 8: Criptografia RSA

No Módulo 8 os conceitos da criptografia RSA, chaves públicas e privadas e sua relação com números primos, são apresentados por um avatar feminino conforme ilustra a Figura 3.

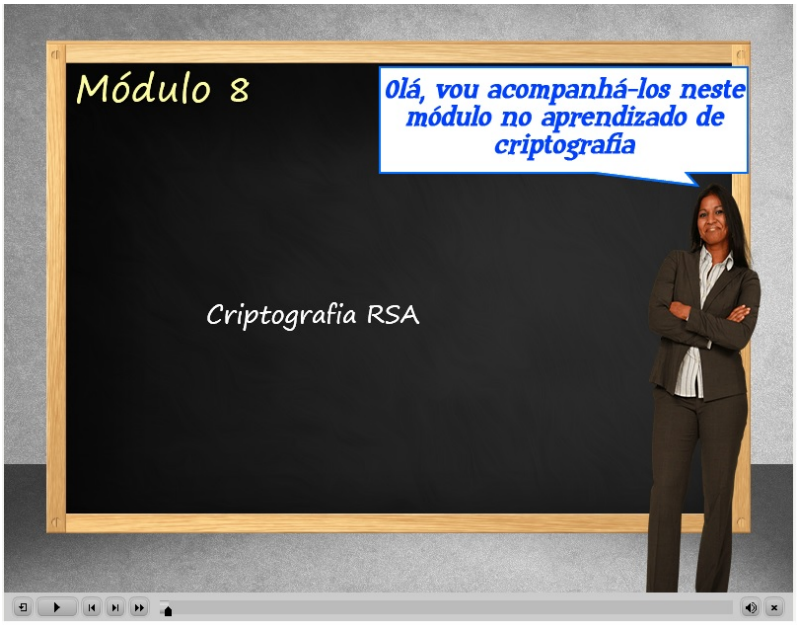

Figure 3. Módulo 8: Conceituando criptografia RSA.

Os conceitos apresentados nesse módulo são base para o desenvolvimento das atividades práticas do módulo subsequente.

3.4. Módulo 9: Praticando criptografia RSA

Este módulo propicia experimentações com a criptografia RSA. Na atual versão, a criptografia funciona somente para números primos pequenos, havendo a necessidade da participação intensiva do professor na explicitação das razões pelas quais as transformações são injetivas, bem como na orientação do desenvolvimento das atividades de cifragem e decifragem. O módulo permite que o aluno escolha números primos para realizar a cifragem e decifragem com o algoritmo RSA e observe o resultado obtido ao clicar em "Mostrar" conforme ilustra a Figura 4.

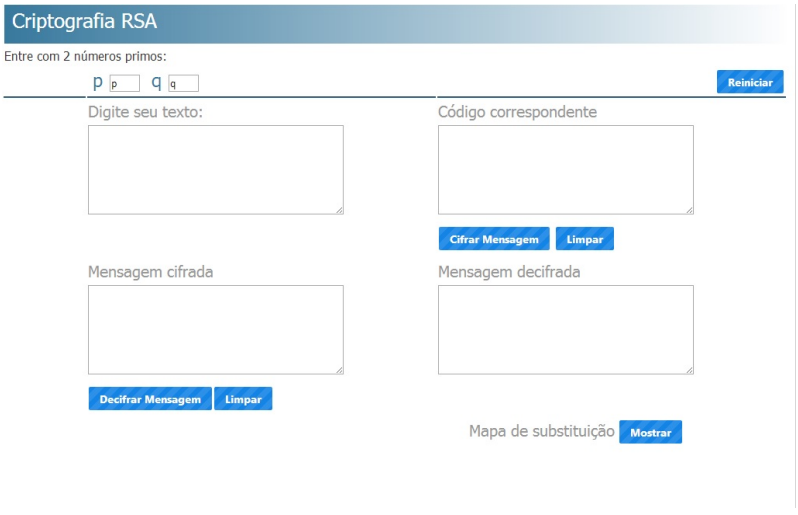

Figure 4. Módulo 9: Praticando criptografia RSA.

4. Considerações finais

Está em andamento uma pesquisa avaliativa dessa primeira versão por um grupo de professores do ensino médio, alunos do PROFMAT, para que esses indiquem se a mesma está adequada ao que se propõe, alem de apresentar sugestões para que melhorias sejam feitas tanto do ponto de vista do uso quanto do ponto de vista didático.

Futuramente, como extensões deste trabalho, podem ser realizadas pesquisas de campo em sala de aula para que alunos e professores avaliem a utilização destes objetos de aprendizagem nas atividades de ensino e aprendizagem, bem como podem ser elaboradas novas versões e outros objetos de aprendizagem com novos temas voltados à criptografia para atingir novos públicos.

Além disso, 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.

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.

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