A MATEMÁTICA A SERVIÇO DA SOCIEDADE: CRIPTOGRAFIA E SEGURANÇA

Igor Bruno Maciel de Souza[1]; Arthur Giovane Campos Batista[2]; Lílian Isabel Ferreira Amorim[3]; Celimar Reijane Alves Damasceno Paiva[4]

Resumo: A proposta dessa pesquisa foi oportunizar aos acadêmicos dos cursos de Licenciatura em Matemática e Tecnologia em Análise e Desenvolvimento de Sistemas (TADS) uma aprendizagem acerca de Criptografia, oferecendo-lhes uma visão da Matemática aplicada e o entendimento a respeito dos algoritmos de criptografia utilizados atualmente, ou seja, a dificuldade de sua decodificação, associada a Matemática envolvida na sua criação. Para tanto, um estudo sobre criptografia foi realizado, os conhecimentos adquiridos foram usados na construção de um material didático que foi utilizado para ministrar um minicurso cujo foco foi o estudo das ferramentas matemáticas usadas em algoritmos de criptografia e a apresentação do software Gpg4Win. Ao final desse trabalho percebeu-se que os acadêmicos conseguiram compreender a partir do estudo sobre criptografia a existência de uma conexão entre a Matemática e a Computação.

Palavras–chave: Criptografia. Aritmética Modular. Matemática Aplicada.

Introdução

Diante da realidade de espionagem internacional e da falta de segurança e privacidade nos meios públicos de comunicação, um assunto que vem à tona é a Criptografia. Atualmente ela está diretamente relacionada à segurança do sistema bancário, do sistema das compras via internet, do sistema de e-mails e a segurança dos agentes do governo. E ao longo do tempo essa ciência foi se desenvolvendo e seus métodos de criptografar foram sendo modificados de modo a ganhar mais segurança, são basicamente dois tipos de cifras: simétricas e assimétricas. As cifras simétricas são aquelas que utilizam apenas uma chave para codificar e para decodificar, enquanto as cifras assimétricas utilizam duas chaves, uma para codificar e outra para decodificar. BARBOSA, L.A.M et al, 2003, entendem o ato de criptografar como a ação de pegar uma mensagem e embaralhar os dados, usando uma senha especial que é o que se chama de chave, de forma que a saída não faça sentido aparente a quem deseja decifrar essa mensagem. Este estudo propõe um elo entre as áreas: Matemática e Computação, ambas responsáveis pelo desenvolvimento da

1 Acadêmico do curso de Licenciatura em Matemática do IFNMG, Campus Januária. Bolsista de Iniciação Científica do PIBIC. Email: igorbruno155@yahoo.com.br

2 Estudante do curso técnico em Informática para Internet do IFNMG, Campus Januária. Bolsista de Iniciação Científica da FAPEMIG. Email: arthurgiovanecb@gmail.com

3 Docente do IFNMG, Campus Januária. Curso de Licenciatura em Matemática. Email: lilian.amorim@ifnmg.edu.br

4 Docente do IFNMG, Campus Januária. Curso de Licenciatura em Matemática. Email: celimar.damasceno@ifnmg.edu.br

Criptografia. A primeira oferece as ferramentas necessárias para criação da própria Criptografia em si, enquanto a segunda é responsável pelo aprimoramento da mesma e pela criação dos algoritmos e das chaves de segurança cada vez mais complexas. Quando se fala em codificar uma informação, o que acontece na prática é a transformação de um texto em uma sequência numérica, a partir das chaves. Essas chaves são produzidas através de conceitos matemáticos variados, podendo ser conceitos da Álgebra Linear e da Teoria dos Números. O rigor das demonstrações matemáticas é que garante a existência das cifras e a segurança das mesmas, em especial, destaca-se o método RSA, que é o método mais utilizado atualmente. Este código foi criado em 1977 por R.L. Rivest, A. Shamir e L. Adleman. A sigla “RSA” corresponde às iniciais dos criadores do código (COUTINHO, 2005). A pesquisa propôs um estudo aprofundado sobre criptografia para que acadêmicos dos cursos de Licenciatura em Matemática e TADS pudessem ter uma visão mais ampla acerca da Matemática como ferramenta para o desenvolvimento da Criptografia.

Material e Métodos

A pesquisa foi realizada no IFNMG – campus Januária e teve como público alvo 14 acadêmicos dos cursos de Licenciatura em Matemática e TADS. Este trabalho foi realizado em três etapas. Na primeira etapa foram estudadas técnicas simples de criptografia: cifras de transposição e substituição. Na sequência as técnicas modernas: criptografia simétrica e assimétrica. Optou-se pelo algoritmo RSA cujo principal problema matemático é a fatoração de números inteiros. Para isso foi necessário o estudo dos seguintes tópicos: Algoritmo da Divisão de Euclides, Teorema Fundamental da Aritmética, Números Primos, Aritmética Modular e Teorema de Euler. Na segunda etapa foi realizado um estudo sobre criação de chaves públicas e privadas e envio de e-mails criptografados, para isso foi escolhido o software gratuito GPG4Win. Na Terceira etapa foi realizada uma pesquisa de campo com os acadêmicos já mencionados, nessa etapa foi desenvolvido um minicurso de 20h/a, onde foram socializados os estudos realizados. Ao final desse minicurso foi feita uma coleta de dados por meio de um questionário, cujo objetivo era avaliar se o objetivo dessa pesquisa foi atingido.

Resultados e Discussão

Os estudos realizados acerca de criptografia permitiram escrever o material didático que foi utilizado no minicurso. Durante o minicurso os acadêmicos tiveram a oportunidade de familiarizar com o tema criptografia, uma vez que quando questionados se tinham conhecimento acerca desse tema 50% dos participantes responderam negativamente e 50% responderam que tinham um conhecimento superficial. Quando estudaram as ferramentas matemáticas, um dos conceitos mais importantes foi a aritmética modular usada no algoritmo de criptografia RSA. Dos acadêmicos 78% disseram usar a função mod como ferramenta disponível nas linguagem de programação utilizadas por eles e os outros 22% nunca a usaram. A porcentagem de estudantes que não tinha conhecimento sobre congruência modular

foi de 93% e 7% já tinha conhecimento. Porém quando questionados sobre o significado da congruência modular usado no método RSA, 100% responderam que não tinham conhecimento. Mesmo depois do estudo da aritmética modular no minicurso, 43% responderam ter compreendido parcialmente a aplicação da congruência modular no algoritmo RSA, alegando dificuldade no entendimento da matemática envolvida e 57% compreenderam plenamente. Dos estudantes, 93% não conheciam nenhum software usado para codificar e decodificar mensagens, apenas um respondeu que conhecia o TrueCrypt. Diante da busca por segurança nos meios eletrônicos, foi questionado aos estudantes como consideravam o domínio acerca das ferramentas de criptografia nos dias atuais, 78% responderam que é necessário para todo cidadão e 22% disseram ser importante apenas para quem trabalha na área. O objetivo principal dessa pesquisa era que os acadêmicos percebessem o elo existente entre a Matemática e a Computação, 100% disseram ter conseguido perceber esse elo. Observa-se pela fala do estudante A5: “Através do minicurso ficou perceptível que a matemática e a computação estão interligadas, por trás da computação tem sempre alguma operação matemática envolvida.”

Conclusões

A Matemática não está restrita somente aos livros, mas é uma ciência viva, que é utilizada em larga escala por outras áreas do conhecimento e não como um fim em si mesmo, ela contribuiu para uma considerável evolução da criptografia quando essa assimilou os conceitos da matemática e tornou-se uma disciplina científica estudada por matemáticos, especialistas em estatística e cientistas ligados ao campo da informática. Daí a importância da disseminação desse conhecimento não só no meio acadêmico, mas para a população de forma geral, uma vez que, todos são de alguma forma reféns das tecnologias e suas vulnerabilidades.

Referências

BARBOSA, L.A.M et al. RSA Criptografia Assimétrica e Assinatura Digital. Especialização em Redes de Computadores. Universidade Estadual de Campinas, 2003

COUTINHO, Severino Collier. Números Inteiros e Criptografia RSA, 2ª edição, Rio de Janeiro: IMPA, 2005

Agradecimentos

À FAPEMIG e ao IFNMG campus Januária pelo apoio para realização dessa pesquisa.