TK042 - CRIPTOGRAFIA E NÚMEROS PRIMOS: UM NAMORO QUE DEU CERTO

CRYPTOGRAPHY AND PRIME NUMBERS: A DATING GONE RIGHT

Ivan de Oliveira Holanda Filho[1]

Faculdade Ateneu - FATE

ivanfilho@ymail.com

Ana Carolina Costa Pereira

Universidade Estadual do Ceará - UECE

carolinawx@gmail.com

Alison Sousa da Silva

Universidade Estadual do Ceará – UECE

alison.silva.90@hotmail.com

RESUMO

Desde que o homem é consciente das atividades que realiza, existe a necessidade de esconder ou mesmo omitir informações para benefício próprio. Este trabalho tratará da Criptografia, também conhecida como Ciência do Sigilo, ela foi capaz de mudar o rumo de guerras, como aconteceu nas grandes guerras mundiais ou mesmo antes, com as técnicas de criptografia usadas pelos gregos da antiguidade. Se antes ela foi vital para construir a história, hoje ela é imprescindível para prevenir fraudes em comércios eletrônicos quando utilizamos a internet, e mais do que garantir uma simples compra de produtos eletrônicos ela é fundamental para a segurança de transações bancarias. Mostraremos com isso a grandiosidade da Matemática que unida a outras Ciências poderá contribuir, e muito no avanço a modernidade.

Palavras-chave: História da Matemática; Criptografia; Aplicações.

ABSTRACT

Since man is aware of the activities carried out, there is a need to conceal or omit information for their own benefit. This research will address the encryption, also known as Science of Secrecy, that was able to change the course of wars, as happened in the world wars or even earlier, how the encryption techniques used by the ancient Greeks. If before this was vital to build the story, it is now essential to prevent fraud in electronic commerce when using the internet, and more than secure a simple purchase of electronics it is crucial for the security of banking transactions. We will show that the grandeur of Mathematics united to the other sciences can contribute a lot in the advance and the modernity.

Keywords: History of Mathematics; Encryption; Applications.

INTRODUÇÃO

Ao ouvirmos falar de Criptografia (do Grego *kryptós*: "escondido", e *gráphein*: "escrita"), pensamos em modernidade ou mesmo em uma parte específica da Computação. Mas a verdade é que a Criptografia é uma ciência que acompanha o homem há milênios. Esta ciência empregada há milênios tem sido amplamente usada com vários objetivos, desde garantir a sobrevivência de livros e manuscritos, até a segurança de dados sigilosos, como coordenadas de alvos em guerras e informações de clientes de bancos.

Durante a realização dessa pesquisa, pudemos constatar o quão importante é o emprego da criptografia, além de curioso, já que o estudo dessa ciência requer um amplo conhecimento de códigos e algoritmos, alguns inclusive de grande importância para grupos secretos e nações importantes, e também de Matemática, já que uma parte considerável se deve ao emprego dos números primos.

Este trabalho tem como objetivo principal apresentar as relações entre a Criptografia e os números primos, através de relatos históricos encontrados ao longo dessa pesquisa, além de apresentar algumas dessas aplicações que foram de grande importância no desenvolvimento da humanidade.

METODOLOGIA

A metodologia utilizada nesse trabalho foi a pesquisa bibliográfica, tendo como fonte de pesquisa artigos, livros, sites e revistas da temática. Com o levantamento de dados podemos trabalhar o que foi lido e fazer uma interpretação dos dados. É o que afirma SEVERINO (2010, pag.122).

"A pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos teses etc. Utiliza-se de dados ou de categorias teóricas já trabalhadas por outros pesquisadores e devidamente registradas. Os textos tornam-se fontes de temas a serem pesquisados. O pesquisador trabalha a partir das contribuições dos autores dos estudos analíticos constantes dos textos."

Na obtenção dos dados, verificamos que um dos primeiros registros que se tem noticia sobre o uso da Criptografia foi no Egito, datado a aproximadamente há 2000 anos A.C. Na idade média, a criptografia foi fundamental para a sobrevivência de livros, textos e documentos importantes, pois nesse período que ficou conhecido como idade

das trevas, era proibida a divulgação de manuscritos e muitos textos e livros foram traduzidos e criptografados para que não se perdesse a riqueza de informações que se tinha da época.

Ao longo dos anos a Criptografia foi largamente utilizada nas guerras mundiais, inclusive pelo exército alemão e definira um capitulo a parte na segunda guerra mundial em que os "aliados" tentavam a todo custo interceptar mensagens criptografadas e assim ganhar vantagem com as informações obtidas.

Na Europa filhos de pessoas importantes eram privados de declararem seu amor publicamente pela pessoa amada, o que fez com que muitos jovens mandassem mensagens cifradas para a pessoa amada, nas colunas de jornais locais. Isso chamou a atenção de criptoanalistas, que tentavam a todo custo decifrar tais conteúdos, seja por intermédio dos pais desses jovens seja por curiosidade própria.

Ao fazermos uma transação bancaria ou mesmo um uma compra em um site via internet. Um tipo de Criptografia em especial protege nossos dados pessoais para que outras pessoas não se beneficie com tudo isso. Esse método criptográfico usado pelas empresas e bancos chama-se Criptografia RSA. O nome da sigla RSA vem dos nomes dos idealizadores desse algoritmo: Ron Rivest, Adi Shamir e Leonard Adleman. Até então, todos os tipos de cifragem e decifragem usados até o momento eram simétrico, ou seja, tanto o emissor quanto o receptor usavam a mesma chave para cifrar e decifrar a mensagem original. Portanto ambos possuem o mesmo "conhecimento", o que não ocorre na cifra assimétrica. Um emissor pode cifrar, mas não pode decifrar a mensagem. Para decifrá-la ela deve ter acesso à chave original de decifragem, o que torna o sistema de chave assimétrica completamente novo.

Inicialmente, a Criptografia de chave publica foi proposto pela dupla Whit Diffie e Martin Hellman. Eles trouxeram uma nova abordagem ao mundo ao proporem um modo criptográfico de acesso a todos sendo por isso público tirando assim o controle absoluto das agencias dos governos. Rivest, Shamir e Adleman inicialmente lançaram um desafio em um artigo da época que despertou interesse mundial. O desafio era encontrar dois números primos que multiplicados gerasse outro número, no qual teria 129 algarismos. Logo o artigo tornou-se conhecido e o número passou a ser chamado "RSA 129". Os idealizadores do artigo cometeram um ato falho e estimaram um tempo gigantesco para que o problema fosse decifrado. No entanto, ainda sim o problema tomaria muito tempo e com tantos números primos para verificar a criptografia, a base

de números primos, passou a ser cada vez mais importante ao longo dos anos. Até mesmo matemáticos como Euler, Gauss e Fermat tiveram dificuldades no estudo e desenvolvimento sobre fatoração o que comprova que a Criptografia estaria segura até que alguém quebre o código e ache tais números. Com o tempo, a Matemática ganhou um espaço maior nas práticas experimentais e o problema da fatoração ganhou um destaque dentre os matemáticos.

A importância de gerar números primos muito grandes ganhou grande destaque no século XXI, tanto que algumas empresas davam certa quantia em dinheiro para pesquisadores e criptoanalistas gerarem números primos com mais de 150 dígitos. Esse prêmio era dado até o ano de 2007.

A grande questão, portanto, da Criptografia RSA, é a decomposição de números em fatores primos, a principio um problema simples. Se alguém conseguir encontrar uma maneira eficiente e rápida de decompor números em fatores primos, então isso viria a ser não só uma catástrofe no mundo criptográfico, mas sim bem mais do que isso. Seria uma catástrofe mundial.

RESULTADOS

Com o desenvolvimento da Computação, essa nova ciência ganha destaque. A Criptografia, juntamente com a Matemática, ganhou novas proporções no mundo moderno. Ao fazermos uma compra pela internet ou uma transação bancária, um tipo especial de Criptografia protege nossos dados pessoais para que outras pessoas não sejam beneficiadas com tudo isso.

Segundo o que se percebe, as empresas estão mais interessadas no desenvolvimento do estudo dos números primos, pois empresas, bancos e todo o comércio eletrônico dependem e depositam a sua segurança na Criptografia à base de números primos.

Não é de se espantar que empresas invistam pesado na construção de um modelo matemático, cujas bases sejam ainda mais sólidas e 100% seguras. Infelizmente esse modelo, ainda não existe, já que a Criptografia é uma ciência que ainda está em expansão.

CONCLUSÃO

A Criptografia, como foi dito anteriormente, é uma ciência bastante antiga e hoje ainda está em desenvolvimento. Foi utilizada em momentos crucias como a Segunda Guerra Mundial na obtenção de informações por parte dos aliados. Ainda nas guerras, foi destaque com os gregos e grandes imperadores, como Julio Cesar. Hoje a Criptografia serve como referência em pesquisas sobre Matemática Aplicada.

A verdade é que, desde que os homens existem, também existe a vontade de guardar informações. Governantes guardavam informações para que não caíssem em domínio público, outros escondiam informações para que não caíssem nas mãos dos inimigos e, a partir disso, a Criptografia evoluiu.

REFERÊNCIAS BIBLIOGRÁFICAS

BRAGHETTO, Luis Fernando. **RSA: Criptografia Assimétrica e Assinatura Digital.** Monografia (Especialização) – Curso de Redes de Computadores, Unicamp, Campinas, 2003.

Chave pública. Disponível em: <http://www.numaboa.com.br/criptografia/chaves>. Acesso em: 23 mai. 2012.

Cifras de Criptografia. Disponível em**:** <http://www.numaboa.com.br/criptografia/cifras>. Acesso em: 22 mai. 2012.

Criptografia. Disponível em: <http://www.numaboa.com.br/criptografia>. Acesso em: 22 mai. 2012.

DU SAUTOY, Marcus. **A Música dos números primos: a história de um problema não resolvido na matemática:** Tradução de Diego Alfaro. Rio de Janeiro, Jorge Zahar, 2007.

História da Criptografia. Disponível em: <http://www.numaboa.com.br/criptografia/historia>. Acesso em: 22 mai. 2012.

POSTAL, Tannery. **Criptografia RSA.** Monografia (Graduação) – Curso de Licenciatura em Matemática, UFMT, Cuiabá, 2008.

SEVERINO, Antonio Joaquim. **Metodologia do Trabalho Cientifico.** São Paulo, Cortez, 2010.

SING, Simon. **O livro dos códigos:** Tradução de Jorge Calife. Rio de Janeiro, Record, 2011.