INSTITUTO FEDERAL
MINAS GERAIS
Campus Ouro Branco

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
CAMPUS OURO BRANCO
COORDENAÇÃO DE EXTENSÃO
Rua Afonso Sardinha, nº 90 – Pioneiros. Ouro Branco, MG. CEP: 36.420-000
Tel.: (31) 3742-2149

PROGRAMA INSTITUCIONAL DE BOLSAS DE EXTENSÃO

IFMG - CÂMPUS OURO BRANCO

A CRIPTOGRAFIA NUMA PERSPECTIVA HISTÓRICA, MATEMÁTICA E COMPUTACIONAL

Autor: Thiago Neves Mendonça

Ouro Branco

30 de Novembro de 2015

Renovação de Projeto?

( ) Sim (X) Não

RESUMO

O presente projeto se trata de uma aplicação da Matemática no ramo da Informática: a Criptografia. Nele, estratégias de ensino, bem como uma alternativa diferenciada para a abordagem da Matemática estão presentes. Seu principal objetivo é levar o conhecimento de Informática e a Matemática que ali se encontra aos alunos da rede pública de ensino da cidade de Ouro Branco, em Minas Gerais. Além de mostrar a aplicação da Matemática na Informática, explicitando os tópicos matemáticos presentes nas diversas formas de criptografias, esse projeto também visa levar aos alunos conhecimento histórico sobre a criptografia. Levando o aluno a vivenciar essas ideias, o projeto também objetiva aproximar o aluno com ferramentas que lhes proporcionem uma melhor relação com a Matemática ensinada na sala de aula, bem como lhes motivem a estudarem mais sobre informática, e quem sabe seguir carreira nessa área. Tendo em vista que o ensino de Matemática se encontra defasado e com problemas questionados por diversos pesquisadores da área da Educação, esse projeto também visa levar aos alunos essa aplicação com intuito de fazer com que eles pensem numa nova Matemática, num novo ensino dessa disciplina e de sua importância em diversas áreas, em especial na informática que propomos. Por fim, com uma avaliação de todas as atividades exercidas, no projeto detalhadas, pretende-se perceber se os objetivos foram alcançados e criar estratégias para que o mesmo possa ser aprimorado e executado em outras edições e com outros alunos envolvidos.

1 - INTRODUÇÃO

1.1. Caracterização do Problema

Nas escolas, a disciplina de Matemática é abordada, ainda, de forma tradicional, sem muita aplicação e sem despertar o interesse de grande parte dos alunos. Além disso, o ensino de Matemática também enfrenta problemas tais como falta de professores, falta de qualificação e de formação continuada dos professores que já atuam na rede, entre outros.

Essa forma de ensinar a Matemática tem sido criticada por diversos autores da Educação Matemática, como D'Ambrósio, Skovsmose, entre outros. Há uma dificuldade de relacionar, ainda hoje, o que é ensinado ao uso prático e com isso o desinteresse e a falta de estímulo dos alunos se torna nítida.

Buscando alternativas para melhorar as estratégias de ensino de Matemática, o projeto propõe uma aplicação da matemática no ramo da informática, a Criptografia. A proposta é para despertar o interesse nos alunos em relação ao conteúdo de Matemática, tendo contato com uma aplicação utilizada sempre, porém sem muito conhecimento. Internet, senhas de banco, códigos de barra, todos intimamente relacionados com a criptografia.

1.2. Caracterização da Região onde será desenvolvido o programa/projeto

O projeto será aplicado na cidade de Ouro Branco, em Minas Gerais. Na cidade, existem cursos técnicos em Informática, e curso de Licenciatura em Computação no Instituto Federal de Minas Gerais. Nesse aspecto, se observa o aumento da demanda de conhecimentos, no nível técnico principalmente, da área de informática.

O projeto levará para as escolas ferramentas matemáticas e da informática para, além de mostrar a relação entre elas, aumentar a gama de conhecimento dessas áreas, dando suporte para alunos que futuramente optem por cursos voltados para a informática numa universidade, ou em cursos técnicos.

1.3. Justificativa

A criptografia é a arte e ciência de fabricar códigos secretos. De maneira mais precisa, é o estudo das técnicas pelas quais uma informação pode ser modificada de forma a ficar oculta, ininteligível, salvo para o destinatário de direito da mensagem. Portanto a função da criptografia é de proteger uma informação. A palavra deriva do grego Kryptós, "escondido", e gráphein, "escrita". (FIGUEIREDO, 2012)

Antigamente, a criptografia era utilizada pelo governo apenas, para guardarem em sigilo suas informações e ninguém mais ter acesso. Atualmente, além do governo, as empresas e as pessoas que precisam de proteção utilizam de criptografia, em senhas, internet, bancos, etc. Um sistema de criptografia utilizado, e conhecido, é o "SWIFT" que faz com que as transações

internacionais se tornem mais seguras, impedindo o acesso de terceiros em informações importantes.

De acordo com Stallings (2004), atualmente a criptografia vai além da função de gerar privacidade na troca de informações. Ela também tem a função de Autentificar: confirmar que certa informação é verdadeira; Irretratabilidade: alguém envia uma informação e depois se nega dizendo que não a enviou (ou alguém se negar dizendo que não recebeu); Integridade: garantir que a mensagem não foi modificada durante seu envio.

Segundo Singh (2011), os primeiros relatos sobre proteção de alguma informação foram narrados por Heródoto, "o pai da história". O mecanismo era utilizado no conflito entre Grécia e Pérsia – 480 a.C. Xerxes (o rei dos Persas) planeja atacar a Grécia e Demarato (grego) transmitia as mensagens de alerta em segurança (raspava a cera de uma tabuleta, escrevia e depois encobria) utilizando a esteganografia: esconder a mensagem. Assim, a vantagem da criptografia sobre a esteganografia é que, se o inimigo interceptar a mensagem ela estará codificada, logo será ininteligível e seu conteúdo não será revelado. Atualmente, em alguns casos, se usa uma combinação das duas afim de oferecer mais segurança (STALLINGS, 2004).

A Citale Espartano é um dos primeiros aparelhos criptográficos que se tem conhecimento, que data do século V antes de Cristo (FIGUEIREDO, 2012b).

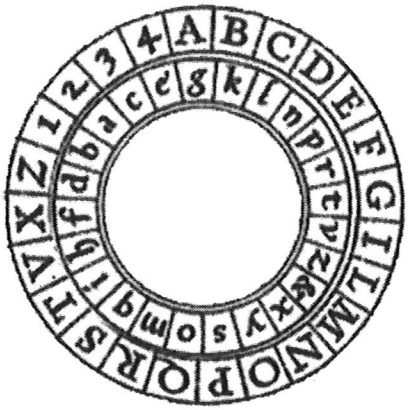
O primeiro documento que usou uma cifra de substituição para propósito militar foi feito Imperador Júlio César. A cifra de César, como ficou conhecida, consiste em deslocar as letras do texto claro em 3 casa para direita, sendo portanto uma cifra de substituição.

Com o avanço da tecnologia, surge então a criptoanálise que é a ciência que estuda as técnicas para obtenção da informação sobre a mensagem original, a partir do texto cifrado. São as técnicas usadas para se "quebrar" a mensagem cifrada. Pelo surgimento desse estudo, as cirfras monoalfabéticas passam a ser polialfabéticas, para dificultar o estudo e a possibilidade de quebrar a chave de codificação.

O surgimento da criptoanálise foi um grande avanço na história da criptografia. O próximo passo ocorre na Europa durante a renascença, onde o italiano Leon Battista Alberti cria a cifra poliafabética (LOUREIRO, 2014).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
CAMPUS OURO BRANCO
COORDENAÇÃO DE EXTENSÃO
Rua Afonso Sardinha, nº 90 – Pioneiros. Ouro Branco, MG. CEP: 36.420-000
Tel.: (31) 3742-2149

Alberti propõe o uso de dois alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial. Ele também foi um dos primeiros a projetar e usar um dispositivo que facilitava o processo criptográfico. Este dispositivo ficou conhecido como Disco de Alberti



De acordo com Singh (2011), a partir do trabalho de Alberti e de outros que também contribuíram, como Johannes Tritheminus e Giovani Porta, o diplomata francês Blaise Vigenère desenvolve a cifra polialfabética: Cifra de Vigenère. Ele trabalha com uma tabela que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocando ciclicamente do anterior para uma posição e uma chave para cifrar e decifrar a mensagem.

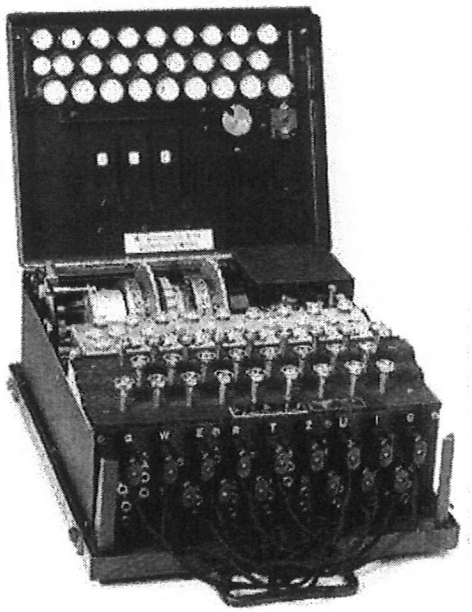
Esse tipo de cifra é "imune" à análise de frequência e possui um número grande de possíveis chaves. Isso fez com que a cifra ficasse conhecida como "le chiffre indechiffrable" (a cifra indecifravél). O próximo passo foi dado por Friedrich Kasiski – 1863 que publicou o livro: "Die Geheimschriften und die Dechiffrierkunst" (Escrita secreta e a arte da decifragem) que relata o primeiro método para quebrar as cifras polialfabéticas (SINGH, 2011). O método ficou conhecido como Exame de Kasiski. A fraqueza observada por Kasiski é que a chave se repete, e isso facilitaria o ataque dos criptoanalistas.

De forma independente, o matemático inglês Charles Babbage, também conseguiu quebrar a cifra de Vigenère, inclusive antes de Kasiski mas foi forçado a manter silêncio pelo governo inglês e não pode publicar a sua descoberta. Só foi revelado pelo governo inglês a descoberta de Babbage em 1887, 24 anos depois da descoberta de Kasiski (SINGH, 2011).

Um fato interessante foi a criação da Máquina "Enigma" que é um divisor de águas entre a criptografia clássica e a moderna, antes e depois da existência do computador.

Os amigos "Scherbius & Ritter" (Richard Ritter) comandavam empresas de diversas áreas e numa delas existia um projeto de substituir os sistemas de criptografia inadequados, usados na

Primeira Guerra Mundial, trocando-se as cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. Nessa busca, eles desenvolveram uma máquina criptográfica que era, basicamente, uma versão elétrica do disco de cifras de Alberti. Chamada de Enigma, a invenção de Scherbius se tornaria uma peça fundamental para o surgimento dos primeiros computadores (SINGH, 2011).



A máquina Enigma era composta de um teclado usado para digitar as letras do texto claro, uma unidade misturadora, que cifra cada letra, transformando-a na letra correspondente da mensagem cifrada, e um mostrador consistindo em várias lâmpadas para identificar as letras do texto cifrado. O coração da enigma era os misturadores. A tradicional usava três misturadores, tendo cada misturador 26 posições possíveis. A posição inicial dos misturadores dentro da câmara formavam a chave da cifra. Era usada em todos os níveis do governo e os alemães estavam seguros de que haviam criado uma máquina indecifrável.

Segundo Singh (2011), o trabalho começou com o matemático polonês Marian Rejewski, que se baseou em textos cifrados interceptados e em uma lista de três meses de chaves diárias, obtidas através do serviço de espionagem francês.

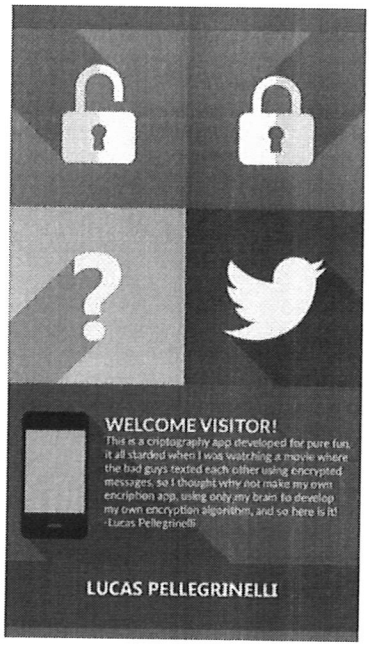
As contribuições de Rejewki foram muito importante apesar de não conclusivas. Seu trabalho continuou e foi concluído com sucesso pela equipe inglesa liderada por Alan Turing e outros, em Bletchey Park, na Inglaterra. (LOUREIRO, 2014). Desenvolveram dois tipos de máquina para manipular as cifras interceptadas: Bomba e Colossus (precursora dos modernos computadores) (LOUREIRO, 2014). A dificuldade encontrada para quebrar a chave era que os alemães mudavam regularmente a configuração da Enigma. Além das chaves com validade mensal, mudanças contínuas foram implementadas, com destaque para o acréscimo de mais dois misturadores, incrementando, de modo impressionante, o número de chaves possíveis. A máquina Enigma foi um grande avanço para o mundo da criptografia. O próximo avanço é o

desenvolvimento da criptografia de chave pública e do RSA.

Os tópicos de Criptografia aplicados na Matemática do Ensino Médio são os que seguem na tabela abaixo:

Criptogramas	Conteúdos de Aritmética
Código ISBS	Aritmética Modular
Cifra de Substituição	Função Linear; quadrática Imagem de Função; Cálculo da função inversa
Cifra de Substituição	Potenciação; Equações exponenciais; Logaritmo
Cifra de Hill	Matrizes; Multiplicação de Matrizes; Operações com Matrizes; Matriz Inversa
RSA	Aritmética Modular; Números Primos
ECC	Curvas Elípticas; Corpos Finitos

Com intuito de uma aplicação sobre criptografia, o aluno que será indicado como bolsista desse projeto desenvolveu o aplicativo seguinte que codifica e decodifica mensagens, e que poderá, com o tempo, ser implementado e apresentado à toda a comunidade de Ouro Branco.



2 - PÚBLICO ALVO

O projeto é destinado aos alunos do ensino Médio das escolas públicas de Ouro Branco, pois os conteúdos abordados para criptografia são conteúdos presentes nesse nível de ensino. Será escolhida uma escola e nela as turmas que o projeto será realizado, em conformidade com a instituição de ensino e com o próprio IFMG.

3 - OBJETIVOS

3.1. Objetivo Geral

Além de trazer para a área de Matemática uma aplicação na informática, interessante por sinal, o objetivo do projeto é fornecer ferramentas para os alunos que se interessam pela informática, e também contribuir para o ensino e a aprendizagem de Matemática nos tópicos abordados.

Objetiva-se ainda fazer com que a disciplina de Matemática seja mais "palpável" e mais aplicada, com o intuito de levar os alunos a experimentarem uma Matemática diferente da fornecida nas aulas tradicionais.

3.2. Objetivos Específicos

Com o presente projeto, os objetivos específicos que se espera alcançar são:

1 – Aprimorar técnicas matemáticas e de informática;

2 – Levar o estudo para os alunos das escolas públicas de Ouro Branco;

3 – Realizar atividades lúdicas, oficinas, aulas, que relacionem a Matemática e a Criptografia apresentando assim a aplicação de conteúdos matemáticos já estudados no Ensino Médio;

4 – Apresentar e implementar o aplicativo de codificar e decodificar códigos;

5 – Levar os alunos a se aproximarem dos conteúdos Matemáticos através da Criptografia, de forma que percebam sua importância nessa aplicação;

6 – Levar aos alunos a reflexão sobre a importância do conteúdo de Matemática no ensino;

4 - PLANO DE TRABALHO

Para fazer o estudo dos conteúdos de Matemática na criptografia, faremos encontros e conversas para discutirmos os textos, artigos e dissertações, que se relacionam com o tema. Esses encontros serão presenciais, de forma a ficar mais claro o direcionamento de estudo. Caso não seja possível, orientações online serão dadas (período de férias, por exemplo).

Após o estudo, iremos elaborar atividades, oficinas, palestras, aulas de forma mais lúdica, diferente da tradicional, de forma a apresentar para os alunos o estudo realizado sobre a criptografia numa perspectiva histórica e teórica. Este passo também contribuirá para o cumprimento do próximo objetivo, por serem intimamente relacionados.

Após o estudo dos aplicativos, e a implementação do mesmo, o ideal será levar para os alunos na escola o aplicativo em si e colocá-lo para funcionar, em seguida explicar-se-á o método de construção, de forma mais simplificada e sem muitos detalhes, para que os alunos das escolas tenham contato com o princípio de programação.

Com um tempo de contato com a criptografia e tendo conhecimento de alguns métodos básicos de criptografar, pretende-se levar aos alunos, através de aulas, atividades e oficinas, a

Modalidade: (X) PIBEX JR ( ) PIBEX

ATIVIDADE A SER DESENVOLVIDA	MESES											
	1	2	3	4	5	6	7	8	9	10	11	12
Levantamento de obras relacionadas à Matemática na Criptografia	X	X	X	X	X	X						
Revisão de Literatura		X	X	X	X	X						
Estudo aprofundado da Matemática presente em algumas áreas da Criptografia		X	X	X	X	X						
Estudo de criação e aperfeiçoamento de aplicativos			X	X	X	X						
Escolha do local de aplicação do projeto – Conhecimento de campo				X	X	X						
Oficinas, palestras, aulas expositivas e lúdicas, confecção de materiais					X	X	X	X	X	X	X	
Utilização e apresentação do aplicativo						X	X	X	X	X	X	
Participação em congressos e encontros							X	X	X	X	X	
Elaboração de artigos, textos e outros							X	X	X	X	X	
Coleta de dados e entrevistas										X	X	
Considerações finais											X	X

Marque com um X nas células para preencher o cronograma.

10 – REFERÊNCIAS

FIGUEIREDO, L. M., **O que é criptografia**. 2012. Disponível em: <www.labcas.uff.br/criptografia>.

FIGUEIREDO, L. M., **Introdução a criptografia.** Disponível em: <www.labcas.uff.br/criptografia>.

LOUREIRO, F, O., **Tópicos de Criptografia para o ensino médio**, Dissertação de mestrado apresentada para a Universidade Estadual do Norte Fluminense Darcy Ribeiro, Campos dos Goytacazes – RJ, 2014.

SINGH, S., **O Livro dos Codigos**. São Paulo, SP: Editora Record, 2011. 446 p.

STALLINGS, W., **Criptografia e Segurança de Redes.** São Paulo, SP: Editora Pearson, 2004. 492 p.