O uso da criptografia no ensino de Matemática

Daiane de **Oliveira**
Universidade de Passo Fundo/RS
Brasil
84855@upf.br
Rosana Maria Luvezute **Kripka**
Universidade de Passo Fundo/RS
Brasil
rkripka@upf.br

Resumo

A busca de segurança em situações de troca de informações impulsionou a criação e uso de métodos de criptografia de forma confiável e segura. No decorrer da história a Criptografia foi decisiva, influenciando inclusive resultados das guerras. Assim, o presente trabalho tem como objetivo abordar conceitos gerais sobre Criptografia, onde são apresentadas as origens e acontecimentos históricos, buscando salientar as contribuições de diversos matemáticos, que foram possíveis devido aos seus conhecimentos prévios de técnicas e habilidades, tanto de métodos e algoritmos de criptografia, como na criptoanálise. Além disso, são apresentados três métodos que podem ser utilizados no ensino de matemática como exemplos de aplicação no ensino médio. Acredita-se que por ser interessante e por possibilitar a aplicação de diversos conceitos matemáticos seu uso, em situações problema, possa estimular o aluno, facilitando o processo ensino aprendizagem de matemática.

Palavras chave: educação, matemática, ensino, aprendizagem, criptografia.

Introdução

O conceito de criptografia surgiu da necessidade de se enviar mensagens com segurança entre aliados de guerras, tendo em vista que muitas informações importantes deviam ser mantidas em segredo. Assim, suas características e procedimentos descrevem como alguns matemáticos conseguiram desenvolver e decifrar sistemas de códigos secretos, encontrando informações sobre o inimigo ou escondendo tais informações.

Hoje em dia, a vida se tornou um pouco mais prática por intermédio da internet, pois as pessoas não precisam sair de suas casas para realizar atividades que exigem sigilo de informações, tais como consultar um extrato bancário ou realizar o pagamento de contas, devido

a facilidade, praticidade e segurança no envio de informações, principal característica da Criptografia.

Dessa forma, apresenta-se um breve resumo sobre a história da Criptografia, com a finalidade de entender sua utilidade ao longo da história e de buscar esclarecer conceitos, características e experimentos utilizados por ela. Também são apresentadas atividades para serem desenvolvidas em sala de aula, onde se busca aplicar conceitos de criptografia no ensino de matemática, utilizando-a como uma ferramenta facilitadora na aprendizagem de matemática.

Fundamentação teórica

Desde a antiguidade, por motivos diversos, as pessoas necessitavam de privacidade na transmissão de mensagens e era preciso encontrar uma forma de disfarçar as informações sem que elas fossem descobertas, como, por exemplo, os meios de comunicação entre aliados de guerra. Assim, foi criada a criptografia, que ao utilizar métodos de codificação de informações, têm por objetivo possibilitar que somente o emissor e receptor consigam interpretar as informações, dificultando que eventuais intrusos possam desvendar a mensagem transmitida.

A necessidade de manter informações em segredo possibilitou a criação de diferentes métodos de criptografia. Sabe-se que alguns matemáticos também influenciaram o seu conhecimento e aplicação, em diversas situações, com objetivo de despistar as pessoas que pretendiam desvendar as mensagens criptografadas.

Hoje em dia a tecnologia da Criptografia, após anos de aprimoramento, é amplamente utilizada na proteção de dados sigilosos, seja de cunho pessoal ou profissional, através da ciência da computação e de seus recursos, onde é possível transmitir uma grande quantidade de dados de maneira extremamente rápida e segura, tendo em vista o conforto e segurança para pessoas que se utilizam de tais recursos.

Alecrim (2005, p.1) explica que o surgimento da palavra Criptografia ocorreu com a união de palavras, em grego, ““Kryptós” e “gráphein”, que significam “oculto” e “escrever”, respectivamente”.

Segundo Coutinho: “A *criptografia* estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos ‘códigos secretos.’” (2008, p.1).

Inicialmente seus procedimentos não exigiam grandes conhecimentos de matemática, sendo utilizados métodos simples, como por exemplo, a substituição de letras através de símbolos, por procedimentos de contagem, ou simplesmente por números.

O pensamento estimulado e moldado do homem, através de palavras, com o passar do tempo, teve um avanço significativo com a invenção da escrita.

Existe um sistema de números em que os gregos antigos denominavam como um sistema cifrado, chamado sistema de numeração Jônico ou alfabético. Sobre este sistema, Eves comenta que: “[...] é um exemplo de sistema cifrado. Ele é decimal e emprega 27 caracteres- as 24 letras do alfabeto grego mais três outras obsoletas: *digamma, koppa e sampi*.” (2004, p.35). De acordo com o autor o mais interessante nesse proceso, criado aproximadamente em 450 a.C, é que nem todos os gregos tinham essa informação e muito menos os outros povos. Assim, o texto verdadeiro é um texto onde o sistema de códigos, por sua vez, não está relacionado com chaves criptográficas, mas sim com tabelas de substituições. Neste caso, o texto era cifrado por um

método que não tem a preocupação de dificultar a leitura da mensagem oculta. No entanto, o mecanismo para interpretar a mensagem, com o passar do tempo passou a ser decifrado e este é um artifício usado para interpretar o texto, e reconhecido como conhecemos hoje o sistema de numeração cifrada.

Dessa forma, um método antigo muito utilizado para decifrar alguns tipos de inscrições antigas consistiu na contagem de freqüência. Coutinho cita um exemplo muito conhecido "da decifração dos hieróglifos por J-F. Champollion em 1822. A chave para a decifração foi a descoberta da *pedra de Roseta*, um bloco de basalto negro que está atualmente no museu Britânico, em Londres." (COUTINHO, 2009, p.2).

Ao longo da história foram encontradas diversas mensagens codificadas simplesmente com códigos simples de letras, o que não era muito bom, pois quem enviava a mensagem poderia ter sua mensagem decifrada facilmente, podendo ser descoberto o seu segredo.

Com a evolução da humanidade foi necessário criar outros tipos de artifícios de codificação para manter as informações das mensagens em segurança. Assim, para dificultar a leitura da mensagem criptografada por pessoas não habilitadas, o aprimoramento de suas técnicas exigiu que fossem utilizados procedimentos mais elaborados, em termos de conhecimento matemático.

Ao se mandar uma mensagem criptografada, quando a mesma for recebida, existe duas alternativas de leitura: ela poderá ser decodificada ou decifrada. Quando se fala em decodificar uma mensagem, se parte do princípio que o receptor da mensagem já conhece o procedimento usado para codificação da mensagem e o usa para retirar o código, podendo desta forma obter a mensagem através da decodificação. Já a palavra decifrada é utilizada quando o receptor da mensagem codificada não é o usuário legítimo a quem ela foi enviada, sendo necessário desvendar qual foi o procedimento utilizado para codificação para somente depois utilizá-lo na decodificação (COUTINHO, 2009, p.1)

Atualmente no processo de criptografia, além do código utilizado, também são utilizadas chaves ou senhas, que se constituem em informações sigilosas e valiosas. Alecrim (2005) afirma que existem dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas. A chave simétrica é uma chave comum, pelo fato que o emissor e o receptor podem usar os dois juntos ou ao mesmo tempo a mesma chave, ou seja, só existe uma única chave que será codificada e decodificada da mensagem (ALECRIM, 2005, p. 2).

Nos anos 70 a tecnologia foi aprimorada e com o surgimento de um método moderno criptográfico, surgiram as chaves assimétricas. Uma chave é assimétrica, também chamada de chave pública, quando existem duas chaves, uma pública, utilizada para codificar as mensagens e outra chave privada (secreta), utilizada para decodificar a mensagem recebida (ALECRIM, 2005, p. 2).

A criptografia tem relação com a criptoanálise, conforme Coutinho: "A criptografia tem uma irmã gêmea na arte de decifrar códigos secretos, ou *criptoanánalise."* (2009, p.1) só que ambas tem finalidades diferentes. A criptoanálise tem por finalidade a busca de algoritmos que possibilitem decifrar a mensagem codificada.

Para decifrar novos códigos é necessário juntar conhecimentos relatados ao longo da história da criptografia, para que seja possível usá-los como ferramentas pelos criptoanalistas, de modo a facilitar o trabalho de decodificação de mensagens. Neste sentido, o conhecimento de

procedimentos utilizados anteriormente fornece pistas valiosas, com grande significado na observação e desvendamento de novos procedimentos de codificação.

Até hoje diversos algoritmos têm sido elaborados e testados, com intuito de se encontrar métodos de criptografia cada vez mais práticos e eficientes. De modo geral, no decorrer da história, os códigos, usados como meio de comunicação, foram importantes para garantir resultados positivos durante as guerras, pois eram usados em situações onde havia informações valiosas, das quais o inimigo não poderia ter conhecimento. Esse papel continua crescendo com o passar do tempo, através do avanço da tecnologia e do crescimento matemático relacionado com a Criptografia, gerado a partir da necessidade de se utilizar conhecimentos para encontrar soluções que possam trazer segurança na transmissão de informações, onde existam situações de perigo, seja no serviço de atendimentos de bancos, ou na transmissão de segredos pessoais, comerciais, militares ou industriais.

O trabalho executado pelos matemáticos torna-se fundamental, pois conforme indica Machado: “na raiz dos processos de elaboração do conhecimento não deve escapar-lhe a captação de razões pragmáticas quase subjacentes e quase nunca suficientemente explicitadas.” (1997, p. 64). Assim, naturalmente os matemáticos, devido às características de sua profissão, apresentam facilidade com a Criptografia e também com a Criptoanálise.

Com o passar anos a criptologia foi reconhecida merecidamente como ciência. Além disso, com a possibilidade de utilização de computadores cada vez mais potentes, tanto a criptografia, como a criptoanálise evoluíram (ALVARENGA, 2010, p. 229).

O autor afirma que a criptoanálise moderna tem diferenças com relação a criptoanálise clássica, pois os algoritmos usados em cada momento da criptografia se diferenciam. A criptografia antiga tinha como base as codificações nas cifras de fluxo de caracteres do próprio idioma e atualmente, os algoritmos utilizam cifras de blocos (ALVARENGA, 2010, p. 229).

Além disso, cabe ressaltar que pelo fato dos criptoanalistas resolverem diversos enigmas ao longo da história, os métodos foram disponibilizados à comunidade acadêmica, o que contribuiu para que novas pesquisas pudessem ser realizadas na área.

Assim, acredita-se que o educador possa se utilizar da história da criptografia para explicar de que forma o computador, atualmente, pode estar vulnerável na troca de informações confidenciais.

Em relação à pesquisa bibliográfica realizada, foram selecionados alguns métodos de criptografia considerados interessantes, do ponto de vista de aplicação de conceitos matemáticos, que nos possibilitaram elaborar atividades, apresentadas a seguir, com objetivo de diminuir as aulas mecânicas, de modo que a criptografia possa ser usada no ensino da matemática, como uma atividade lúdica, voltada para a aprendizagem com significado.

O uso da criptografia em sala de aula

Como a criptografia é um assunto importante e interessante no contexto atual, acredita-se que seu uso possa motivar os alunos, ajudando o professor a contornar dificuldades ao tentar estimular seus alunos, no aprendizado e conceitos relacionados com o ensino da Matemática.

Assim, a seguir são apresentadas atividades, elaboradas para serem utilizadas em sala de aula, relacionadas ao uso da criptografia no ensino de Matemática, com objetivo de

disponibilizar uma proposta alternativa, que possa ser utilizada como recurso metodológico, de forma a possibilitar que a aprendizagem da matemática seja mais interessante e significativa.

A aula pode ser iniciada com um breve histórico sobre o surgimento e evolução dos métodos de criptografia, salientando a participação de matemáticos e simpatizantes que fizeram história e suas participações no sucesso de cada método criptográfico.

Em seguida são definidas as estratégias utilizadas por três métodos, sendo, em seguida, apresentados, com detalhes, exemplos de cada método, para finalmente se propor a resolução de exercícios de aplicação de cada método criptográfico abordado.

Descrição das atividades

Inicialmente o professor pode informar que o conceito de criptografia surgiu da necessidade de se enviar mensagens com segurança, sendo que muitas informações importantes devem ser mantidas em segredo, como, por exemplo, o envio de mensagem entre aliados de guerra e também pode informar sobre o surgimento da palavra Criptografia, que ocorreu com união de palavras, em grego, ““Kryptós” e “gráphein”, que significam “oculto” e “escrever”, respectivamente”.

Também pode dizer que além da criptografia, existe a criptoanálise, que consiste na arte de decifrar códigos secretos, tendo por finalidade a busca de algoritmos que possibilitem decifrar a mensagem codificada.

Neste momento, o professor pode diferenciar os termos decodificar e decifrar, informando que a diferença entre eles seria que ao decodificar uma mensagem o receptor já conhece o código e simplesmente aplica o algoritmo para retirar o código da mensagem recebida, enquanto que para decifar uma mensagem é necessário “quebrar o código” ou seja, descobrir qual o algoritmo foi utilizado na codificação que possibilite retirar a cifra da mensagem.

Também pode informar que, ao longo da história, a necessidade de manter informações em segredo possibilitou a criação de diferentes métodos de criptografia, onde o método de César, criado em 50 a.C., é considerado um dos métodos criptográficos mais antigos que se conhece. Além disso, pode enfatizar que o processo de codificação é feito por um processo simples, que utiliza apenas as 26 letras do alfabeto, o que tornou fácil sua decifração.

Para introduzir os métodos abordados o professor também pode falar um pouco sobre o método de Vigenère, informando que foi criado em 1586 e que mensagens eram cifradas com código mais elaborado, sendo mais difícil de ser quebrada. Como curiosidade pode também citar que o mesmo ficou indecifrável por quase três séculos, uma vez que o sistema elaborado considerava diversas combinações entre as letras do alfabeto.

O professor também pode dizer que existiram várias outras cifras importantes, elaboradas ao longo da história, e que, dentre elas se destacaram as cifras de Hill, desenvolvidas por Lester S. Hill em 1929, as quais utilizam Transformações Lineares no desenvolvimento de mensagens criptográficas, o que possibilitou que os métodos se tornassem cada vez mais seguros.

Após introduzir os conceitos e um breve histórico da criptografia o professor poderá dar prosseguimento à atividade, passando para a explicação dos métodos selecionados para serem trabalhados em sala de aula.

Métodos de criptografia

Método de César

O professor pode explicar o método da seguinte forma: "É o método que tem a característica de substituir a letra da palavra em que se quer esconder por sua sucessora e formar assim com cada uma das letras da palavra em que se deseja manter em segredo. Neste caso, o código obedeceria a seguinte correspondência:

A – B – C – D – E – F – G – H – I – J – K – L – M – N – O – P – Q – R – S – T – U – V – W – X – Y – Z
B – C – D – E – F – G – H – I – J – K – L – M – N – O – P – Q – R – S – T – U – V – W – X – Y – Z – A"

Como exemplo de codificação, a palavra "VIDA" criptografada seria "WJEB" e como exemplo de decodificação do código de César, a seguinte mensagem criptografada "NPSUF" precisaria que as letras fossem substituídas pelas suas respectivas antecessoras do alfabeto, ou seja: a mensagem original seria "MORTE".

Com o passar do tempo, foi percebido que código de César era considerado muito simples e fácil de resolver. Nestes casos de codificação, como o valor das variações pelas letras sucessoras poderiam variar da primeira até a vigésima quinta letra, existiria no máximo vinte e cinco tentativas para se descobrir como foi realizado o tipo de decodificação de uma mensagem, o que indica que os códigos criados por César seriam fáceis de serem decifrados.

Método de Vigenère

Em seguida, o professor pode apresentar o método da seguinte forma: A cifra de Vigenère utiliza uma tabela, em que se repete o alfabeto. Cada linha da matriz se tem uma reprise do alfabeto com um deslocamento pelo sucessor do alfabeto da linha anterior. Assim, a matriz é de ordem 26 x 26, pois são 26 as letras que existem no alfabeto. Esta matriz antigamente era conhecida como "quadro de Vigenère" (SILVA, PAPANI, 2008, p.4-5), apresentada na Tabela 1. Também pode explicar que cada linha da matriz proporciona uma codificação diversificada nas letras do alfabeto, o que possibilita uma codificação diferente para as letras do alfabeto. Por exemplo, a letra "m", caso a codificação fosse feita pela linha 14 seria codificada por "a" e, no entanto, caso a codificação da letra "m" fosse realizada através da linha 23, seria codificada por "j".

Além da tabela, Vigenère também inseriu o que chamou de "palavras-chave" utilizadas tanto na codificação como na decodificação, de modo a dificultar o deciframento da mensagem criptografada. Assim, pessoa que codifica e a pessoa que recebe a mensagem para decodificação combinam uma palavra que será a palavra-chave do código.

Para se realizar a codificação da mensagem se repete a palavra-chave sobre as letras da mensagem a ser codificada, tantas vezes, quantas for necessário o que dependerá do tamanho da mensagem.

Como exemplo, considere que a palavra-chave seja "dado" e que se queira enviar a mensagem "jogue e olhe".

A letra da chave indica a linha que deve ser utilizada para a codificação. Deve-se considerar a linha em que o "d" está para depois analisar a coluna em que está o "j", para, em seguida observar a intersecção entre essas duas letras, onde será encontrada a letra "m". Para as demais letras, procede-se conforme apresentado na Tabela 2.

Assim, a mensagem "jogueeolhe" fica codificada por "mojiherzke". Para poder decifrar essa mensagem "mojiherzke", é necessário realizar o caminho contrário feito anteriormente. Por exemplo, na decodificação da letra "m" toma-se a linha indicada pela letra correspondente da

palavra-chave, neste caso, “d” e se faz a busca da letra “m” nesta linha, com a finalidade de se localizar a letra da coluna a que ela corresponde, neste caso, a letra “j”, conforme apresentado na Tabela 3.

Tabela 1
Quadro de Vigenère

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	F	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	J	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	R	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	T	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v	x	y
26	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v	x	y	z

Fonte: (FERRONI, 2003, p. 35)

Tabela 2
Codificação segundo o quadro de Vigenère

Chave	d	a	d	o	d	a	d	o	d	a
Texto plano	j	o	g	u	e	e	o	l	h	e
Texto Cifrado	m	o	j	i	h	e	r	z	k	E

Fonte: Elaborado pelo autor

Tabela 3
Decodificação segundo o quadro de Vigenère

Chave	d	a	d	o	d	a	d	o	d	a
Texto Cifrado	m	o	j	i	h	e	r	z	k	e
Texto plano	j	o	g	u	e	e	o	l	h	e

Fonte: Elaborado pelo autor

O professor pode informar também que a cifra de Vigenère, por se basear em diferentes combinações entre letras do alfabeto, conseguiu desviar a atenção dos criptoanalistas em relação à análise de freqüência de letras, o que havia sido muito eficaz quando os métodos eram de substituição literal monogramática simples.

O avanço obtido pela cifra de Vigenère, realizada pelo método de substituição polialfabética, tornou, naquela época, o trabalho dos criptoanalistas extremamente difícil no processo de deciframento de mensagens, pois na escolha das possibilidades de chaves, as opções seriam essas 26^{26}, seriam várias tentativas, com poucas chances de encontrar o procedimento de decifração da mensagem, pois sem a chave fica quase impossível decifrar.

A cifra de Vigenère, se tornou um código muito respeitado, pois na época era considerado indecifrável, Em francês se dizia: “Le chiffre indéchiffable” (SILVA, PAPANI, 2008 p.5)

Desta forma, a criptografia, nessa época, estava acima da criptoanálise devido a cifra desenvolvia por Vigenére. Porém, com o passar do tempo a tecnologia foi se aprimorando e o método utilizado por Vigenère, passou a ser mais vulnerável aos investigadores da criptoanalise, que já tinham muitas informações sobre tal método. Um dos motivos de descoberta se deve ao fato de que na chave e também no texto plano ocorrem a freqüência na distribuição das letras do alfabeto, que é padronizada de forma lógica e, ainda, que as informações da chave e do plano texto podem ser visivelmente analisadas por estatística. (ZANCANELLA, 2001, P.180).

Método das Transformações Lineares

O método de criptografia das transformações lineares, baseado nas Cifras de Hill, apresentado em Kolman (1999, p. 136), também utiliza matrizes e suas respectivas inversas como chaves no processo de codificação e decodificação de mensagens.

No entanto, o método é aplicado de maneira mais simplificada do que o procedimento utilizado nas Cifras de Hill, pois ao invés de enviar a mensagem codificada em letras, autor propõe o envio da mensagem codificada através dos números correspondentes às letras do alfabeto transformadas.

O professor pode comentar, que o processo se inicia associando um número a cada letra do alfabeto, conforme a Tabela 4.

Tabela 4
Correspondência entre letras e números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: (Elaborado pelo autor).

Em seguida, para exemplificar, o professor pode escrever uma frase, substituindo as letras pelos números correspondentes para formar o código. Como por exemplo: Caso se queira codificar “ver para crer” associam-se os números da seguinte maneira:

V	E	R	P	A	R	A	C	R	E	R
22	5	18	16	1	18	1	3	18	5	18

Em seguida, o professor pode explicar que pelo fato do método de substituição de letra por número poder ser quebrado facilmente, para dificultar o deciframento do código, neste método toma-se como chave para codificação uma matriz que admita inversa, ou seja, que possua determinante não nulo.

O método de codificação, neste caso, consiste em obter os valores dos vetores transformados de acordo com a transformação linear $L: R^3 \to R^3$, associada à matriz A, ou seja: $L_A\left(\vec{x}\right) = A\vec{x}$. Desta forma, considera-se como chave para codificação a matriz original e, como chave assimétrica, para decodificação a sua inversa.

Neste momento o professor poderá explorar os conceitos de determinantes de matrizes inversas. Como exemplo, poderá citar que a matriz $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$ possui determinante $det(A) = -1 \neq 0$, ou seja, possui inversa. Neste caso, a inversa seria. $A^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}_{3x3}$

Em seguida, o professor pode explicar que, como a matriz é de ordem 3, o próximo passo para codificação, consiste em agrupar os números associados a mensagem original em vetores de R^3, da seguinte forma:

$$\vec{v_1} = \begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix} \quad , \quad \vec{v_2} = \begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix} \quad , \quad \vec{v_3} = \begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix} \quad \text{e} \quad \vec{v_4} = \begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix}$$

Cabe observar que nesta mensagem, como o número de letras não é múltiplo de três, para completar o último vetor, repetiu-se o último número associado à última letra.

O professor poderá completar a explicação do processo informando que para finalizar a codificação da mensagem, deve se proceder da seguinte forma:

Codificação de $\vec{v_1} = \begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix}$: $L\left(\vec{v_1}\right) = A\vec{v_1} \Rightarrow L\left(\begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix} = \begin{bmatrix} 45 \\ 63 \\ 23 \end{bmatrix} \Rightarrow L\left(\vec{v_1}\right) = \begin{bmatrix} 45 \\ 63 \\ 23 \end{bmatrix}$

Codificação de $\vec{v_2} = \begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix}$: $L\left(\vec{v_2}\right) = A\vec{v_2} \Rightarrow L\left(\begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix} = \begin{bmatrix} 35 \\ 53 \\ 19 \end{bmatrix} \Rightarrow L\left(\vec{v_2}\right) = \begin{bmatrix} 35 \\ 53 \\ 19 \end{bmatrix}$

Codificação de $\vec{v_3} = \begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix}$: $L\left(\vec{v_3}\right) = A\vec{v_3} \Rightarrow L\left(\begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} 22 \\ 40 \\ 21 \end{bmatrix} \Rightarrow L\left(\vec{v_3}\right) = \begin{bmatrix} 22 \\ 40 \\ 21 \end{bmatrix}$

Codificação de $\vec{v_4} = \begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix}$: $L\left(\vec{v_4}\right) = A\vec{v_4} \Rightarrow L\left(\begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 41 \\ 59 \\ 36 \end{bmatrix} \Rightarrow L\left(\vec{v_4}\right) = \begin{bmatrix} 41 \\ 59 \\ 36 \end{bmatrix}$

Neste caso, na codificação da mensagem se obteve:

V	E	R	P	A	R	A	C	R	E	R	R
22	5	18	16	1	18	1	3	18	5	18	18
45	63	23	35	53	19	22	40	21	41	59	36

Assim, a mensagem codificada a ser enviada seria: 45 63 23 35 53 19 22 40 21 41 59 36.

Depois que a mensagem codificada for enviada para o destinatário, para decodificá-la o receptor deve usar a chave assimétrica que seria, neste caso a matriz inversa, para obter a mensagem original. Assim, decofidicação será feita de acordo com a transformação inversa, da seguinte forma:

$$L_A\left(\vec{x}\right) = A\vec{x} \quad \Rightarrow \qquad A^{-1}L_A\left(\vec{x}\right) = A^{-1}A\vec{x} \quad \Rightarrow \qquad A^{-1}L_A\left(\vec{x}\right) = \vec{x}$$

Neste caso para cada vetor $\vec{x}$, a decodificação será obtida por $\vec{x} = A^{-1}L_A\left(\vec{x}\right)$, ou seja:

Decodificação de $L\left(\vec{v}_1\right) = \begin{bmatrix} 45 \\ 63 \\ 23 \end{bmatrix}$ $\Rightarrow A^{-1}\begin{bmatrix} 45 \\ 63 \\ 23 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}.\begin{bmatrix} 46 \\ 63 \\ 23 \end{bmatrix} = \begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix}$ $\Rightarrow \vec{v}_1 = \begin{bmatrix} 22 \\ 5 \\ 18 \end{bmatrix}$

Decodificação de $L\left(\vec{v}_2\right) = \begin{bmatrix} 35 \\ 53 \\ 19 \end{bmatrix}$ $\Rightarrow A^{-1}\begin{bmatrix} 35 \\ 53 \\ 19 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}.\begin{bmatrix} 35 \\ 53 \\ 19 \end{bmatrix} = \begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix}$ $\Rightarrow \vec{v}_2 = \begin{bmatrix} 16 \\ 1 \\ 18 \end{bmatrix}$

Decodificação de $L\left(\vec{v}_3\right) = \begin{bmatrix} 22 \\ 40 \\ 21 \end{bmatrix}$ $\Rightarrow A^{-1}\begin{bmatrix} 22 \\ 40 \\ 21 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}.\begin{bmatrix} 22 \\ 40 \\ 21 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix}$ $\Rightarrow \vec{v}_3 = \begin{bmatrix} 1 \\ 3 \\ 18 \end{bmatrix}$

Decodificação de $L\left(\vec{v}_4\right) = \begin{bmatrix} 41 \\ 59 \\ 36 \end{bmatrix}$ $\Rightarrow A^{-1}\begin{bmatrix} 41 \\ 59 \\ 36 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 0 \end{bmatrix}.\begin{bmatrix} 41 \\ 59 \\ 36 \end{bmatrix} = \begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix}$ $\Rightarrow \vec{v}_4 = \begin{bmatrix} 5 \\ 18 \\ 18 \end{bmatrix}$

Assim, na decodificação da mensagem se obtém:

45	64	23	35	53	19	22	40	21	42	61	36
22	5	18	16	1	18	1	3	18	5	18	18
V	E	R	P	A	R	A	C	R	E	R	R

Finalizando os exemplos, o professor poderá comentar que os três métodos apresentados, possibilitam manter o conteúdo da mensagem em segredo. Porém o primeiro, devido a simplicidade de codificação pode ser decifrado facilmente, o que não ocorre nos dois últimos casos.

Atividades sobre aplicação dos Métodos de criptografia

Em seguida, o professor poderá disponibilizar a seguinte lista de atividades, como desafios. Como atividade alternativa, sugere-se também que o professor também poderá solicitar

aos alunos que inventem métodos próprios de criptografia e que elaborem uma atividade que possa ser compartilhada com os demais colegas, contendo proposta e resolução das mesmas.

Atividade 1: Codifique a frase "paciência para interpretar", utilizado o método de César de decodificação de letras sucessoras. Resposta: qbdjfodjb qbsb joufsqsfubs

Atividade 2: Decodifique a frase "SÁBADO É O DIA DE ATACAR", utilizado o método de César de decodificação de letras sucessoras. Resposta: TBCBEPFPEJBEFBUBDBS

Atividade 3: Utilizando como palavra- chave "tempo" codifique a frase "paciência para interpretar", utilizado o método de Vigenère. Resposta: ieoxsggupdtwmxbmidefxxmg

Atividade 4: Decodifique a mensagem "WYUSOVSBDVLTMHGT", utilizado o método de Vigenère, utilizando a palavra-chave "tempo" Resposta: CUIDADOPOISPASSA

Atividade 5: Utilizando como chave a matriz $A=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 2\\ 0 & 1 & 1\end{bmatrix}$ codifique a frase "paciência para interpretar", utilizado o método das Transformações Lineares.
Resposta : 20 23 4 28 42 19 13 14 10 35 53 19 24 38 23 43 61 23 39 44 23 39 57 19

Atividade 6: Decodifique a mensagem "13 17 9 13 14 4 32 41 14 39 44 25 52 70 34 26 27 21", utilizado o método das Transformações Lineares e inversa $A^{-1}=\begin{bmatrix}1 & 0 & -1\\ 1 & -1 & 1\\ -1 & 1 & 0\end{bmatrix}$

Resposta: 4 5 4 9 3 1 18 5 9 14 20 5 0 20 2 5 20 1
d e d i c a r e i n t e r p r e t a

Considerações finais

Com o passar dos anos, a criptologia foi reconhecida, merecidamente, como ciência. De fato seu desenvolvimento ao longo da história foi, e tem sido, muito importante na transmissão de mensagens e de dados confidenciais.

Além disso, devido aos avanços tecnológicos, a utilização de computadores possibilitou maiores avanços, não somente em relação à criação de novos métodos de criptografia, mas também contribuiu significativamente com os métodos desenvolvidos pela criptoanálise.

Paralelamente a este processo de aprimoramento na busca de resoluções de problemas práticos próprios da Criptografia, acredita-se que o acesso a estas informações também puderam e podem ajudar aos educadores matemáticos na árdua tarefa de incentivarem seus educandos, uma vez que os conceitos de criptografia possibilitam inserir atividades lúdicas e diferenciadas em sala de aula.

Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade.

Como a Criptografia da atualidade está relacionada ao uso de computadores e os alunos, atualmente, os utilizam muito, é possível que se interessem e que queiram saber sobre seus

conceitos e aplicações. Da mesma forma, também vão querer saber sobre a Criptoanálise, com intuito de tentar interpretar informações criptografadas, o que pode contribuir não só na vida escolar do aluno, mas também com seu crescimento pessoal.

Ao se utilizar a Criptografia em sala de aula, é possível oportunizar ao aluno o conhecimento de fatos importantes ocorridos na história e suas contribuições, relacionando-os com acontecimentos da atualidade. Assim, o aprendizado da matemática pode se tornar mais fácil e significativo, o que vem a contribuir não só com o desenvolvimento da vida escolar do aluno, mas também com seu crecimento pessoal

Acredita-se que, ao se buscar estimular a percepção de aplicação de conceitos teóricos na resolução de problemas reais, de seus cotidianos, tanto os resultados da pesquisa bibliográfica, como em relação à atividade proposta, podem vir a contribuir para que o ensino de matemática seja mais produtivo, possibilitando que o aprendizado seja mais significativo na vida social e pessoal do educando.

Bibliografia e referências

Alecrim, Emerson. (2010, Julho 26) *História e Aplicações da Criptografia*. Recuperado de http://www.infowester.com/criptografia.php

Alvarenga, Luis G. (2010, Agosto 18) *Criptografia Clássica e moderna*. Recuperado de http://www.scribd.com/doc/35442992/Criptografia-Classica-e-Moderna

Coutinho, S. C. (2008) *Programa de iniciação Científica da OBMEP 2007.* Rio de Janeiro, Brasil: Instituto Nacional de Matemática Pura e Aplicada-IMPA.

Coutinho, S. C. (2009) *Números Inteiros e Criptografia RSA.* 2. ed. Rio de Janeiro, Brasil: Instituto Nacional de Matemática Pura e Aplicada-IMPA.

Ferroni, Marcelo (2003) Quebrando códigos. *Revista Galileu Especial Eureca*. Ed. Globo. 1, pp. 34-35.

Eves, Howard. (2004) *Introdução à história da matemática*. São Paulo, Brasil: Editora da Unicamp.

Kolman, Bernard. (1999) *Introdução à Álgebra Linear com aplicações*. Rio de Janeiro, Brasil: Livros técnicos e Científicos Editora S.A.

Machado, Nilson José. (1997) *Matemática e realidade*. 4.d. São Paulo, Brasil: Cortez.

Silva Fernanda T. Da, Papine Fabiana Garcia. (2008) *Um pouco da história da criptografia.* XXII Semana Acadêmica da Matemática. Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste. Cascavel, Brasil. pp. 76-81.

Zancanella, Luis Carlos. (2001). *Fundamentos da Criptografia.* Florianópolis, Brasil: INE/UFSC/SC.