18. Criptografia e Matemática: Onde e Como Usarmos essa Interdisciplinaridade?

Mário Augusto de Araujo Caneco[1]

RESUMO

A palavra interdisciplinar é formada pela união do prefixo "*inter*", que exprime a ideia de "em meio"; com a palavra "disciplinar", que tem um sentido pedagógico de instruir regras e preceitos de alguma arte. Assim entendemos interdisciplinar como processo de se obter ligação entre as disciplinas. Na área pedagógica, essa interdisciplinaridade se evidencia quando podemos planejar a utilização de duas ou mais disciplinas, relacionando seus conteúdos para aprofundar, e maioria das vezes, facilitar sua aprendizagem através de dinâmica no ensino, proporcionando bases para um ensino mais interessante, onde uma matéria auxilia a outra.

Criptografia é a arte de escrever mensagens cifradas que, nos dias atuais, é muito utilizada em processos eletrônicos, transmissão digital de informações, transações bancárias online, sistemas de compras eletrônicos, entre outras aplicações muito utilizadas na vida moderna. Mas neste artigo, apresentamos o significado, histórico e utilização desses códigos e senhas como instrumentos utilizados na segurança das comunicações militares – através da chamada "Transposição por Quadros: Chaves Simples e Chave Dupla".

Após as explicações apresentadas nos parágrafos anteriores; e aproveitando o bom momento que vive a educação matemática brasileira, lembrando termos, em 2018, sediado o congresso mundial de matemática, e que uma equipe de estudantes brasileiros recebeu 04 (quatro) medalhas de bronze e 01 (uma) de ouro na Olimpíada Internacional de Matemática no país Romênia; pesquisamos e apresentamos através de alguns exemplos da "Criptografia de Júlio César" e da "Criptografia com Função Linear", a constatação da interdisciplinaridade entre Criptografia e Matemática, como possíveis atividades didáticas a serem utilizadas, visando a facilitação do ensino e despertar o

(1) Tenente Coronel do Exército Brasileiro, graduado na AMAN (1998). Professor de Matemática, licenciado na UFSJ (2013), e Coordenador Pedagógico, pós-graduado pelo CEP/FDC (2017). Atualmente está vinculado profissionalmente à Escola de Aperfeiçoamento de Sargentos das Armas (EASA); e-mail: marioenane@bol.com.br.

interesse individual dos alunos.

Vamos aos resultados!

Palavras-chave: Criptografia. Interdisciplinaridade, Educação Matemática, Função Linear.

INTRODUÇÃO

Em dicionários, criptografia é defina como os procedimentos, processos e métodos de fazer e usar a escrita secreta, como códigos ou cifras. O militar usa criptografia verbal e escrita ou digitada para se comunicar e transmitir informações secretas.

Enviar mensagens secretas é uma tarefa muito antiga; ela nasceu com a diplomacia e com as transações militares. Hoje em dia, entretanto, com o advento da comunicação eletrônica, muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet.

A ciência que estuda sistemas de envio e recepção de mensagens secretas chama-se Criptologia.

1 CRIPTOGRAFIA E SUA HISTÓRIA

Criptografia vem do grego *krypto*, que significa escondido, secreto, oculto, e *grapho*, que significa grafia, escrita (SINGH, 2003). Consiste em codificar informações usando uma chave antes que essas sejam transmitidas, e em decodificá-las, após a recepção, através de um processo de codificação. A criptografia torna possível o envio de mensagens incompreensíveis para uma terceira pessoa que, eventualmente, venha a interceptá-las, mas que poderão ser lidas pelo seu destinatário, que conhece o critério para decifrar o texto encriptado. (TERADA, 1988; TAMAROZZI, 2001; SCHEINERMAN, 2003; ZATTI; BELTRAME, 2009).

Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. O processo de converter um texto comum em cifrado é chamado cifrar ou criptografar, e o processo inverso, de converter um texto cifrado em comum, é chamado decifrar (ZATTI; BELTRAME, 2009). A criptografia é uma arte bastante antiga, presente desde o sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. E, o mais interessante, é que a tecnologia de criptografia não mudou muito até meados deste século.

Depois da segunda guerra mundial, com a invenção do computador, a área realmente floresceu, incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços na decifração de códigos utilizados. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna. O ***Citale Espartano*** (SINGH, 2011) foi o primeiro aparelho criptográfico militar utilizado durante o século V a.C. Era um bastão de madeira em que se enrolava uma tira de couro e escrevia-se a mensagem em todo o comprimento desse bastão. Para enviar a mensagem, de forma despercebida, a tira de couro era desenrolada do ***citale*** e utilizada como um cinto, com a mensagem voltada para dentro. Como na tira de couro a mensagem ficava sem sentido, para decifrá-la era necessário que o receptor tivesse um ***citale*** de mesmo diâmetro para enrolar a tira de couro e ler a mensagem.

Outro tipo de cifra utilizada, esta idealizada por Júlio César, consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. César utilizava o alfabeto normal para escrever a mensagem e o alfabeto cifrado para codificar a mensagem que mais tarde seria enviada. Esse método de criptografia ficou conhecido como Cifra de César. Como as cifras de substituição monoalfabéticas eram muito simples e facilmente decifradas por criptoanalistas, através da análise de frequência de cada letra, no texto cifrado, surgiu a necessidade da criação de novas cifras, mais elaboradas e mais difíceis de serem descobertas. A solução encontrada, no século XVI, pelo diplomata francês Blaise Vigenère, sua ma-

neira – Cifra de Vigenère, utilizava 26 alfabetos cifrados diferentes para codificar uma mensagem. Também podemos citar Alberti, como o criador da primeira máquina criptográfica, o Disco de Cifras, um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado.

Em 1943, foi projetado um computador utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O *Colossus*, assim denominado, deu início a uma era moderna da criptografia, em que os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma. Essa nova técnica de criptografia era de uso exclusivo do governo e de militares para guardar informações.

2 OBJETIVO DA INVESTIGAÇÃO

O objetivo geral deste trabalho foi investigar a Criptografia e suas possíveis aplicações no ensino da Matemática; e de maneira inversa, a exigência de noções básicas da Matemática para a aprendizagem da criptografia em instruções das comunicações militares.

3 METODOLOGIA DA INVESTIGAÇÃO

Inicialmente optei por uma rápida busca exploratória em livros, revistas e documentos on-line, em torno do significado e história da criptografia. Em seguida, recordei a aprendizagem do emprego da criptografia, em minha formação básica como profissional militar.

E por fim, busquei o planejamento e a constatação da interdisciplinaridade dessa criptografia, como atividades didáticas utilizadas para facilitar o ensino e despertar o interesse individual dos alunos, na aprendizagem de alguns conteúdos da matemática básica.

4 ATIVIDADES DIDÁTICAS COM O TEMA CRIPTOGRAFIA

4.1 Criptografia de Júlio César

Um dos primeiros sistemas de criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César substituiu cada letra, pela terceira letra que a segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

Tabela 1: quadro do método de substituição utilizado por Júlio César.

Segundo esse sistema, temos:

 # Palavra: MATEMÁTICA.

M	A	T	E	M	A	T	I	C	A
P	**D**	**W**	**H**	**P**	**D**	**W**	**L**	**F**	**D**

Tabela 2: quadro solução do método de substituição utilizado por Júlio César.

 # Criptografia: PDWHPDWLFD.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Tabela 3: quadro do método de substituição utilizando letras e números.

Atividade 1: Decifre a mensagem: OHJDO FRQVHJXL Ao invés de caminhar 3 letras para frente, podemos andar um outro número de letras e teremos um novo método de cifrar mensagens. Este número é chamado de "chave ou senha do sistema criptográfico"; ele deve ser conhecido apenas por quem envia e por quem a recebe a mensagem.

Podemos também transformar letras em números, segundo uma ordem preestabelecida.

Por exemplo:

Deste modo, a letra codificada seria obtida da letra original, somando-se 5 ao número correspondente.

 # Expressão: *ATAQUE COORDENADO*

A	T	A	Q	U	E	C	O	O	R	D	E	N	A	D	O
F	Y	F	V	Z	J	H	T	T	W	I	J	S	F	I	T

Tabela 3: quadro solução do método de substituição utilizando letras e números.

 # Código: *FYFVZJ HTTWIJSFIT*

E se o resultado ultrapassar 25? Caso isto ocorra, a letra codificada estará associada ao resto da divisão por 26 do número associado à letra original somado com 5. Por exemplo, a letra Y corresponde originalmente ao número 24, somando-se 5, obteremos 24 + 5 = 29 e, dividindo 29 por 26, obteremos resto 3 que corresponde à letra "D". Assim "Y" deve ser codificado por "D".

Em outros sistemas que seguem o princípio de Júlio César, o alfabeto é codificado seguindo a ordem usual, apenas iniciando em um lugar diferente. Se, entretanto, pudermos alterar a ordem, obteremos um enorme número de maneiras de criptografar. Vejamos alguns exemplos:

a) Alfabeto quebrado ao meio:

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

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

Tabela 4: quadro do método de substituição utilizando alfabeto quebrado ao meio.

b) Troca de dois vizinhos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
B	A	D	C	F	E	H	G	J	I	L	K	N	M

O	P	Q	R	S	T	U	V	W	X	Y	Z
P	O	R	Q	T	S	V	U	X	W	Z	Y

Tabela 5: quadro do método de substituição utilizando troca de dois vizinhos.

c) Usando a sequência que aparece no teclado do computador:

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

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	H	J	K	L	Z	X	C	V	B	N	M

Tabela 6: quadro do método de substituição utilizando sequência do teclado do computador.

Observem que nos casos anteriores nenhuma letra ficou no seu lugar original. Dizemos então que

houve um completo desordenamento.

4.2 Criptografia com Função Linear

A seguir, apresentaremos um exemplo de atividade didática que é costumeiramente utilizada no Ensino Médio, utilizando a função linear – também conhecida como função polinomial de grau 1 ou função polinomial de primeiro grau. (Tamarozzi, 2001).

Primeiro relacionamos cada letra do alfabeto a um número, conforme as tabelas abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26

Tabela 7: quadro do método de substituição utilizando a Função Linear.

Exemplo 1: Criptografe a mensagem "Tudo é Matemática", sendo a função cifradora (linear) do tipo f(x) = 2x + 1 <----> y = 2x + 1.

Solução:

1º passo: Relacionamos cada letra da mensagem com seu respectivo numeral.

T	U	D	O	E	M	A	T	E	M	A	T	I	C	A
20	21	4	15	5	13	1	20	5	13	1	20	9	3	1

Tabela 8: quadro solução parcial do método de substituição utilizando a Função Linear.

2º passo: Depois calculamos, uma a uma, substituindo cada número da função cifradora.

- *T = 20, logo f (20) = 20.2 + 1 = 41*
- *U = 21, logo f (21) = 21.2 + 1 = 43*
- *D = 4, logo f (4) = 4.2 + 1 = 9*
- *O = 15, logo f (15) = 15.2 + 1 = 31*

....

- *até a letra A = 1, logo f (1) = 1.2 + 1 = 3*

Encontramos assim, a imagem da função; isto é, a sequência numérica encontrada, é a mensagem criptografada:

T	U	D	O	E	M	A	T	E	M	A	T	I	C	A
41	**43**	**9**	**31**	**11**	**27**	**3**	**41**	**11**	**27**	**3**	**41**	**19**	**7**	**3**

Tabela 9: quadro solução final do método de substituição utilizando a Função Linear.

Para decifrar uma mensagem o receptor calcula a imagem dos elementos, utilizando a função inversa, logo usaremos x = (y – 1) / 2.

4.3 Criptografia Militar

Nossa intenção agora é apresentar atividades com criptografia ensinada nas instruções básicas de segurança militar (comunicações).

Para isso utilizaremos os "Sistemas Criptográficos com Transposição Por Quadros"

DIA DA SEMANA	CHAVE SIMPLES	CHAVE DUPLA	
SEGUNDA	8–5–10–1–6–9–4–2–7–3	FEDERAL	CRIPTOGRAMA
TERÇA	PERNAMBUCO	5–7–8–1–4–3–2–10–6–9	3–9–10–7–1–6–2–8–5–4
QUARTA	11–7–4–2–6–1–9–10–3–5–8	PRESIDENTE	FAZENDA
QUINTA	EMERGENTE	9–2–1–6–7–4–3–8–5	2–3–5–7–1–6–4
SEXTA	2–7–3–6–8–5–1–9–4	ADVOGADO	BRASEIRO
SÁBADO	EQUIPAMENTOS	7–4–1–6–3–5–2	COMPUTADOR
DOMINGO	7–1–5–4–8–2–3–6–9	DRAMATICO	1–2–4–3–6–5–7

Tabela 10: quadro do método de Sistemas Criptográficos com Transposição Por Quadros.

Observações:

1) Nas Chaves Simples ou Dupla, o texto em claro deverá ser escrito na horizontal, da esquerda para a direita, e de cima para baixo;

2) Na Chave Simples o Criptograma deverá ser retirado na vertical de cima para baixo, na ordem numérica crescente da chave;

3) Na Chave Dupla a primeira chave é escrita na horizontal nos dias SEG, QUA, SEX, e na vertical nos dias TER, QUI, SAB e DOM. O criptograma será retirado letra por letra na ordem numérica crescente da coluna (chave da horizontal) e dentro da coluna na ordem numérica crescente da fileira (chave da vertical).

Exemplo 1: Criptografe a mensagem "O inimigo atacará pela porção oeste da cota pelada", utilizando a Transposição por Quadros – Chave Simples, sendo hoje, uma sexta-feira:

Solução: Pelo Sistema Criptográfico em vigor, devemos utilizar a Chave Simples prevista para **sexta-feira (2 – 7 – 3 – 6 – 8 – 5 – 1 – 9 – 4)**, *para a montagem do quadro criptográfico:*

	2	7	3	6	8	5	1	9	4
→ 1	O	I	N	I	M	I	G	O	A
2	T	A	C	A	R	A	P	E	L
3	A	P	O	R	C	A	O	O	E
4	S	T	E	D	A	C	O	T	A
5	P	E	L	A	D	A	#	#	#

Tabela 11: quadro solução parcial do método de Sistemas Criptográficos com Transposição Por Quadros.

Em seguida, faremos a leitura do Criptograma conforme regra estabelecido no Sistema Cartográfico de Chave Simples, na vertical de cima para baixo, e na ordem numérica crescente da chave. Logo, a mensagem "O inimigo atacará pela porção oeste da cota pelada" criptografada deverá ser transmitida da seguinte maneira:

GPOO# OTASP NCOEL ALEA# IAACA IARDA IAPTE MRCAD OEOT#

Exemplo 2: Decifre a mensagem **(PSRI# CPFNC ERSSO EEEE# EOOD# NAAS# IAEEA TMFA# RDTR#)**, utilizando a Transposição por Quadros – Chave Simples, sendo hoje, uma sexta-feira:

Solução: Pelo Sistema Criptográfico em vigor, devemos utilizar a Chave Simples prevista para **sexta-feira (2 – 7 – 3 – 6 – 8 – 5 – 1 – 9 – 4)**, para a montagem do quadro criptográfico:

	2	7	3	6	8	5	1	9	4
1	C	I	E	N	T	E	P	R	E
2	P	A	R	A	M	O	S	D	E
3	F	E	S	A	F	O	R	T	E
4	N	E	S	S	A	D	I	R	E
5	C	A	O	#	#	#	#	#	#

Tabela 12: quadro solução parcial do método de Sistemas Criptográficos com Transposição Por Quadros.

Após o lançamento da Criptografia conforme regra estabelecido no Sistema Cartográfico de Chave Simples, na vertical de cima para baixo, e na ordem numérica crescente da chave, acharemos a mensagem: "CIENTE, PREPARAMOS DEFESA FORTE NESSA DIREÇÃO!"

CONSIDERAÇÕES FINAIS

Até meados do século XX, a criptografia era considerada uma arte; hoje em dia, entretanto, passou a ser considerada uma ciência. Com o avanço da tecnologia e o uso da internet, telefones celulares, satélites e GPS, destacamos como aplicações atuais da criptografia: sigilo em banco de dados; investigações governamentais; decisões estratégicas empresariais; comandos militares; mensagens diplomáticas; operações bancárias; e recuperação de documentos arqueológicos e hieróglifos.

As atividades apresentadas neste artigo são sugestões para que o professor possa utilizar para revisar, exercitar e aprofundar os conteúdos desenvolvidos no ensino de conceitos de aritmética básica, bem como uma oportunidade de incentivar o desenvolvimento de estratégias de resolução de problemas, da matemática do ensino médio (funções quadrática, exponencial e logarítmica).

REFERÊNCIAS

_____. Apostila de Comunicações da Escola de Sargentos das Armas. (EsSA), Três Corações, 2001.

FOGUEL, Débora. Instituto de Bioquímica Médica Leopoldo de Meis. UFRJ - Rio de Janeiro. Disponível em: < https://blogs.oglobo.globo.com/ciencia-matematica/post/matematica-em-casa-ajuda-criancas-na-escola.html >Acesso 21 ago 2018.

GROENWALD, Claudia Lisete Oliveira. FRANKE, Rosvita Fuelber; OLGIN, Clarissa de Assis. Códigos e Senhas no Ensino Básico - EMR-RS - ANO 10 - 2009 - número 10 - v.2 - pp. 41 a 50.

SCHEINERMAN, Edward R. Matemática discreta: uma introdução. São Paulo: Thompson, 2003.

SINGH, Simon. O livro dos códigos: a ciência do sigilo – do Antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2003.

TAMAROZZI, Antônio Carlos. Codificando e decifrando mensagens. Revista do Professor
de Matemática (RPM), São Paulo, n.45, 41-43, 2001

TERADA, Routo. Criptografia e a importância das suas aplicações. Revista do Professor de Matemática (RPM), São Paulo, n.12, 1-6, 1988.

ZATTI, Sandra Beatriz; BELTRAME, Ana Maria. A presença da álgebra linear e da teoria dos números na criptografia. São Paulo, 2009.