ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Cap QCO Mag Anderson Pinheiro Machado

CRIPTOGRAFIA E MATEMÁTICA: UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O TURNO INTEGRAL DO SISTEMA COLÉGIO MILITAR DO BRASIL

Rio de Janeiro
2019

Cap QCO Mag ANDERSON PINHEIRO MACHADO

CRIPTOGRAFIA E MATEMÁTICA: UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O TURNO INTEGRAL DO SISTEMA COLÉGIO MILITAR DO BRASIL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares

Orientador: Maj QCO Mag Tupolevck Florencio

Rio de Janeiro
2019

Cap QCO Mag ANDERSON PINHEIRO MACHADO

CRIPTOGRAFIA E MATEMÁTICA: UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O TURNO INTEGRAL DO SISTEMA COLÉGIO MILITAR DO BRASIL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares

Aprovado em:

COMISSÃO DE AVALIAÇÃO

_____

Tupolevck Florencio – Maj QCO – Presidente
Escola de Formação Complementar do Exército

_____

Sérgio Inácio da Silva – Maj QCO – Membro
Escola de Formação Complementar do Exército

CRIPTOGRAFIA E MATEMÁTICA: UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O TURNO INTEGRAL DO SISTEMA COLÉGIO MILITAR DO BRASIL

Anderson Pinheiro Machado[1]

RESUMO

Com o objetivo de contribuir com a qualidade do ensino do Sistema Colégio Militar do Brasil (SCMB), este trabalho apresenta uma proposta de sequência didática visando atender, prioritariamente, embora possa não ser exclusiva, demandas do turno integral. A opção de relacionar Criptografia e Matemática busca, em um primeiro momento, despertar a atenção dos discentes a partir de um assunto atual e amplo. A Criptografia engloba áreas de interesse diversas, podendo partir de seu caráter histórico até discussões sobre tecnologia, segurança na *internet* e compras *online*, por exemplo. Disto, surgem oportunidades de ensino estruturadas em pilares desejáveis pelo SCMB como contextualização, interdisciplinaridade e o uso de tecnologia em sala de aula. Porém, este trabalho, embora indique fontes de consulta para o leitor que deseje outros direcionamentos em Criptografia, também delimita o tema, principalmente pela amplitude de possibilidades. Com isto, após um referencial teórico que trata de conceitos básicos e fatos relevantes em Criptografia – que visa ambientar o leitor – são apresentados os resultados, colocados na forma da Sequência Didática em si, com os Planos de Aula (PA) e Matriz de Descritores (MD) desenvolvidos conforme modelos adotados pelos Colégios Militares. A particularidade desta sequência didática também pode ser notada pelo uso do ensino de competências e habilidades, exploradas durante as aulas, como apontam as sugestões de atividades que constituem parte dos apêndices deste trabalho. Por fim, conclui-se que o turno integral também pode ser uma excelente oportunidade para as atividades da área cognitiva, desde que haja comprometimento em complementar assuntos trabalhados no turno regular, desenvolvidos de maneira atraente para os alunos. O que pode ser conferido na leitura deste estudo são possibilidades, indicando caminhos para o professor dentro de um tema tão vasto quanto a Criptografia.

Palavras-chave: Criptografia. Matemática. Turno Integral. Ensino por competências e habilidades.

ABSTRACT

In order to contribute to the quality of the teaching of the Brazilian Military College System, this work presents a proposal for a didactic sequence aiming to attend, although it may not be exclusive, full shift demands. The option of relating Cryptography and Mathematics seeks, at first, to arouse students' attention from a current and broad subject. Cryptography encompasses several areas of interest, ranging from its historical character to discussions about technology, internet security and online shopping, for example. From this, learning opportunities arise structured in desirable pillars by SCMB such as contextualization, interdisciplinarity and the use of technology in the classroom. However, this work, although indicating sources of consultation for the reader who wants other directions in Cryptography, also delimits the theme, especially by the breadth of possibilities. Thus, after a theoretical framework that deals with basic concepts and relevant facts in Cryptography - which aims to set the reader at ease - the results are presented, placed in the form of the Didactic Sequence itself, with the Class Plans and Descriptor Matrix developed according to models adopted by the Military Colleges. The particularity of this didactic sequence can also be noted by the use of teaching of competences and skills, explored during the classes, as pointed out by the suggestions of activities that are part of the appendices of this work. Finally, it is concluded that the full shift can also be an excellent opportunity for cognitive activities, as long as there is a commitment to complement subjects worked in the regular shift, developed in an attractive way for students. What can be seen in the reading of this study are possibilities, indicating ways for the teacher within a theme as vast as Cryptography.

Keywords: Criptography. Mathematics. Integral shift. Teaching by skills and abilities.

[1] Capitão QCO Magistério Matemática da turma de 2011. Mestre em Matemática pela UFSM/PROFMAT em 2018. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2011.

SUMÁRIO

CRIPTOGRAFIA E MATEMÁTICA: UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA O TURNO INTEGRAL DO SISTEMA COLÉGIO MILITAR DO BRASIL

1. INTRODUÇÃO

O presente trabalho apresenta uma proposta de sequência didática sobre o estudo da Criptografia, relacionada, principalmente, com a disciplina de Matemática. Possui, como objetivo principal, fornecer aos professores do Sistema Colégio Militar do Brasil (SCMB) possibilidades direcionadas – mas não restritas – a aplicações no turno integral para alunos dos 6º ao 9º anos do Ensino Fundamental.

O turno integral, que já é uma realidade no âmbito do SCMB, pode ser descrito como uma extensão do turno regular, devendo estar integrado com este, onde “as atividades oferecidas deverão se enquadrar em uma de três grandes temáticas: cognitivas, físicas e artísticas” conforme determinam as Normas de Planejamento e Gestão de Ensino - NPGE (2018, p. 53), documento consolidado pela Diretoria de Educação Preparatória e Assistencial (DEPA). Buscando atingir esta meta, cada colégio militar desenvolve atividades próprias, de acordo com suas características e capacidades.

Assim, em conjunto com o aprendizado proporcionado pelo ensino da Música, do Teatro, da Dança e de tarefas esportivas que vão do Atletismo à Orientação, que preenchem, prioritariamente, as temáticas artísticas e/ou físicas, surge o desafio de elaborar atividades atraentes sob a temática cognitiva.

Na verdade, o melhor cenário é o que enxerga o desenvolvimento de tais atividades cognitivas como uma oportunidade de complementar habilidades, trazendo aos discentes problemas e projetos instigantes, aproveitando o tempo disponível com um ensino dinâmico, em contraste ao que poderia ser “maçante” ou “mais do mesmo” para os alunos, principalmente na área da Matemática, no que Lorenzato (2010, p. 63) acrescenta: “ensinar matemática utilizando-se de suas aplicações torna a aprendizagem mais interessante e realista (...)”.

Diante desta situação, surge a Criptografia, assunto que este trabalho não pretende esgotar ou exaurir, mas sim trazer ao leitor um estudo que pode mostrar-se eficiente ao abranger áreas de interesse tão diversas, desde funções matemáticas a guerras e compras *online*. É um tema atual em uma época de debates sobre

criptomoedas, privacidade e segurança na *internet*, por exemplo. O próprio Exército Brasileiro, como instituição, investe e destina parte de seu interesse na salvaguarda de informações e documentos sigilosos pertinentes à área de Inteligência.

De fato, um maior contato com o assunto em questão relaciona-se com uma dissertação de mestrado (MACHADO, 2018) então desenvolvida. O foco desta foi a Criptografia RSA que apresenta o centro de seu entendimento na Aritmética Modular e na decomposição em fatores primos. Porém, diferente da proposta desta dissertação, este artigo trata de outras possibilidades com a Criptografia, muitas delas sem a construção de pré-requisitos, mas aproveitando a experiência e parte da pesquisa realizada para explorar outros públicos e condições. Aliás, esta era uma das conclusões deste trabalho anterior, pois desde então percebeu-se que existiam outras oportunidades para serem ampliadas envolvendo Criptografia e Educação.

Com este direcionamento em mente, esta proposta de ensino estrutura-se em três pilares: a contextualização, a interdisciplinaridade e o uso da tecnologia na educação. Estas, são ferramentas desejáveis nos colégios militares - como apontam vários documentos internos - atendendo aos parâmetros do currículo baseado em habilidades e competências. Neste sentido, o Projeto Pedagógico do SCMB (2016, p.15) direciona que:

> A busca da interdisciplinaridade é um objetivo imperioso para a consecução dos resultados do processo educacional. A adoção do ensino por competências colabora, de forma patente, com este intento, bem como quanto à contextualização, na medida em que se ancora em situações-problema nas quais os objetos de conhecimentos são evocados para o desenvolvimento de habilidades. Nesta metodologia, os conteúdos devem ser justificados por seu emprego, o que os remove da dimensão unicamente teórica para a dimensão da prática.

Sobre o uso de tecnologia em sala de aula, cita-se uma das premissas das NPGE (2018, p. 44): “A tecnologia educacional utiliza-se de ferramentas tecnológicas de informação e comunicação que potencializam as estratégias de ensino e de aprendizagem”.

Por fim, com a elaboração desta proposta de ensino, espera-se contribuir com os professores do SCMB, fornecendo ferramentas que enriqueçam suas aulas e, a partir da leitura deste estudo, possam ser direcionados a ampliarem suas escolhas, com especial atenção ao turno integral, mas que podem também ser estendidas às

aulas regulares e outros projetos educacionais. A expectativa é a de despertar o interesse dos alunos, desenvolvendo atividades que estimulem o raciocínio, a concentração e a organização em um aprendizado realmente motivador.

2. REFERENCIAL TEÓRICO

2.1 Primeiros conceitos em Criptografia

Segundo Hefez (2014, p. 310), a palavra criptografia origina-se do grego, onde *kriptos* significa oculto e, portanto, a palavra criptografia significa "escrita oculta".

O desenvolvimento da Criptografia parte justamente da necessidade de ocultar mensagens, proteger documentos sigilosos e tornar confiável a troca de informação. E isto nos remete diretamente à história de guerras e diplomacia, onde reis, generais e líderes de Estado precisavam de métodos seguros para alcançar os mais diferentes objetivos. Shokranian (2012, p. 21) complementa que “enviar mensagens em código pode servir essencialmente para dois objetivos: servir para enviar uma mensagem secreta e proteger o conteúdo da mensagem contra fontes não autorizadas”.

De fato, não faltam fatos históricos que exemplificam a importância da Criptografia ao longo da História, como a Cifra de César, a Cifra de Políbio, o telegrama Zimmermann e a Máquina Enigma, só para citar alguns que terão maiores referências neste trabalho.

Por outro lado, alguns conceitos são necessários para uma leitura adequada sobre Criptografia. Os primeiros dizem respeito ao ato de codificar\decodificar uma mensagem. Diz-se que o emissor da mensagem codifica (cifra), tornando-a incompreensível aos demais para que chegue ao seu destino, o receptor, que decodificará (decifrará) a mensagem secreta. A maneira como esta codificação/decodificação é realizada, geralmente faz uso de uma chave (regra ou fórmula) conhecida apenas entre emissor e receptor. Quase sempre, o processo de decodificação é o inverso da codificação, o que definirá este método criptográfico como simétrico.

Obviamente, pode ser do interesse de um terceiro personagem (geralmente o inimigo ou espião) “burlar” ou “quebrar” o código, interceptando a mensagem e, mesmo sem conhecimento da chave combinada entre emissor e receptor, tentar

decifrar a mensagem secreta. Carneiro (2017, p.3) detalha que: “a contínua batalha entre os codificadores e os decifradores de códigos inspiraram toda uma série de notáveis descobertas científicas. Os codificadores estavam sempre criando códigos cada vez mais fortes, enquanto os decifradores estavam sempre querendo encontrar alguma fraqueza nesses códigos”.

Singh (2001, p.32) denomina-os como criptógrafos e criptoanalistas, termos bem conhecidos na área: “(...) a criptoanálise, a ciência que permite decifrar uma mensagem sem conhecer a chave”. De qualquer forma, emissor e receptor podem escolher diferentes técnicas para comunicarem-se secretamente, onde os métodos variam quanto à segurança e complexidade. Carneiro (2017, p. 4) define que a criptografia tradicional pode ser dividida em dois ramos: substituição e transposição (alguns métodos combinam ambos).

A seguir, serão exemplificados métodos criptográficos que serão utilizados nas atividades da sequência didática.

2.1.1 Cifras de Substituição

A cifra de substituição consiste em trocar uma letra ou conjunto de letras por outras letras, símbolos ou números, considerando-se um alfabeto cifrado em relação ao alfabeto original. Quando cada letra do alfabeto original (no caso do nosso alfabeto consideram-se vinte e seis letras) apresenta correspondência única com um símbolo ou conjunto de símbolos de apenas um alfabeto cifrado, diz-se que a substituição é monoalfabética.

Exemplo 1. Conforme o que pode ser visto em Singh (2001, p. 43), na Idade Média, religiosos estudiosos da Bíblia ficavam intrigados com o fato de que o Velho Testamento continha trechos criptografados, codificados com o que ficou conhecido como *atbash*, uma forma tradicional de substituição hebraica. Neste sistema, a primeira letra do alfabeto hebreu (*aleph*) é substituída pela última (*taw*), a segunda letra (*beth*) é trocada pela penúltima (*shin*). Destas quatro letras deriva o nome da cifra: **A**leph, **T**aw, **B**eth, **Sh**in.

Aplicando a mesma ideia ao nosso alfabeto, tem-se:

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

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

Observa-se que a palavra COLÉGIO seria cifrada como XLOVTRL, por exemplo.

Exemplo 2. Singh (2001, p. 405) também explica o funcionamento de outro tipo de cifra de substituição monoalfabética: a cifra do chiqueiro – do inglês, *pigpen* – usada por maçons livres por volta de 1700. Cada letra do alfabeto é trocada por um símbolo segundo o contorno do padrão estabelecido pela chave abaixo.

E	S	C	O	L	A	D	E	A	P	E	R	F	E	I	C	O	A	M	E	N	T	O
□	⋁	∟	⊡	⊡	⌟	⌐	□	⌟	⌝	□	⌜	⊏	□	⌜	∟	⊡	⌟	⌐	□	⊡	>	⊡

Na mensagem “ESCOLA DE APERFEIÇOAMENTO”, suprimiu-se espaços e usou-se o C no lugar do Ç. Assim, a mensagem codificada ficou: □⋁∟⊡⊡⌟⌐□⌟⌝□⌜⊏□⌜∟⊡⌟⌐□□⊡>⊡ .

Exemplo 3. Coutinho (2014 p. 2) traz informações sobre o imperador romano Júlio César, que utilizava uma técnica de cifra por substituição que mais tarde ficou conhecida por seu nome: Cifra de César. Com ela, mensagens ao campo de batalha eram repassadas, distraindo o inimigo. A ideia é usar um alfabeto cifrado, deslocado um determinado número de posições em relação ao alfabeto original. No Quadro 1 abaixo, tem-se um alfabeto deslocado de quatro posições.

Quadro 1 – Exemplo de alfabeto cifrado.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto cifrado	E	F	G	H	I	J	K	L	M	N	O	P	Q

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Fonte: o autor.

Utilizando o alfabeto cifrado do Quadro 1, uma frase como "MATEMÁTICA PARA TODOS" ficaria QEXIQAXMGETEVEXSHSW, onde foram suprimidos espaços e pontuação.

Ainda que este tipo cifra seja muito simples, foi muito eficiente na época de Júlio César. Tanto que foi adotada muitos anos depois, na Guerra Civil americana, conforme traz Singh (2001, p. 144). Eram utilizados discos concêntricos, como os da Figura 1, contendo todas as letras do alfabeto.

Figura 1 - Discos concêntricos.

Fonte: Disponível em: <https://www.amazon.com/Classic-Caesar-Cipher-Medallion Decoder/dp/B004D1L0B0>. Acesso em: 04 Jul 2019.

Exemplo 4. Alvarenga (2010, p. 21) descreve uma cifra de substituição de origem no século II a.C, que ficou conhecida pelo nome do historiador grego Políbio, sendo que este explica o funcionamento da cifra. A ideia é dispor as letras em um quadrado de cinco linhas e cinco colunas. Adaptado para nosso alfabeto de 26 letras, podemos colocar as letras I e J em uma mesma célula, levando este fato em consideração na codificação e decodificação, para que a mensagem faça sentido.

Quadro 2 – Cifra de Políbio

	Coluna 1	Coluna 2	Coluna 3	Coluna 4	Coluna 5
Linha 1	A	B	C	D	E
Linha 2	F	G	H	I/J	K
Linha 3	L	M	N	O	P
Linha 4	Q	R	S	T	U
Linha 5	V	W	X	Y	Z

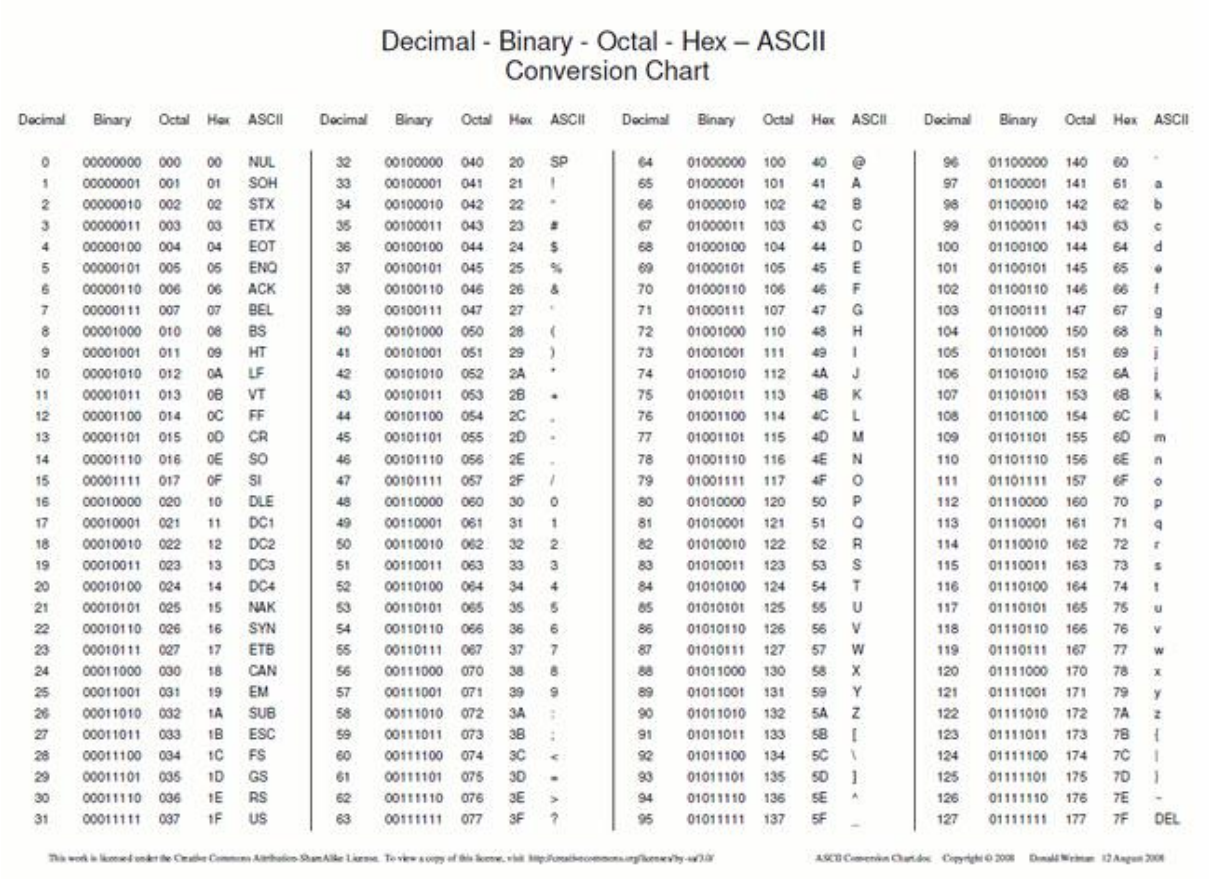
Fonte: o autor.

Na codificação, cada letra é substituída observando, respectivamente, a linha e a coluna ao qual pertence. A mensagem ESAO, por exemplo, seria codificada como 15431134. Na decodificação, basta fazer o processo inverso, pois sabe-se que cada letra é substituída por dois números. Variações da cifra de Políbio podem

ocorrer, aumentando a segurança e alterando os símbolos utilizados nas linhas e colunas das letras, desde que previamente combinadas entre emissor e receptor.

Exemplo 5. Um paralelo que pode ser realizado com a cifra de substituição é a representação de caracteres como números em diferentes bases numéricas, mais precisamente com a Tabela ASCII (*American Standard Code for Information Interchange*) apresentada na Figura 2 abaixo.

Figura 2 – Tabela ASCII



Decimal - Binary - Octal - Hex – ASCII
Conversion Chart

Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
0	00000000	000	00	NUL	32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
1	00000001	001	01	SOH	33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
2	00000010	002	02	STX	34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
3	00000011	003	03	ETX	35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
4	00000100	004	04	EOT	36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
5	00000101	005	05	ENQ	37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
6	00000110	006	06	ACK	38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
7	00000111	007	07	BEL	39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
8	00001000	010	08	BS	40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
9	00001001	011	09	HT	41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
10	00001010	012	0A	LF	42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
11	00001011	013	0B	VT	43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
12	00001100	014	0C	FF	44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
13	00001101	015	0D	CR	45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
14	00001110	016	0E	SO	46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
15	00001111	017	0F	SI	47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
16	00010000	020	10	DLE	48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
17	00010001	021	11	DC1	49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
18	00010010	022	12	DC2	50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
19	00010011	023	13	DC3	51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
20	00010100	024	14	DC4	52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
21	00010101	025	15	NAK	53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
22	00010110	026	16	SYN	54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
23	00010111	027	17	ETB	55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
24	00011000	030	18	CAN	56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
25	00011001	031	19	EM	57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
26	00011010	032	1A	SUB	58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
27	00011011	033	1B	ESC	59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
28	00011100	034	1C	FS	60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
29	00011101	035	1D	GS	61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
30	00011110	036	1E	RS	62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
31	00011111	037	1F	US	63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Fonte: Disponível em: <https://wiki.sj.ifsc.edu.br>. Acesso em: 05 Jul 2019.

A Tabela ASCII é usada para representar textos em computadores, codificando 128 caracteres (entre letras do alfabeto, sinais de pontuação e símbolos matemáticos). Desenvolvida a partir de 1960, muitos sistemas de codificação moderna na computação ainda a utilizam com base.

Particularmente, as letras maiúsculas do alfabeto variam, na representação decimal, de 65 (para o “A”) até o 90 (para o “Z”) com a consequente representação em outras bases numéricas como a binária, a octal e a hexadecimal. Observa-se

que a letra F, por exemplo, cuja representação decimal é o número 70, é representada na base binária como 01000110. Uma sugestão de atividade envolvendo a conversão entre as bases decimal e binária ocorre na Nota de Aula 03 (Apêndice E).

Por muitos anos, cifras de substituição monoalfabética foram largamente utilizadas e consideradas praticamente inquebráveis (pelo menos em tempo hábil). Porém, conforme a humanidade foi elevando seu nível de conhecimento em diversas áreas como estatística e linguística, por exemplo, os criptoanalistas ganharam ferramentas adequadas para "quebrar" este tipo de cifra. Surge então a análise de frequências.

Dentro de cada idioma, as letras do alfabeto utilizado podem aparecer com maior ou menor frequência. Na Língua Portuguesa, esta frequência, em porcentagem, é mostrada no Quadro 3.

Quadro 3 - Frequência das letras na Língua Portuguesa.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: (COUTINHO, 2014, p.3).

Ou seja, no contato com um texto cifrado usando substituição monoalfabética, o símbolo que aparecer com maior frequência provavelmente será a letra "A". As vogais aparecem mais que as consoantes; além disso, em nosso idioma é comum o uso de dígrafos (NH, LH, SS, RR, por exemplo) que funcionam como "dicas" aos criptoanalistas. Em resposta, os criptógrafos criaram melhorias para as cifras de substituição monoalfabética, como escrever deliberadamente uma mensagem com ortografia incorreta (porém sem perder o sentido original) ou acrescentar caracteres nulos no texto.

Os caracteres nulos não possuíam correspondente no alfabeto original, servindo de distração ao criptoanalista, mas eram de conhecimento do receptor, que sabia que deviam ser ignorados. Mesmo assim, para um criptoanalista experiente, não costumavam ser obstáculo suficiente. Era preciso criar uma cifra mais forte. Surgiram então cifras mais complexas, conhecidas como polialfabéticas, dos quais cita-se o quadrado de Vigènere, um tipo de código que, como o próprio nome sugere, utiliza vários alfabetos cifrados. Embora mais complexas, as cifras polialfabéticas também foram “quebradas” com o tempo.

2.1.2 Cifras de Transposição

Na transposição, as letras da mensagem são simplesmente rearranjadas (embaralhadas) criando anagramas. Por exemplo: a palavra CMB (Colégio Militar de Brasília) possui seis anagramas distintos: CMB, CBM, MBC, MCB, BCM e BMC. Porém, com uma noção mínima de combinatória, percebe-se que quanto maior a mensagem, maiores são as possibilidades de anagramas distintos. Uma palavra relativamente curta, como “Militar”, por exemplo, possui 2520 anagramas possíveis. Imagine um texto inteiro.

Isto cria uma boa dose de segurança, pois seriam muitas possibilidades a serem testadas pelo criptoanalista. Por outro lado, alguns destes anagramas podem ser mais sugestionáveis que outros. Além disso, como o receptor irá codificar a mensagem? O exemplo abaixo ilustra o funcionamento de um tipo de cifra de transposição.

Exemplo 1. Suponha que se queira cifrar a mensagem "ESTOU APRENDENDO MATEMÁTICA". Uma maneira de fazê-la é que emissor e receptor convencionem uma chave. Escolhendo-se LIVRO, o resultado será a criação do Quadro 4 abaixo:

Quadro 4 – Exemplo de cifra de transposição.

ORDEM	**2**	**1**	**5**	**4**	**3**
CHAVE	**L**	**I**	**V**	**R**	**O**
MENSAGEM ORIGINAL	E	S	T	O	U
	A	P	R	E	N
	D	E	N	D	O
	M	A	T	E	M

	A	T	I	C	A

Fonte: o autor.

No Quadro 4, o número 21543 é a ordem alfabética que as letras ocorrem dentro da palavra LIVRO: I é a primeira letra; L é a segunda, O é a terceira, R a quarta e V a quinta. A mensagem é escrita linha após linha. A cifra é obtida lendo as colunas na ordem numérica. Assim, suprimindo espaços e acento, ESTOUAPRENDENDOMATEMATICA resulta em SPEATEADMAUNOMAOEDECTRNTI. Para a decodificação, o receptor divide a mensagem codificada em palavras de cinco letras cada (número de letras da palavra-chave LIVRO) e organiza o resultado até também obter o Quadro 4.

Outra forma de cifra por transposição é conhecida como "cerca de ferrovia" – do inglês, *rail fence* – trazida no exemplo seguinte.

Exemplo 2. O objetivo é cifrar a mensagem "COLÉGIO MILITAR". A ideia consiste em escrever a mensagem alternando as letras em duas linhas diferentes (variações desta técnica podem usar três ou mais linhas). O resultado pode ser conferido no Quadro 5, abaixo.

Quadro 5 - Exemplo da cifra "cerca de ferrovia".

Linha 1	C		L		G		O		I		I		A	
Linha 2		O		E		I		M		L		T		R

Fonte: o autor.

O texto cifrado fica: CLGOIIAOEIMLTR, onde foram suprimidos espaços e acento. O receptor deve simplesmente reverter o processo para obter a mensagem original. É um tipo de cifra simples e, talvez por isso mesmo, muito vulnerável.

2.2 Fatos Relevantes

Nesta seção serão trazidos alguns exemplos que ilustram a importância da criptografia em diferentes momentos da História, corroborando com o fato de que a informação é um bem valioso e de que a comunicação entre as fontes deve ser segura e adequada. Para uma leitura mais completa destes fatos, recomenda-se Singh (2001).

2.2.1 A Máquina Enigma

A Enigma foi uma máquina criptográfica utilizada pelo exército alemão durante a Segunda Guerra Mundial (1939-1945), com o objetivo de estabelecer segurança na comunicação entre o comando e a frota de navegação. O criador da Enigma foi o engenheiro alemão Alan Scherbius.

A grande dificuldade, na época, de decifrar a Enigma (Figura 3) explica-se pelo seu funcionamento: dentro de cada máquina existiam três discos com cifras, chamados de rotores, que poderiam ser substituídos ou retirados. Cada rotor possui um alfabeto de A a Z, ligado à diferentes sistemas internos de fiação. Quando uma letra do texto original é acionada no teclado da Enigma, os rotores são acionados de acordo com uma configuração pré-estabelecida. O resultado é que uma luz, no painel de lâmpadas, ficava acesa, indicando a letra codificada. Cada vez que uma letra era pressionada, os rotores mudavam de posição e, se esta mesma letra fosse acionada posteriormente, provavelmente seria cifrada de forma distinta.

Figura 3 – A Máquina Enigma.

Fonte: Disponível em: <https://www.theregister.co.uk/2015/10/23/enigma_machine_4_rotor_sale/> Acesso em: 04 Jul 2019.

Outras versões da Enigma, poderiam ter cinco ou mais rotores, aumentando a segurança. Toda a segurança dependia da chave, que neste caso era a configuração inicial dos rotores. Por isto, os alemães alteravam a chave todos os dias e os operadores de codificação recebiam um livro-código com as chaves usadas no mês. Estes livros, além de serem bem guardados, geralmente eram escritos com tinta solúvel, sendo mergulhados na água em caso de contato com o inimigo. Os alemães acreditavam que a Enigma era "inquebrável" pois seria impossível para os aliados descobrir a chave entre bilhões de possibilidades a serem testadas dentro de um dia.

Fato é que antes mesmo da Segunda Guerra, intelectuais poloneses já estudavam maneiras de decifrar a Enigma e grandes avanços foram feitos pelo matemático Marian Rejewski. Estas descobertas foram passadas aos franceses e ingleses.

Naquela época, as mensagens eram transmitidas usando código Morse. Uma vez interceptadas pelos ingleses, eram encaminhadas para um lugar chamado Bletchley Park - onde diversos estudiosos reuniam esforços para quebrar os códigos recebidos. Entre estes, encontrava-se Alan Turing, matemático britânico que sempre demonstrou brilhantismo intelectual diferenciado.

Turing idealizou uma máquina construída especificamente para quebrar os códigos da máquina Enigma. Suas ideias foram o princípio do computador moderno. O sucesso na empreitada de decodificar estes códigos certamente alterou o rumo da guerra. Acredita-se que muitas vidas foram salvas, antecipando o fim da guerra em pelo menos três anos.

Obviamente, houve todo um esforço conjunto: pesquisadores, serviço de espionagem e militares em objetivo comum. Isto não diminui o intelecto de Turing. É também desta época que a criptografia começou a ser uma área dominante dos matemáticos (até então era creditada a linguistas e historiadores).

Infelizmente, Turing não viveu para ter o reconhecimento público que merecia. Homossexual assumido (o que era crime na época), foi obrigado a ser submetido a um tratamento hormonal. Deprimido, suicidou-se em 7 de junho de 1954, aos 42 anos. Acrescenta-se ainda o fato de que as descobertas sobre a Enigma não puderam ser reveladas até a década de 1970.

2.2.2 Código Morse

O código Morse é um sistema de representação de letras, algarismos e sinais de pontuação que utiliza apenas sequências de pontos, traços e espaços. Foi criado por Samuel Morse, inventor americano e criador do telégrafo elétrico, em 1835. O código Morse não é, por si só, uma forma de criptografia, porque a mensagem final não precisa, necessariamente, ficar oculta. No entanto, costuma ser usado juntamente com métodos criptográficos quando exigido algum tipo de segurança.

A mensagem em Morse pode ser transmitida de várias maneiras, utilizando pulsos (ou tons) curtos e longos, como em sinais elétricos, ondas sonoras ou sinais visuais. Abaixo, a Figura 4 com alguns caracteres:

Figura 4 – O Código Morse.

A •–	J •–––	S •••	2 ••–––
B –•••	K –•–	T –	3 •••–––
C –•–•	L •–••	U ••–	4 ••••–
D –••	M ––	V •••–	5 •••••
E •	N –•	W •––	6 –••••
F ••–•	O –––	X –••–	7 ––•••
G ––•	P •––•	Y –•––	8 –––••
H ••••	Q ––•–	Z ––••	9 ––––•
I ••	R •–•	1 •––––	0 –––––

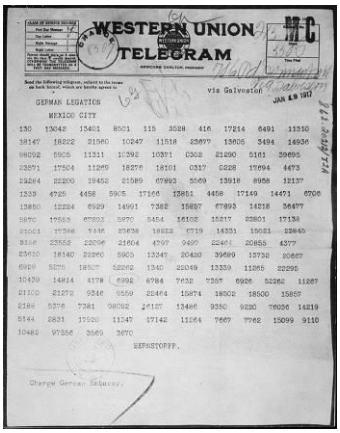
Fonte: Disponível em: <https://brasilescola.uol.com.br/geografia/codigo-morse.htm>. Acesso em 31 Jul 2019.

Embora considerado atualmente obsoleto, o código Morse teve amplo uso durante o século XX em conflitos como a 2ª Guerra Mundial.

2.2.3 O telegrama Zimmermann

Não raras vezes, a criptografia mudou o rumo de guerras e tramas políticas. O telegrama Zimmermann (Figura 5) é um exemplo disto.

Figura 5 – Telegrama Zimmermann



Fonte: Disponível em: <https://www.historytoday.com/david-nicholas/lucky-break-zimmermann-telegram>. Acesso em: 04 Jul 2019.

Arthur Zimmermann era o Ministro das Relações Exteriores da Alemanha em 1917. Um telegrama, codificado, foi enviado para Heinrich von Eckardt, embaixador alemão no México durante a Primeira Guerra Mundial. O telegrama propunha uma aliança com o México para atacar os Estados Unidos. Porém, a mensagem foi interceptada e decodificada pelos britânicos que alertaram os americanos. Este fato, acelerou a entrada dos EUA na Primeira Guerra Mundial, que até então mantinha posição de neutralidade.

Tudo foi feito de maneira secreta pelos britânicos. Quando o conteúdo do telegrama foi revelado, os alemães acharam que a falha foi dos mexicanos. A autenticidade do telegrama foi confirmada pelo próprio Zimmermann.

2.2.4 A modernização da Criptografia

Cifras como as de César e da Máquina Enigma, por exemplo, embora muito úteis em suas respectivas origens, encontram-se obsoletas, não sendo grande desafio para o processamento de um computador. Por isto, métodos mais complexos foram desenvolvidos, aplicados geralmente com o uso de linguagem de programação e outras ferramentas tecnológicas.

Atualmente, a Criptografia cresce em importância, sempre relacionada a debates de privacidade e segurança de redes, não só para governos e militares, mas também para o usuário comum que, mesmo não sabendo, a utiliza nas compras *online* e envio de *e-mail*, gerando contínua pesquisa para obter o sigilo desejado.

3. METODOLOGIA

Quanto à natureza, o presente estudo caracteriza-se por ser uma pesquisa do tipo aplicada, pois tem por objetivo a produção de conhecimentos que tenham aplicação prática e dirigidos à solução de problemas reais específicos, envolvendo verdades e interesses locais, no caso, uma atividade de ensino-aprendizagem para o SCMB. Já quanto à forma de abordagem, enquadra-se como pesquisa qualitativa.

Esta pesquisa também pode ser caracterizada quanto ao objetivo geral, sendo classificada como descritiva, pois pretende descrever processos para a

implementação de uma proposta de ensino de Criptografia no formato de sequência didática.

Para atingir este objetivo, realizou-se uma revisão teórica sobre o assunto, através da pesquisa bibliográfica a material didático e trabalhos científicos (artigos, trabalhos de conclusão de curso, dissertações e teses), dos quais destaca-se a dissertação do Major José Luís dos Santos (SANTOS, 2013) que também pode ser usada como referência e extensão na relação Educação/Criptografia.

Acrescenta-se ainda que a estrutura da sequência didática tem por base orientações do “Caderno de Didática” do SCMB. Este documento traz que: “As sequências didáticas devem ser organizadas de acordo com os objetivos que o professor quer alcançar para a aprendizagem de seus alunos, elas envolvem atividades de aprendizagem e avaliação”, além de serem “(...) um conjunto de atividades ligadas entre si, planejadas para desenvolver um conteúdo etapa por etapa”. (DEPA, 2016, p. 20).

Antes de continuar, é importante salientar os conceitos de Competência, definida como a “faculdade de mobilização de um conjunto de recursos cognitivos com saberes, habilidades e informações para solucionar com pertinência e eficácia uma série de situações” (DEPA, 2016, p. 16) e a definição de Habilidades, que “são os meios pelos quais se pretende atingir os objetivos, ou seja, devem ser desenvolvidas em busca das competências” (DEPA, 2016, p. 17).

Por fim, o conceito de Descritor:

> O descritor é o detalhamento de uma habilidade em face dos processos cognitivos/ operações mentais nela constantes/ envolvidas e que está sempre associada a um conteúdo que o estudante deve dominar na etapa de ensino em análise. Esses descritores são expressos da forma mais detalhada possível, permitindo-se a mensuração por meio de aspectos que podem ser observados. (DEPA, 2016, p. 24).

De fato, os conceitos de Competência, Habilidade e Descritor são fundamentais na elaboração e execução da Sequência Didática.

4. RESULTADOS

Como resultado tem-se a elaboração de uma Sequência Didática que utiliza os modelos de Plano de Execução Didática (PED) e de Plano de Aula (PA) adotados pelo SCMB, conforme segue:

Aulas 01 e 02 – Aspectos Históricos da Criptografia e Principais Conceitos.
Aulas 03 e 04 – Cifra de César e Análise de Frequência.
Aulas 05 e 06 – Cifra de Políbio e Código Binário.
Aulas 07 e 08 – Cifras de Transposição e o Princípio Fundamental da Contagem.
Aulas 09 e 10 – Estudo de Funções Matemáticas associadas à Criptografia.

As competências utilizadas no desenvolvimento da Sequência Didática foram aproveitadas dos Planos de Sequência Didática (PSD) da Matemática do Ensino Fundamental abaixo relacionadas:

C3 – Resolver situações-problema envolvendo números reais, ampliando, construindo e consolidando os significados de adição, subtração, multiplicação, divisão, potenciação e radiciação.

C6 – Produzir e interpretar diferentes escritas algébricas (expressões, igualdades e desigualdades), identificando as equações, inequações e sistemas e aplicá-las na resolução de situações-problema.

C7 – Observar regularidades e estabelecer leis matemáticas que expressem a relação de dependência entre as variáveis.

C13 – Interpretar tabelas e gráficos de dados estatísticos, formular argumentos convincentes e elaborar conclusões a partir da interpretação das informações.

C15 – Valorizar o trabalho em grupo, sendo capaz de ação crítica e cooperativa para a construção coletiva do conhecimento.

C16 – Entender os princípios, a natureza, a função e o impacto das tecnologias da comunicação e da informação na sua vida pessoal e social, no desenvolvimento do conhecimento, associando-os aos conhecimentos científicos, às linguagens que lhe dão suporte, às demais tecnologias, aos processos de produção e aos problemas que se propõem solucionar.

As habilidades, associadas a cada uma destas competências, também foram aproveitadas dos PSD de Matemática do Ensino Fundamental. Apenas os descritores foram criados com o devido direcionamento que esta sequência didática de Criptografia propõe. Com isto, foi elaborada uma Matriz de Descritores (MD) que reúne a organização da proposta (Apêndice A) e um Plano de Execução Didática (PED) com o detalhamento das estratégias a serem empregadas, que podem ser observadas no Apêndice B.

Baseado nestes dois documentos, uma carga horária de 10 (dez) horas/aula foi desenvolvida com sugestões de atividades que podem ser adotadas pelos

professores. As quatro primeiras aulas não exigem maiores pré-requisitos, e podem ser aplicadas livremente dos 6º ao 9º anos do Ensino Fundamental. As aulas 05 a 08 são mais adequadas para os 8º e 9º anos, embora, com simplificação e/ou orientações do professor, também possam ser objeto de aprendizado dos 6º e 7º anos. As aulas 09 e 10 exigem pré-requisitos e são direcionadas apenas ao 9º ano do Ensino Fundamental. O ideal é que os alunos já tenham tido contato com o estudo das funções afim e quadrática. Estas aulas serviriam como aprofundamento e discussão sobre funções.

O que segue, são os Planos de Aula seguidos de comentários sobre o desenvolvimento e objetivos destes. As Notas de Aula, indicadas nestes planos, constituem os apêndices indicados.

4.1 Plano de Aula nº 01

A descrição do Plano de Aula nº 01 está ilustrada pela Figura 6 abaixo.

Figura 6 – Plano de Aula nº 01

COLÉGIO MILITAR DE PORTO ALEGRE

PLANO DE AULA

DISCIPLINA: Matemática	Plano de Aula nº 01		
Data: XX/XX/XXXX	Ano: 6º ao 9º	Turmas: Turno Integral	Prof.: Cap Anderson
1. Referência: Sequência Didática 01		**Assunto:** Criptografia	
2. Descritores: D1 a D12, D14 e D15, D26 e D27.			
3. Competência discursiva a ser trabalhada: relacionar conhecimentos de Criptografia em distintos contextos históricos, explorar técnicas simples de codificação e decodificação, contextualizar propriedades dos números naturais e inteiros.			
4. Mediação: Aulas 01 e 02		**Duração:** 2 horas/aula	
Apresentação do OC	Apresentação de *slides* sobre aspectos históricos da Criptografia, bem como conceitos iniciais. A ideia é motivar os alunos destacando a importância da Criptografia na História bem como seu emprego atual.		
Sistematização / significado	Será distribuída uma Nota de Aula aos alunos com os principais pontos vistos na apresentação de *slides* além da aplicação de uma parte prática com métodos criptográficos simples de substituição monoalfabética como a cifra do chiqueiro (*pigpen*) e o atbash. O Código Morse também será apresentado, com auxílio de mensagens sonoras aos alunos obtidas de um aplicativo para celular.		
Resumo / Transcendência	Serão retomados os principais conceitos, salientando que o assunto continuará com o aprendizado de outros métodos criptográficos.		
Avaliação	Os alunos serão observados quanto a realização das atividades propostas na Nota de Aula.		
Observações Gerais:	Anexo a este Plano de Aula, segue a Nota de Aula a ser distribuída aos alunos.		

Fonte: o autor.

Considerando que seja o primeiro contato com o tema, é importante apresentar aos alunos os principais conceitos e definições que serão corriqueiros nas próximas aulas, além dos aspectos históricos que certamente enriquecerão o aprendizado. Sugere-se que esta introdução seja realizada por meio de *slides*, com muitas ilustrações e vídeos sobre o assunto. A abordagem histórica pode ser de maneira mais geral, detalhando alguns fatos como a Máquina Enigma e o Telegrama Zimmermann. O código Morse também é um ponto a ser considerado, principalmente pela associação com a atividade militar, sendo de domínio até hoje de militares da arma de Comunicações.

Depois deste momento inicial, pode-se seguir no aprendizado de alguns métodos criptográficos simples, conforme sugestão da Nota de Aula 01 (Apêndice C). As atividades desenvolvidas nesta Nota de Aula estimulam o raciocínio, a concentração e a interpretação diante de instruções simples, o que é algo fundamental no aprendizado, principalmente da Matemática. Os debates e o trabalho em grupo também podem fortalecer a experiência obtida com estas aulas.

O destaque final destas aulas é sobre o “Exercício 7”, aproveitado da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). É sempre estimulante agregar um exercício de olimpíada, seja pelo desafio, seja pelas reflexões que eles costumam propor. No caso, discussões sobre o Teorema Fundamental da Aritmética – que trata da decomposição em fatores primos de um número inteiro – podem ser realizadas com intervenção adequada do professor.

4.2 Plano de Aula nº 02

O Plano de Aula nº 02 está ilustrado pela Figura 7 abaixo.

Figura 7 – Plano de Aula nº 02.

COLÉGIO MILITAR DE PORTO ALEGRE

PLANO DE AULA

DISCIPLINA: Matemática		Plano de Aula nº 02	
Data: XX/XX/XXXX	Ano: 6º ao 9º	Turmas: Turno Integral	Prof.: Cap Anderson
1. Referência: Sequência Didática 01		**Assunto:** Criptografia	
2. Descritores: D11, D12, D16, D17, D21 a D25, D28 a D31.			
3. Competência discursiva a ser trabalhada: explorar técnicas simples de codificação e decodificação, porcentagem, tabela, gráficos estatísticos.			
4. Mediação: Aulas 03 e 04		**Duração:** 2 horas/aula	
Apresentação do OC	Retomar o conceito de cifra de substituição da aula anterior, bem como os conceitos de emissor e receptor de uma mensagem criptografada.		
Sistematização / significado	O foco desta aula será a Cifra de César, trabalhada por meio de Nota de Aula, com construção de um disco de cifragem que auxiliará nos exercícios propostos.		
Resumo / Transcendência	Reflexão sobre as vulnerabilidades das cifras de substituição por meio de Análise de Frequências das letras no idioma português apresentado em tabela e com noção de sua criação por meio de gráfico de colunas.		
Avaliação	Os alunos serão observados quanto a realização das atividades propostas na Nota de Aula.		
Observações Gerais:	Anexo a este Plano de Aula, segue a Nota de Aula a ser distribuída aos alunos.		

Fonte: o autor.

Estas aulas focam em um tipo particular de cifra de substituição: a Cifra de César. Justamente por sua simplicidade, é possível ter certo nível de debate diante de suas fraquezas, atividade que pode ser bem aceita pelos alunos, justamente pelo desafio de “quebrarem” códigos secretos.

Por isto mesmo, é oportuno o aprendizado da “Análise de Frequências” das letras de uma mensagem codificada. A Nota de Aula 02 (Apêndice D) sugere uma ideia de como esta análise pode ser realizada, associando porcentagem e estatística básica. Outro ponto-chave é o uso do disco de cifragem, que auxiliará em todos os exercícios, tanto na codificação quanto na decodificação.

4.3 Plano de Aula nº 03

O Plano de Aula nº 03 está ilustrado pela Figura 8 abaixo.

Figura 8 – Plano de Aula nº 03.

COLÉGIO MILITAR DE PORTO ALEGRE

PLANO DE AULA

DISCIPLINA: Matemática		Plano de Aula nº 03	
Data: XX/XX/XXXX	Ano: 6º ao 9º	Turmas: Turno Integral	Prof.: Cap Anderson
1. Referência: Sequência Didática 01		**Assunto:** Criptografia	
2. Descritores: D13, D18, D19 e D20.			
3. Competência discursiva a ser trabalhada: explorar técnicas simples de codificação e decodificação, bases numéricas.			
4. Mediação: Aulas 05 e 06		**Duração:** 2 horas/aula	
Apresentação do OC	Continuando a aula anterior, serão apresentadas mais técnicas de cifras de substituição: a Cifra de Políbio e uma possibilidade de cifra de substituição utilizando o Código Binário, ambas desenvolvidas segundo a distribuição de uma Nota de Aula.		
Sistematização / significado	O aprendizado da Cifra de Políbio serve como atividade complementar das aulas anteriores. O foco desta aula será entender parte da construção da Tabela ASCII (*American Standard Code for Information Interchange*) com a compreensão do uso de uma base binária.		
Resumo / Transcendência	Haverá um momento de reflexão e discussão sobre a importância da pesquisa e da Matemática nas diversas áreas de tecnologia e informação.		
Avaliação	Os alunos serão observados quanto a realização das atividades propostas na Nota de Aula.		
Observações Gerais:	Anexo a este Plano de Aula, segue a Nota de Aula a ser distribuída aos alunos.		

Fonte: o autor.

A cifra de Políbio, apresentada nesta aula, visa fixar o trabalho desenvolvido com as cifras de substituição. Sua aplicação é relativamente simples, exigindo basicamente atenção e concentração dos discentes, onde a ordenação entre linhas e colunas é fundamental.

A Nota de Aula 03 (Apêndice E) também traz atividades envolvendo códigos binários com a apresentação da Tabela ASCII. Estas são aulas que facilmente podem ser ampliadas, inclusive com a representação em outras bases numéricas como a octal e a hexadecimal, ambas de uso corriqueiro em computação.

4.4 Plano de Aula nº 04

O Plano de Aula nº 04 está ilustrado pela Figura 9 abaixo.

Figura 9 – Plano de Aula nº 04.

COLÉGIO MILITAR DE PORTO ALEGRE

PLANO DE AULA

DISCIPLINA: Matemática		Plano de Aula nº 04	
Data: XX/XX/XXXX	Ano: 6º ao 9º	Turmas: Turno Integral	Prof.: Cap Anderson
1. Referência: Sequência Didática 01		**Assunto:** Criptografia	
2. Descritores: D32 a D39.			
3. Competência discursiva a ser trabalhada: explorar técnicas simples de codificação e decodificação, combinatória, anagrama.			
4. Mediação: Aulas 07 e 08		**Duração:** 2 horas/aula	

Apresentação do OC	Será apresentada o conceito de cifra de transposição em comparação com as técnicas de cifras de substituição trabalhadas nas aulas anteriores.
Sistematização / significado	Por meio de Nota de Aula, os alunos terão contato com exercícios de codificação e decodificação com técnicas de transposição como a cerca de ferrovia. Será realizado um paralelo com a combinatória, mais precisamente o Princípio Fundamental da Contagem e o cálculo da quantidade de anagramas de uma mensagem.
Resumo / Transcendência	Os aplicativos para *smartphone Decrypto* e *Criptography*, ambos gratuitos, serão sugeridos nas atividades, complementando o estudo e permitindo aos alunos explorarem possibilidades além de ser uma nova oportunidade na troca de mensagem secretas.
Avaliação	Os alunos serão observados quanto a realização das atividades propostas na Nota de Aula.
Observações Gerais:	Anexo a este Plano de Aula, segue a Nota de Aula a ser distribuída aos alunos.

Fonte: o autor.

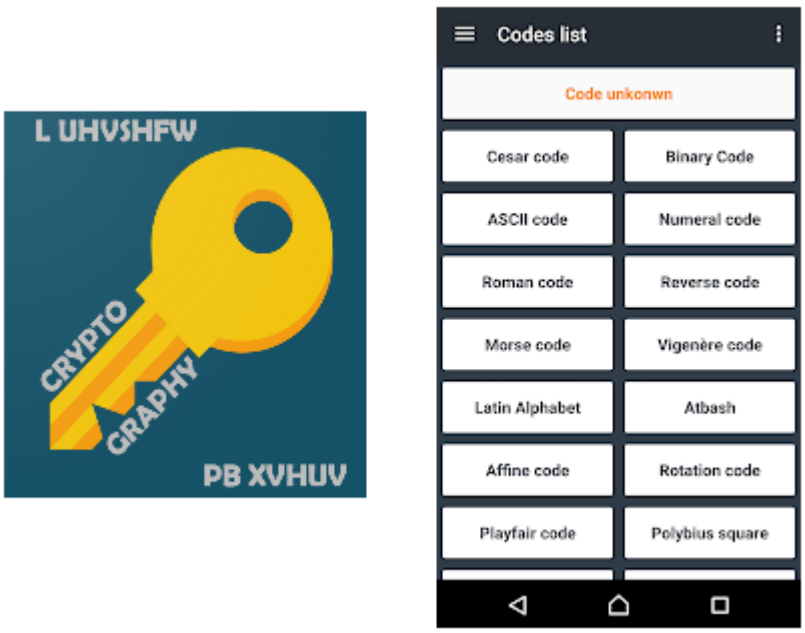
Estas aulas apresentam um tipo distinto das cifras de substituição trabalhadas anteriormente: as cifras de transposição. A Nota de Aula 04 (Apêndice F) propõe inicialmente o entendimento destas técnicas para posterior relação com Análise Combinatória, focando no Princípio Fundamental da Contagem. Possivelmente, esta relação com a combinatória possa ter maior direcionamento para alunos de 8º e 9º anos de Ensino Fundamental, embora as ferramentas para seu entendimento sejam bem simples, pois os exercícios exigem apenas contagem de anagramas. O professor pode fazer adaptações conforme achar conveniente, com algumas aulas anteriores sobre o assunto, por exemplo.

Ideias simples de contagem já devem ser trabalhadas no Ensino Fundamental, conforme apontam documentos como a BNCC (Base Nacional Comum Curricular) que estão sendo levados em consideração nas revisões curriculares do SCMB.

Estas aulas podem ser particularmente interessantes pela sugestão de emprego dos aplicativos para *smartphone Decrypto* e *Cryptography* (Figura 10). Ambos são bem intuitivos (mesmo na versão em inglês) e gratuitos, podendo inclusive auxiliar o professor na montagem das atividades, pois codificam e decodificam mensagens em todas as técnicas sugeridas nestas e nas aulas anteriores.

Recomenda-se o uso destes aplicativos em momento posterior ao aprendizado “manual” de algumas técnicas de codificação. Os alunos podem verificar seus erros e trocarem mensagens secretas entre si, fato que torna este uso oportuno, mas não acrescenta maior inferência ou discussão, e sim complementaridade do que foi desenvolvido.

Figura 10 – Interface dos aplicativos *Cryptography* e *Decrypto*.



Fonte: o autor.

4.5 Plano de Aula nº 05

O Plano de Aula nº 05 está ilustrado pela Figura 11 abaixo.

Figura 11 – Plano de Aula nº 05.

COLÉGIO MILITAR DE PORTO ALEGRE

PLANO DE AULA

DISCIPLINA: Matemática		Plano de Aula nº 05	
Data: XX/XX/XXXX	Ano: 9º	Turmas: Turno Integral	Prof.: Cap Anderson
1. Referência: Sequência Didática 01		**Assunto:** Criptografia	
2. Descritores: D40 a D48.			
3. Competência discursiva a ser trabalhada: explorar técnicas simples de codificação e decodificação, valor numérico, equação, função, função inversa, injetividade, domínio, contradomíno e gráfico de uma função.			
4. Mediação: Aulas 09 e 10		**Duração:** 2 horas/aula	
Apresentação do OC	Será feita relação entre Funções e Criptografia, focando nas funções do tipo afim e quadrática. Da maneira que esta será construída, será feito um paralelo com as cifras de substituição.		
Sistematização / significado	Por meio de Nota de Aula, serão propostos exercícios de codificação e decodificação com funções matemáticas, permitindo ao aluno atividades com o cálculo do valor numérico de uma função, resolução de equações, análise de gráfico e obtenção da lei de uma função inversa.		
Resumo / Transcendência	Os exercícios também propõem reflexões sobre injetividade, domínio e contradomínio de uma função.		
Avaliação	Os alunos serão observados quanto a realização das atividades propostas na Nota de Aula.		
Observações Gerais:	Anexo a este Plano de Aula, segue a Nota de Aula a ser distribuída aos alunos.		

Fonte: o autor.

Como citado anteriormente, as aulas 09 e 10 exigem pré-requisitos, sendo indicadas para o 9º ano do Ensino Fundamental, onde o ideal é que os alunos já tenham trabalhado funções afim e quadrática, pois a sugestão de atividades da Nota de Aula 05 (Apêndice G) é constituída de exercícios que exigem certa investigação matemática.

Neste sentido, após o esboço manual dos gráficos das funções envolvidas, pode ser realmente agregador o uso do *software Geogebra*. O *Geogebra* foi desenvolvido com cunho educacional, permitindo explorar graficamente funções e

aspectos geométricos, por exemplo. Seu uso é livre e intuitivo, disponível *online* (sem a necessidade de *download*) ou como aplicativo.

5. DISCUSSÃO

Na elaboração desta sequência didática foram levadas em consideração todas as particularidades do SCMB, sendo esta estruturada segundo o ensino de competências e habilidades, com a consequente criação de uma Matriz de Descritores (MD), um Plano de Execução Didática (PED) e os Plano de Aula (PA) seguindo modelos sugeridos pela DEPA. Isto poderia tornar esta proposta bem específica, mas mesmo com atualizações curriculares, as atividades se mantêm, visto que objetivam oportunizar raciocínio, concentração e interpretação, além debates sobre assuntos rotineiros da Matemática. Adequações seriam simples devido ao fato de que o estudo da Criptografia é bem amplo e transversal.

Outro ponto a ser considerado, é que a oportunidade de trabalhar com o turno integral não ocorreu por acaso. Com a implementação deste nos colégios militares, surgiram desafios de criar atividades da área cognitiva que complementassem e aprimorassem o ensino do turno regular. Não seria admissível exigir de nosso aluno que permaneça uma ou duas tardes por semana, por mais três ou seis horas, em atividades que pouco contribuam para seu desenvolvimento pedagógico. Não deve existir espaço para amadorismo em Educação. É preciso levar em conta o planejamento e a seriedade esperados de nosso ensino e pensar como sistema no que se deseja para a formação de nossos alunos.

Assim, esta proposta parte como premissa de sugestões de atividades, mas aqui também se registra uma reflexão sobre o turno integral: não seria mais adequado nos prepararmos enquanto escola, com formação dos professores, metas bem definidas, infraestrutura e logística? Particularmente sobre a Matemática, o que pode ser feito? Com este trabalho, espera-se que a Criptografia possa ser uma ferramenta do professor, mas também pode-se levantar outras necessidades de formação global do aluno como educação financeira, só para citar um exemplo.

Voltando ao tema Criptografia, chama-se a atenção para a diversidade de possibilidades. Este trabalho apresenta algumas destas possibilidades, delimitadas, principalmente por terem sido pensadas para o Ensino Fundamental. No entanto,

outros direcionamentos poderiam ser tomados, como a Cifra de Hill e o estudo de matrizes, assunto do Ensino Médio. Ou seja, mais oportunidades para o professor.

De fato, a própria sequência didática aqui apresentada pode derivar em outras aulas, com maior aprofundamento e discussão no turno integral, de acordo com o público, mas também em atividades pontuais para o turno regular, podendo ser estendida para projetos e pesquisa em feiras de ciências, por exemplo, criando ambientes propícios de aprendizado, além de explorar habilidades desejáveis para todos nossos discentes, como traz o Caderno de Didática (DEPA, 2016, p. 37):

> No ensino por competências, um de seus pressupostos teóricos centra-se na capacidade de aprender a aprender. Esta capacidade destaca a necessidade de que os alunos não adquiram somente o conjunto de conhecimentos já elaborados, mas que adquiram habilidades e estratégias que lhes permitam aprender por si mesmos, ou seja, construírem novos conhecimentos, construírem sua aprendizagem.

Todas as atividades da sequência didática têm caráter motivacional, algo fomentado em nossos documentos orientadores: “As situações-problemas podem ser apresentadas inicialmente, como motivação para a aula, ou como um problema a ser resolvido no final da aula. O que não se pode esquecer é de sua capacidade desafiadora para o aluno”. (DEPA, 2016, p. 38).

6. CONCLUSÃO

Ainda no estágio de desenvolvimento do tema, procurou-se, em um primeiro momento, focar em algumas atividades-chave, principalmente as de maior relação com a Matemática do Ensino Fundamental. A Criptografia, como centro deste trabalho, é um assunto de grande amplitude: sigilo e salvaguarda na troca informações, segurança em compras *online*, importância histórica, desenvolvimento de tecnologia, etc.

De fato, desde o primeiro contato com a Criptografia, percebeu-se que as oportunidades com Educação eram diversas, englobando interdisciplinaridade e contextualização em seu estudo. No entanto, justamente por esta variedade de possibilidades era preciso ter em mente um direcionamento correto, principalmente sobre os tópicos a serem relacionados com a Matemática e sobre o público-alvo a ser atingido.

Diante disto e, considerando-se o turno integral do SCMB, esta sequência didática foi criada, tanto como oportunidade de ensino como resposta para uma realidade enfrentada pelos colégios militares - no caso, a elaboração de propostas atrativas sobre a ótica principal da área cognitiva.

Então, acredita-se que o trabalho aqui apresentado tenha alcançado seus objetivos iniciais, ao propor uma sequência didática com sugestões de atividades para o professor interessado. O SCMB está em constante avaliação de seu desempenho, atualizando metas e metodologias empregadas, como apontam as revisões curriculares necessárias em qualquer projeto pedagógico. Porém, mesmo que estas revisões alterem documentos e direcionamentos, salienta-se que a sequência didática aqui desenvolvida deve manter-se sólida o suficiente, dado à flexibilidade e amplitude da relação Criptografia/Matemática com a Educação. Espera-se, realmente, que a leitura deste trabalho tenha sido pertinente e reflexiva, contribuindo de forma edificante com as particularidades do nosso sistema de educação.

Por fim, acrescenta-se que a validade desta proposta tornar-se-á maior com a aplicação em sala de aula, para que os documentos elaborados sejam consolidados.

REFERÊNCIAS

ALVARENGA, Luiz Gonzaga de. **Criptografia clássica e moderna.** 2ª Ed. Clube de Autores, 2010.

BRASIL. Ministério da Defesa. **Caderno de Didática do Sistema Colégio Militar do Brasil.** Elaborado em 2016. Disponível em: <http://www.depa.eb.mil.br/images/secs/ensino/caderno_de_ditatico.pdf>. Acesso em 04 Jul 2019.

BRASIL. Ministério da Defesa. **Projeto Pedagógico do Sistema Colégio Militar do Brasil.** Promulgado em 18 de maio de 2016. Disponível em: <http://www.depa.eb.mil.br/images/legislacao/Projeto_Pedagogico_2019_versao_SCMB.pdf>. Acesso em 04 Jul 2019.

BRASIL. Ministério da Defesa. **Normas e Planejamento de Gestão Escolar (NPGE).** Elaboradas em outubro de 2018. Disponível em: <http://www.depa.eb.mil.br/legislacao>. Acesso em 04 Jul 2019.

CARNEIRO, Framilson José Ferreira. **Criptografia e Teoria dos Números.** Rio de Janeiro: Editora Ciência Moderna Ltda, 2017.

COUTINHO, Severino Collier. **Programa de Iniciação Científica da OBMEP:** Criptografia. Rio de Janeiro: IMPA, 2014.

HEFEZ, Abramo. **Aritmética:** Coleção PROFMAT. 1ª ed, 2ª impressão. Rio de Janeiro: SBM, 2014.

LORENZATO, Sérgio. **Para aprender matemática:** Coleção Formação de Professores. 3ª ed. Campinas: Autores Associados, 2010.

MACHADO, Anderson Pinheiro. **Teoria dos Números e Criptografia RSA:** uma proposta de ensino para alunos de Matemática Olímpica. Dissertação de Mestrado PROFMAT/UFSM aprovada em 24 de agosto de 2018.

MALAGUTTI, Pedro Luiz. **Atividades de Contagem a partir da Criptografia.** Rio de Janeiro. IMPA, 2015.

SANTOS, José Luiz dos. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de Matemática básica.** Dissertação de Mestrado PROFMAT/UFBA aprovada em 04 de abril de 2013.

SHOKRANIAN, Salahoddin. Criptografia para iniciantes. 2ª ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

SINGH, Simon. **O livro dos códigos:** a ciência do sigilo - do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

APÊNDICE A – MATRIZ DE DESCRITORES

MINISTÉRIO DA DEFESA
DEPARTAMENTO DE EDUCAÇÃO E CULTARA DO EXÉRCITO
DIRETORIADEEDUCAÇÃOPREPARATORIAEASSISTENCIAL
COLÉGIO MILITAR DE PORTO ALEGRE

MATRIZ DE DESCRITORES MATEMÁTICA Turno Integral
Área: Ciências da Natureza, Matemática e suas Tecnologias
Carga-horária: 10 horas

MATEMÁTICA – 6º ao 9º anos

Competência Discursiva: Nas atividades de estudo da Criptografia, os estudantes devem ter oportunidades de, relacionar conhecimentos em contextos históricos, explorando técnicas simples de codificação e decodificação, associadas com o raciocínio e a elaboração de hipóteses, contextualizadas na Matemática por: propriedades dos números naturais e inteiros, porcentagem, tabela, gráficos estatísticos, bases numéricas, combinatória, anagrama, valor numérico, equação, função, função inversa, injetividade, domínio, contradomínio e gráfico de uma função.

COMP	HABILIDADE	DESCRITORES	OBJETO DE CONHECIMENTO
C15	**H44** Elaborar, individualmente e em grupo, relatos orais e outras formas de registro acerca do tema em estudo, considerando informações obtidas por meio de observação, experimentação, textos ou outras fontes.	**D1** Compreender o conceito de Criptografia. **D2** Compreender os conceitos de codificação e decodificação. **D3** Compreender os conceitos de emissor e receptor de uma mensagem no âmbito do estudo de Criptografia. **D4** Comprender o conceito de Criptoanálise.	**1 Criptografia** 1.1 Introdução à Criptografia
	H45 Confrontar as diferentes explicações individuais e coletivas, inclusive as de caráter histórico, para reelaborar suas idéias e interpretações.	**D5** Refletir sobre o uso da Criptografia na História da humanidade. **D6** Relacionar a Criptografia à pesquisa e o desenvolvimento de conhecimento.	

C16	**H48** Reconhecer a função e o impacto social das diferentes tecnologias da comunicação e informação.	**D7** Situar o uso cotidiano e atual da Criptografia associada à tecnologia e segurança de dados.	
	H49 Identificar, pela análise de suas linguagens, as tecnologias da comunicação e informação.	**D8** Relacionar o estudo da Criptografia em diferentes áreas do conhecimento. **D9** Fazer uso de aplicativos e *softwares* que explorem recursos relacionados à Criptografia.	
	H50 Relacionar as tecnologias de comunicação e informação ao desenvolvimento das sociedades e ao conhecimento que elas produzem.	**D10** Refletir sobre a importância do desenvolvimento da Criptografia e da pesquisa relacionada com a mesma em um ambiente cada vez mais tecnológico.	
C15	**H44** Elaborar, individualmente e em grupo, relatos orais e outras formas de registro acerca do tema em estudo, considerando informações obtidas por meio de observação, experimentação, textos ou outras fontes.	**D11** Compreender o conceito de cifra de substituição monoalfabética. **D12** Compreender os conceitos de alfabeto original e alfabeto cifrado. **D13** Compreender a construção de uma tabela ASCII.	1.2 Cifras de Substituição
	H45 Confrontar as diferentes explicações individuais e coletivas, inclusive as de caráter histórico, para reelaborar suas idéias e interpretações.	**D14** Compreender o funcionamento da cifra do chiqueiro. **D15** Compreender o funcionamento da cifra atbash. **D16** Compreender o funcionamento da cifra de César. **D17** Construir um disco de cifragem. **D18** Compreender o funcionamento da Cifra de Políbio. **D19** Compreender o funcionamento do código binário. **D20** Compreender o funcionamento do código hexadecimal.	
	H46 Elaborar perguntas e hipóteses, selecionando e organizando dados e ideias para resolver problemas.	**D21** Conhecer uma tabela de Análise de Frequências das letras no idioma português. **D22** Explorar as vulnerabilidades de códigos criados por cifras de substituição. **D23** Criar um sistema de cifra de substituição próprio baseado em alfabeto cifrado próprio.	
	H47 Participar de debates coletivos para a solução de problemas, colocando suas ideias por escrito ou oralmente e reconsiderando sua opinião em face de evidências obtidas por diversas fontes de informação.	**D24** Propor a troca de mensagens secretas utilizando alfabeto cifrado próprio ou cifra de substituição aprendida. **D25** Resolver desafios de criptografia propostos por outros colegas.	

C3	**H8** Analisar, interpretar, formular e resolver situações-problema, compreendendo diferentes significados das operações, envolvendo números naturais, inteiros, racionais e irracionais.	**D26** Explorar particularidades dos números inteiros na criação de códigos associados a um alfabeto original. **D27** Utilizar o Teorema Fundamental da Aritmética como argumentação em problemas envolvendo números inteiros.	
C13	**H38** Organizar dados e construir recursos visuais adequados, como gráficos (de colunas, de setores, histogramas, polígonos de frequência) para apresentar globalmente os dados, destacar aspectos relevantes, sintetizar informações e permitir a elaboração de conclusões.	**D28** Relacionar o cálculo da porcentagem à frequência de uma letra em uma mensagem. **D29** Construir um gráfico de colunas a partir do estudo da Análise de Frequências das letras de uma mensagem.	
	H39 Ler e interpretar dados expressos em tabelas e gráficos.	**D30** Interpretar o significado de uma tabela de porcentagens da Análise de Frequências das letras no idioma português. **D31** Fazer uso da Análise de Frequências na decodificação de mensagens geradas por cifras de substituição	
C15	**H44** Elaborar, individualmente e em grupo, relatos orais e outras formas de registro acerca do tema em estudo, considerando informações obtidas por meio de observação, experimentação, textos ou outras fontes.	**D32** Compreender o conceito de cifra de transposição. **D33** Compreender o conceito de anagrama.	1.3 Cifras de Transposição
	H45 Confrontar as diferentes explicações individuais e coletivas, inclusive as de caráter histórico, para reelaborar suas idéias e interpretações.	**D34** Codificar mensagens utilizando diferentes técnicas de cifras de transposição como a cerca de ferrovia. **D35** Decodificar mensagens utilizando diferentes técnicas de cifras de transposição como a cerca de ferrovia.	
	H46 Elaborar perguntas e hipóteses, selecionando e organizando dados e ideias para resolver problemas.	**D36** Refletir sobre a segurança de códigos criados a partir de cifras de transposição. **D37** Criar mensagens secretas a partir do uso de aplicativos.	
C3	**H8** Analisar, interpretar, formular e resolver situações-problema, compreendendo diferentes significados das operações, envolvendo números naturais, inteiros, racionais e irracionais.	**D38** Conhecer o Princípio Fundamental da Contagem (princípio multiplicativo). **D39** Aplicar o Princípio Fundamental da Contagem na obtenção da quantidade de anagramas de uma palavra.	
C6	**H16** Resolver situações-problema que podem ser traduzidas por equação, inequação ou sistema de equações do segundo grau, discutindo o significado dessas raízes em confronto com a situação proposta.	**D40** Codificar mensagens calculando o valor numérico de uma função a partir de uma associação convencionada entre letras e números. **D41** Decodificar mensagens associadas ao uso de funções do	1.4 Funções Matemáticas e Criptografia

		tipo afim ou quadráticas.	
C7	**H17** Identificar a natureza entre grandezas, expressando a relação existente por meio de uma sentença algébrica e representando-a no plano cartesiano.	**D42** Construir a representação gráfica de funções do tipo afim. **D43** Construir a representação gráfica de funções do tipo quadrática. **D44** Analisar, por meio de *softwares*, funções afim e quadráticas e a construção de suas inversas.	
	H18 Compreender a noção de variável pela interdependência da variação de grandezas.	**D45** Determinar a lei da função inversa conhecida a função original. **D46** Discutir sobre a existência de função inversa considerando o intervalo do domínio.	
C15	**H46** Elaborar perguntas e hipóteses, selecionando e organizando dados e ideias para resolver problemas.	**D47** Refletir sobre a injetividade de uma função. **D48** Discutir sobre a ambiguidade na troca de mensagens que utilizam funções não injetivas.	

APÊNDICE B – PLANO DE EXECUÇÃO DIDÁTICA

	COLÉGIO MILITAR DE PORTO ALEGRE **PLANO DE EXECUÇÃO DIDÁTICA**	

SCMB/DEPA **CMPA**	**ANO LETIVO: 2019**
	Área: Ciências da Natureza, Matemática e suas Tecnologias **Disciplina**: Matemática **Ano Escolar**: 6º ao 9º anos (turno integral)
	Professor: Cap Anderson

Sequência didática Nº 01: Criptografia.

Aulas	Competências	Habilidades	Estratégias de Aprendizagem - Desenvolvimento	Tempo previsto
Aula 1 **Semana 1ª**	**C15**	**H44**	**1.1 Introdução à Criptografia** Aula expositiva dialogada, com suporte de apresentação de *slides*, onde serão apresentados conceitos e definições básicas da Criptografia: cifra, codificação, decodificação, chave, alfabeto cifrado, entre outros. A mesma apresentação de *slides* trará aspectos históricos da importância da Criptografia, ilustrada em fatos e curiosidades, como o Telegrama Zimmermann, a Máquina Enigma, a relação com o código Morse e o uso da Criptografia no contexto atual de tecnologia, segurança e privacidade. O código Morse será explorado com auxílio de aplicativo para *smartphone* e auxílio de lousa digital.	**1 h/a**
		H45		
	C16	**H48**		
		H49		
		H50		

	Avaliação	Questionamentos/exercícios em sala de aula.	

Aulas	**Competências**	**Habilidades**	**Estratégias de Aprendizagem - Desenvolvimento**	**Tempo previsto**
Aulas 2 a 6 **Semanas 1ª, 2ª e 3ª**	**C3**	**H8**	**1.2 Cifras de Substituição** Em um primeiro momento, a teoria será apresentada por meio de aula expositiva. O conceito de cifras de substituição, será complementado com o ensino de de técnicas simples, como a cifra do chiqueiro (*pigpen*), o atbash, a cifra de César e o quadrado de Políbio. A cifra de César será terá destaque especial com a construção de um disco de cifragem, além do conhecimento sobre as vulnerabilidades de cifras de substituição monoalfabética: a análise de frequências, relacionando porcentagem e Estatística. Também será proposta uma ideia sobre a construção de uma tabela ASCII, com conversão de base binária para decimal e vice-versa. O aprendizado e fixação destas técnicas, tanto na codificação quanto na decodificação, se dará com a distribuição de notas de aula com exercícios que valorizem o raciocínio e autonomia do aluno, estimulando o trabalho em grupo e a criação de estratégias para solucionarem situações-problema.	**5 h/a**
	C13	**H38**		
		H39		
	C15	**H44**		
		H45		
		H46		
		H47		
	Avaliação		Questionamentos/exercícios em sala de aula.	

<table>
<tr><th>Aulas</th><th>Competências</th><th>Habilidades</th><th>Estratégias de Aprendizagem - Desenvolvimento</th><th>Tempo previsto</th></tr>
<tr><td rowspan="4">Aulas
7 a 8

Semana
4ª</td><td rowspan="2">C3</td><td>H8</td><td rowspan="3">1.3 Cifras de Transposição
Inicialmente, por meio de aulas expositivas, será trabalhado um novo conceito: o de cifra de transposição. Esta, será ilustrada por meio de técnicas simples como a cerca de ferrovia (rail fence) em um paralelo com a combinatória, particularmente o Princípio Fundamental da Contagem e a quantidade de anagramas de uma palavra.
A utilização dos aplicativos Criptography e Decrypto, complementarão o estudo, pois permitem aos alunos a troca de mensagens secretas, comparando-as com as técnicas de codificação aprendidas “manualmente” nas aulas anteriores. As notas de aula relacionadas estimulam o debate e a discussão.</td><td rowspan="4">2 h/a</td></tr>
<tr><td rowspan="3">C15</td><td>H44</td></tr>
<tr><td>H45</td></tr>
<tr><td>H46</td></tr>
<tr><td colspan="2">Avaliação</td><td>Questionamentos/exercícios em sala de aula.</td></tr>
</table>

<table>
<tr><th>Aulas</th><th>Competências</th><th>Habilidades</th><th>Estratégias de Aprendizagem - Desenvolvimento</th><th>Tempo previsto</th></tr>
<tr><td rowspan="5">Aulas
9 e 10

Semana
5ª</td><td>C6</td><td>H16</td><td rowspan="3">1.4 Funções Matemáticas e Criptografia
Inicialmente, por meio de aula expositiva, será realizado um paralelo entre funções e Criptografia, com o cálculo do valor numérico de uma função, o conceito de função inversa e a representação gráfica no plano cartesiano (primeiramente manual, depois com auxílio do software Geogebra).
Os alunos receberão nota de aula com exercícios que permitirão discussões sobre a existência de funções inversas, refletindo sobre o estudo de funções do tipo afim e do tipo quadrática.</td><td rowspan="4">2 h/a</td></tr>
<tr><td rowspan="2">C7</td><td>H17</td></tr>
<tr><td>H18</td></tr>
<tr><td>C15</td><td>H46</td></tr>
<tr><td colspan="2">Avaliação</td><td>Questionamentos/exercícios em sala de aula.</td></tr>
</table>

Visto do Coordenador de Disciplina

Visto da Supervisão Escolar

APÊNDICE C – NOTA DE AULA 01

AULAS 01 E 02: ASPECTOS HISTÓRICOS DA CRIPTOGRAFIA E PRINCIPAIS CONCEITOS

1. ASPECTOS IMPORTANTES.

a) **Criptografia:** a palavra criptografia vem do grego, *kryptos*, cujo significado é secreto, oculto; e *graphein*, que quer dizer escrita; ou seja, critptografia é um termo para escrita secreta, oculta.
b) A Criptografia sempre se mostrou importante ao longo da História da humanidade tanto em guerras quanto na diplomacia entre países, garantindo a segurança necessária. Destacam-se o uso da **Máquina Enigma** na Segunda Guerra Mundial e do **Telegrama Zimmermann**. Atualmente, a Criptografia continua sendo usada nestes meios, porém, associada com tecnologia no envio de *e-mails*, mensagens de aplicativos e compras *online*.
c) **Cifrar** ou **codificar** uma mensagem é utilizar um método para ocultar um texto conhecido apenas pelo emissor e receptor.
d) Muitos métodos criptográficos usam uma **chave**. Para garantir a segurança da codificação, esta chave deve ser secreta para todos quem não devem ter acesso a uma informação sigilosa. Geralmente, estes métodos usam esta mesma chave para **decifrar** ou **decodificar** a mensagem, muitas vezes usando o processo reverso de cifrar ou codificar.
e) O **código Morse** não é um método criptográfico, mas sim um alfabeto alternativo. No entanto, as mensagens costumavam ser criptografadas antes de serem transmitidas.

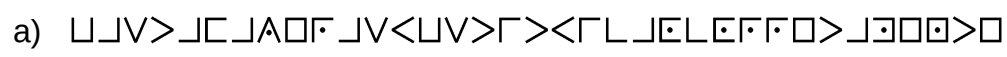
2. CIFRAS DE SUBSTITUIÇÃO

A cifra de substituição consiste em trocar uma letra ou conjunto de letras por outras letras, símbolos ou números, criando um alfabeto cifrado em relação ao alfabeto original. Neste tipo de criptografia, a chave geralmente é o próprio alfabeto cifrado. Quando um símbolo do alfabeto cifrado corresponde a uma única letra do alfabeto original, dizemos ter uma **cifra de substituição monoalfabética**.

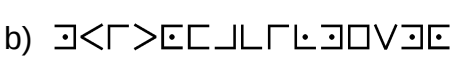
Exemplo 1. Existem diversas formas de criptografia de substituição, e uma das mais famosas é a cifra do chiqueiro (em inglês, chamada *pigpen*), popularmente divulgada como sendo usada entre maçons. Ela usa símbolos no lugar de letras. A seguir, a chave e um exemplo. Espaços e acentuação são suprimidos na mensagem codificada.

C	A	S	A	R	A	O	D	A	V	A	R	Z	E	A
C	A	S	A	R	A	O	D	A	V	A	R	Z	E	A

Exercício 1. Utilizando a cifra do chiqueiro (*pigpen*) decifre as mensagens abaixo:

a) 

Resposta: BASTAFAZERASUBSTITUICAOCORRETAMENTE (Basta fazer a substituição corretamente).

b) 

Resposta: MUITOFACILMESMO (Muito fácil mesmo).

c) 

Resposta: GOSTOUDERESOLVER? (Gostou de resolver?)

Exercício 2. Codifique as mensagens abaixo utilizando a cifra do chiqueiro (*pigpen*).

a) ZUM ZARAVALHO.

Resposta: 

b) MÁQUINA ENIGMA.

Resposta: 

c) CRIPTOGRAFIA É LEGAL.

Resposta: 

Exemplo 2. Na Idade Média, religiosos estudiosos da Bíblia ficavam intrigados com o fato de que o Velho Testamento incluía trechos criptografados, codificados com o que ficou conhecido como *atbash*, uma forma tradicional de substituição hebraica. Neste sistema, a primeira letra do alfabeto hebreu (*aleph*) é substituída pela última (*taw*), a segunda letra (*beth*) é trocada pela penúltima (*shin*). Destas quatro letras deriva o nome da cifra: **A**leph, **T**aw, **B**eth, **Sh**in.

Aplicando a mesma ideia ao nosso alfabeto, teríamos:

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

Observe que a palavra MILITAR seria cifrada como NRORGZI, por exemplo.

Exercício 3. Usando a técnica ATBASH:

a) Codifique a mensagem COLÉGIO DOS PRESIDENTES.

Resposta: XLOVTRLWLHKIVHRWVMGVH.

b) Decodifique a mensagem VCGIVNZNVMGVUZXRO.

Resposta: EXTREMAMENTEFACIL (extremamente fácil).

Exercício 4. Nesta aula, você pôde ouvir a transmissão de mensagens em código Morse. Dominar seu entendimento pleno apenas reconhecendo os sinais sonoros exige certo estudo. No entanto, escrever uma mensagem é relativamente simples. Utilize a tabela de correspondência abaixo para codificar seu nome. Também escreva a mensagem SOS - do inglês, *save our souls*, ou salve nossas almas em tradução livre, um padrão em pedidos de resgate ou socorro.

A ·−	J ·−−−	S ···	2 ··−−−
B −···	K −·−	T −	3 ···−−
C −·−·	L ·−··	U ··−	4 ····−
D −··	M −−	V ···−	5 ·····
E ·	N −·	W ·−−	6 −····
F ··−·	O −−−	X −··−	7 −−···
G −−·	P ·−−·	Y −·−−	8 −−−··
H ····	Q −−·−	Z −−··	9 −−−−·
I ··	R ·−·	1 ·−−−−	0 −−−−−

Resposta pessoal para o nome. SOS fica codificado como: ···−−−···

Exercício 5. Tiago criou seu próprio alfabeto cifrado para trocar mensagens secretas com seu irmão, Josias. Ele associou um número a cada letra do alfabeto como na tabela abaixo:

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

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	14	15	16	17	18	19	20	21	22	23	24	25	26

Tiago, passou a seguinte mensagem para Josias: 521191521151351281518. Mesmo com o alfabeto cifrado, Josias teve dificuldade em decifrar a mensagem. Ele sabia que 52 não poderia representar uma letra, mas sobre o número 21, ele não tinha como ter certeza se 21 era “U” ou era 2 e 1, ou seja, “BA”.

a) Depois disso, Tiago lembrou que esqueceu de colocar “tracinhos” na mensagem, que deveria ser: 5 – 21 – 19 – 15 – 21 – 15 – 13 – 5 – 12 – 8 -15 – 18. Ajude Josias a decifrar.

Resposta: EUSOUOMELHOR. (Eu sou o melhor).

b) Reflita sobre a possiblidade de continuar utilizando números como alfabeto cifrado, mas que não precise dos “tracinhos” na mensagem secreta (de fato, eles tornam este método menos seguro).

Resposta: este exercício talvez precise de uma intervenção maior do professor. Alguns métodos criptográficos utilizando a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35
-												
36												

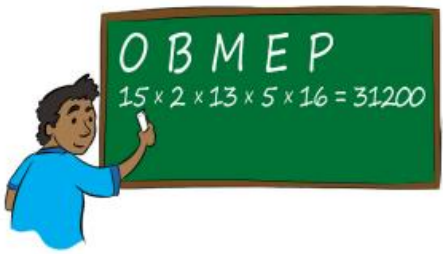
Com ela, emissor e receptor devem combinar que todos os caracteres são formados por dois algarismos. Inclusive, os espaços podem ser codificados como “36”.

Exercício 6. Crie um alfabeto cifrado utilizando simbologia própria para cada letra do alfabeto original. Troque mensagens com seus colegas utilizando o alfabeto cifrado que você criou. Resposta pessoal.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto cifrado													

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado													

Exercício 7 (OBMEP 2013 2ª fase) Cirilo associa a cada palavra um número, da seguinte maneira: ele troca cada letra por um número, usando a tabela abaixo e, em seguida, multiplica esses números.



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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Por exemplo, o número associado à palavra MAR é 13 x 1 x 18 = 234.

a) Qual é o número associado à palavra CABIDE?

Resposta: o número será 3 x1 x 2 x 9 x 4 x 5 = 1080.

b) Escreva uma palavra com quatro letras cujo número associado seja 455.

Resposta: como a decomposição em fatores primos de 455 é 5 x 7 x 13 e, temos 5 associado à letra E, 7 associado com G e 13 associado com M, uma palavra de quatro letras poderia ser GEMA, onde acrescentamos a letra A associado ao número 1.

c) Explique por que não existe uma palavra cujo número associado seja 2013.

Resposta: pois a decomposição em fatores primos de 2013 é 3 x 11 x 67. Como a tabela de Cirilo apresenta apenas números de 1 a 26 e 67 é primo (não pode ser “quebrado” em números inteiros menores), não teremos uma letra associada ao número 67.

APÊNDICE D – NOTA DE AULA 02

AULAS 03 E 04: CIFRA DE CÉSAR

1. REVISANDO...

Na aula anterior, vimos aspectos históricos e conceitos importantes sobre Criptografia. Também estudamos alguns métodos simples, classificados como **cifras de substituição monoalfabética**. Na aula de hoje, vamos estudar um método particular da substituição monoalfabética: a cifra de César.

2. CIFRA DE CÉSAR

Conta-se que o imperador romano Júlio César utilizava uma técnica de cifra por substituição que mais tarde ficou conhecida por seu nome: Cifra de César. Com ela, mensagens ao campo de batalha eram repassadas, distraindo o inimigo. A ideia é usar um alfabeto cifrado, deslocado um determinado número de casas em relação ao alfabeto original. Abaixo, um alfabeto deslocado três casas.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Utilizando o alfabeto cifrado da tabela acima, uma frase como "CASARÃO DA VÁRZEA" ficaria FDVDUDRGDYDUCHD, onde foram suprimidos espaços e a pontuação.

Ainda que esta cifragem seja muito simples, foi muito eficiente na época de Júlio César. Tanto que foi adotada muitos anos depois, na Guerra Civil americana. Eles utilizavam discos concêntricos, contendo todas as letras do alfabeto como na figura abaixo.

Aqui, entra outro conceito importante na

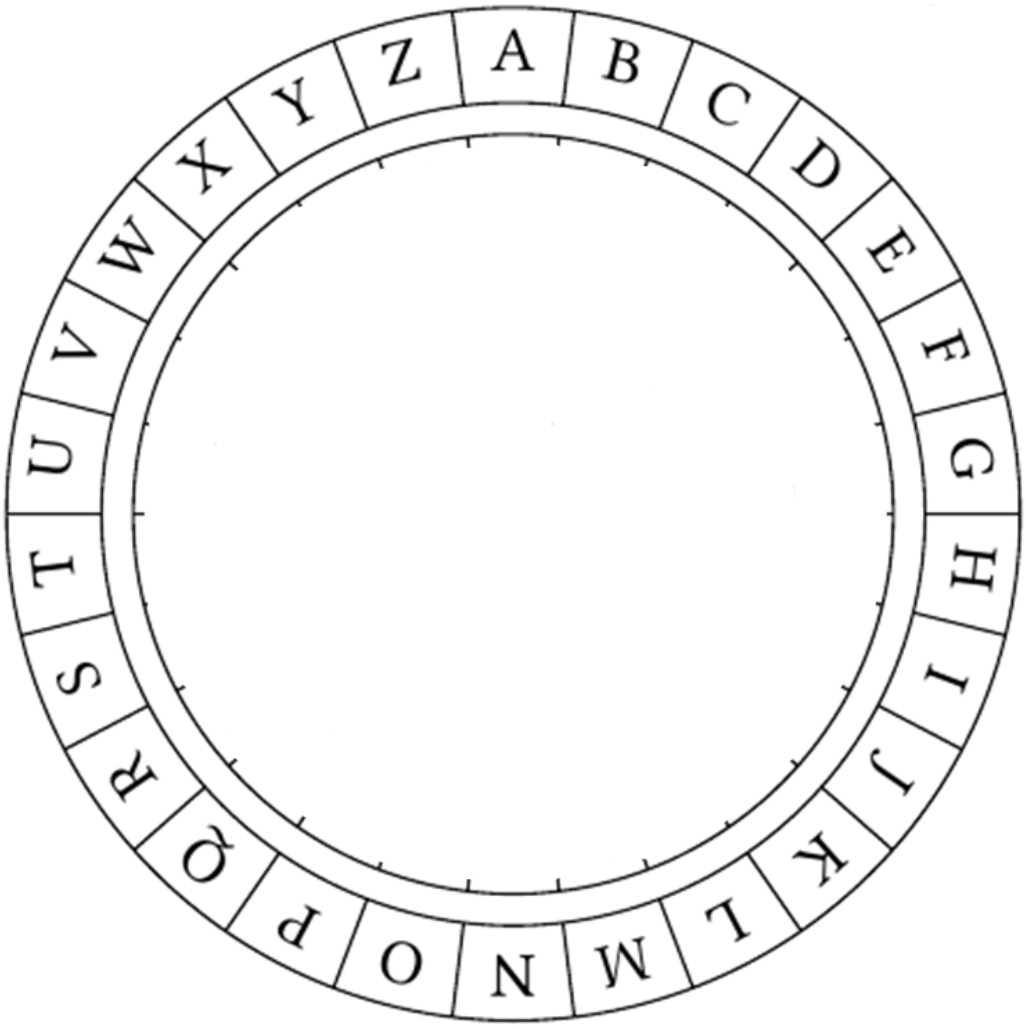
Criptografia: o criptoanalista. A criptoanálise é o estudo realizado para decifrar uma mensagem codificada, mesmo sem conhecimento da chave secreta. Geralmente ocorria quando a mensagem codificada era interceptada pelo inimigo que tentava “quebrar” o código utilizado.

Se você fosse o criptoanalista, como decifraria FDVDUDRGDYDUCHD sem saber qual alfabeto cifrado foi utilizado? De fato, nada aqui indica que foi utilizada cifra de César. Nem sempre é fácil, mas iremos discutir dicas de como a criptoanálise pode ser feita.

Primeiramente, vamos praticar! O Exercício 1 propõe a construção de um disco de cifragem que nos ajudará muito tanto na codificação quanto na decodificação.

Exercício 1. Construção de um disco de cifragem.

1º passo: recorte os círculos abaixo.



2º passo: faça um pequeno furo central nos dois círculos. Junte-os por meio do "colchete" distribuído pelo professor.

Resposta: Esta atividade propõe algumas habilidades dos alunos, sendo aproveitada inclusive como forma de encontrar o centro de um círculo. A ideia é que o círculo maior possa girar livremente para fazer a correspondência entre os alfababetos cifrado e original. Por convenção, pode-se adotar que o alfabeto original é o interno (do círculo menor) e que o alfabeto cifrado é do externo (do círculo menor).
O "colchete" é um material comum "de escritório". Outras construções podem ser feitas utilizando capas de CD. A escolha deste exercício decorre do fato de sua simplicidade.

Exercício 2. Utilizando o disco de cifragem construído no Exercício 1, codifique as mensagens abaixo.

a) O ATAQUE SERÁ ÀS SEIS HORAS, utilizando um alfabeto deslocado 5 posições.

Resposta: em um alfabeto deslocado 5 posições, a letra A do alfabeto original será codificada como F; a letra B como G e, assim por diante. Então,

OATAQUESERAASSEISHORAS será codificada como TFYFVZJXJWFFXXJNXMTWFX.

b) PREPARE A TROPA, utilizando um alfabeto deslocado 10 posições.

Resposta: em um alfabeto deslocado 10 posições, a letra A do alfabeto original será codificada como K; a letra B como L e, assim por diante. Então, PREPAREATROPA, será codificada como ZBOZKBOKDBYZK.

c) Codifique a mensagem RASA usando um alfabeto deslocado em 14 posições.

Resposta: em um alfabeto deslocado 14 posições, a letra A do alfabeto original será codificada como O; a letra B como P e, assim, por diante. Então, RASA será codificada como FOGO.

Exercício 3. Vamos decodificar a mensagem IHZAHHWSPJHYHUHSPZLKLMYLXBLUJPH utilizando a Cifra de César. O nosso alfabeto possui 26 letras. Considerando que o alfabeto cifrado será diferente do original teríamos 25 possibilidades para testar! Talvez isto não seja difícil para um computador, por exemplo, mas certamente era um ponto de dificuldade para quem tentasse “quebrar” um código manualmente. No entanto, a vulnerabilidade da Cifra de César está na “Análise de Frequências” de cada letra.

Em cada idioma, as letras do alfabeto utilizado podem aparecer com maior ou menor frequência. Na Língua Portuguesa, esta frequência, em porcentagem, é mostrada na tabela abaixo:

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Observe que a letra que possui maior frequência é o “A”, seguido do “E” e do “O”. De fato, é difícil escrever uma mensagem muito longa sem o uso destas vogais.

Ou seja, quando temos contato com um texto cifrado, o símbolo que aparecer com maior frequência provavelmente será a letra A, o E ou o O. Além disso, em nosso idioma é comum o uso de dígrafos (NH, LH, SS, RR, por exemplo) que funcionam como "dicas" aos criptoanalistas.

Agora, volte a mensagem IHZAHHWSPJHYHUHSPZLKLMYLXBLUJPH e tente decodificá-la utilizando o disco de cifragem construído no Exercício 1.

Resposta: na mensagem IHZAHHWSPJHYHUHSPZLKLMYLXBLUJPH, a letra H apresenta maior frequência. Provavelmente, a letra H do alfabeto deve corresponder à letra A do alfabeto original, fato que fica confirmado pelo disco de cifragem ou pela construção da tabela abaixo:

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

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Por fim, temos BASTAAPLICARANALISEDEFREQUENCIA (basta aplicar análise de frequência).

Exercício 4. Como uma tabela de frequências das letras de um idioma é construída? Neste exercício teremos uma noção, visto que isto é relativamente simples. Porém, a tabela com a frequência em porcentagem do exercício anterior foi construída a partir de um estudo de amplos textos, considerando diversos assuntos, autores e áreas do conhecimento. Para melhor visualização, um gráfico estatístico (de barras ou de colunas) é construído.
Seria bem complexo (e, principalmente trabalhoso) realizar uma análise completa de todas as letras do alfabeto considerando nosso idioma. Mas podemos ter uma ideia analisando a frase abaixo.

EDUCAÇÃO É A CHAVE

Agora, responda as perguntas abaixo:

a) Quantas letras (mesmo repetidas) formam esta mensagem?

Resposta: Foram utilizadas 15 letras.

b) Quais são as letras que aparecem?

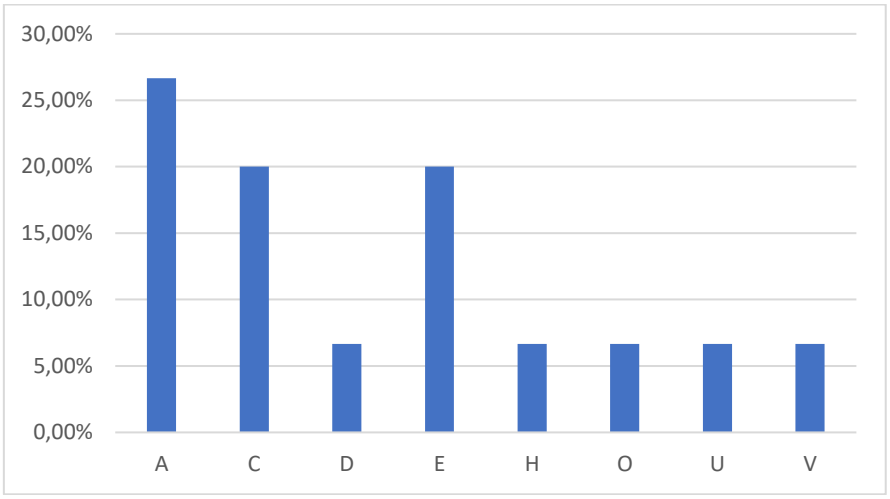
Resposta: Foram utilizadas 4 vezes a letra A, 3 vezes a letra C, 1 vez a letra D, 3 vezes a letra E, 1 vez a letra H, 1 vez a letra O, 1 vez a letra U e 1 vez a letra V.

c) Determine a porcentagem da frequência de cada letra.

Resposta: Para a letra A, temos: $\frac{4}{15} \cdot 100 = 26{,}67\%$. Para a letra C, temos: $\frac{3}{15} \cdot 100 = 20\%$. Para a letra D, temos: $\frac{1}{15} \cdot 100 = 6{,}67\%$. Para a letra E, temos: $\frac{3}{15} \cdot 100 = 20\%$. Para a letra H, temos: $\frac{1}{15} \cdot 100 = 6{,}67\%$. Para a letra O, temos: $\frac{1}{15} \cdot 100 = 6{,}67\%$. Para a letra U, temos: $\frac{1}{15} \cdot 100 = 6{,}67\%$ e para a letra H, temos: $\frac{1}{15} \cdot 100 = 6{,}67\%$.

d) Construa um gráfico de colunas correspondente.

Resposta:



e) Compare a porcentagem obtida para a construção do gráfico acima com a tabela do Exercício 3. Na sua opinião, o que influencia a diferença nos resultados?

Resposta: Talvez o professor possa intervir, mas é esperado que o aluno conclua que na construção do gráfico, houve apenas o estudo da frequência das letras A, C, D, E, H, O, U e V em uma mensagem curta, ao contrário da tabela do Exercício 3, baseada em distintos textos com milhares de caracteres.

APÊNDICE E – NOTA DE AULA 03

AULAS 05 E 06: CIFRA DE POLÍBIO E CÓDIGOS BINÁRIOS

1. CIFRA DE POLÍBIO

Continuando a aula anterior, veremos mais um exemplo de cifra de substituição: a cifra de Políbio. Ela utiliza uma tabela de letras, combinada entre emissor e receptor, que substitui cada letra da mensagem por um par de números. A origem desta técnica de cifrar é do século II a. C e seu funcionamento foi relatado pelo historiador grego Políbio.

A ideia é muito simples. Utilizando o quadrado abaixo, substituímos a letra observando, respectivamente, a linha e a coluna a que pertence esta letra.

	Coluna 1	Coluna 2	Coluna 3	Coluna 4	Coluna 5
Linha 1	A	B	C	D	E
Linha 2	F	G	H	I/J	K
Linha 3	L	M	N	O	P
Linha 4	Q	R	S	T	U
Linha 5	V	W	X	Y	Z

Assim, a letra C será codificada como 13; M será codificada como 32; P como 35 e A como 11. A mensagem CMPA será codificada como 13323511. Para decodificar, basta separar a mensagem codificada a cada dois algarismos e, com a mesma tabela acima, fazer o processo inverso.

Como nosso alfabeto possui 26 letras para uma tabela de 25 espaços (5 por 5), colocamos as letras I e J em um mesmo espaço. Na decodificação terá de ser levado em conta qual letra (I ou J) faz sentido na mensagem já que ambas serão codificadas da mesma maneira (24).

Exercício 1. Codifique as mensagens abaixo usando a Cifra de Políbio.

a) CRIPTOANÁLISE.
Resposta: 13422435443411331131244315
b) ORDEM E PROGRESSO.
Resposta: 34421415321535423422421543433 4

Exercício 2. Decodifique as mensagens abaixo usando a Cifra de Políbio.
a) 5111323443211155154214343215452415244434.
Resposta: VAMOSFAZERDOMEUJEITO (Vamos fazer do meu jeito).

b) 414515242424332334.
Resposta: QUEIJINHO (o aluno terá de perceber que o uso das letras I e J na mesma palavra deve ser levado em consideração).

Exercício 3. A tabela utilizada nos Exercícios 1 e 2 pode ser alterada, embora o princípio de substituição das letras do alfabeto permaneça o mesmo. Isto aumenta a segurança, desde que a tabela seja de conhecimento apenas do emissor e do receptor da mensagem. Márcio e Manuela, por exemplo, utilizam a tabela abaixo:

	Coluna !	Coluna ?	Coluna +	Coluna &	Coluna =
Linha @	A	B	C	D	E
Linha #	F	G	H	I/J	K
Linha $	L	M	N	O	P
Linha %	Q	R	S	T	U
Linha *	V	W	X	Y	Z

a) Como Manuela codifica seu próprio nome utilizando esta tabela?

Resposta: $?@!$+%=@=$!@!

b) Decodifique a mensagem #!#&$!#+@!, utilizando a tabela combinada entre Márcio e Manuela.
Resposta: FILHA.

c) Junte-se com um colega e crie sua própria tabela de cifragem, utilizando símbolos próprios para as linhas e colunas, semelhante ao que fizeram Márcio e Manuela. Use a tabela criada por vocês na troca de mensagens secretas.
Resposta pessoal.

2 – CÓDIGOS BINÁRIOS

Normalmente, trabalhamos com os números em uma representação decimal, onde cada algarismo tem um "peso" segundo uma potência de base 10. Neste sistema, são utilizamos dez símbolos - os algarismos 0,1,2,3,4,5,6,7,8 e 9 - onde é levada em consideração a posição que cada algarismo ocupa. Veja, os exemplos abaixo:

a) O número 153 pode ser escrito como $\mathbf{1} \cdot 10^2 + \mathbf{5} \cdot 10^1 + \mathbf{3} \cdot 10^0$. Disto, temos que o 1 é o algarismo das centenas, o 5 é o das dezenas e o 3 é o das unidades.

b) O número 1202 pode ser escrito como $\mathbf{1} \cdot 10^3 + \mathbf{2} \cdot 10^2 + \mathbf{0} \cdot 10^1 + \mathbf{2} \cdot 10^0$. Disto, temos que o 1 é o algarismo das unidades de milhar, o 2 é o algarismo das centenas, o 0 é o algarismo das dezenas e o 2 é o algarismo das unidades.

A ideia de um sistema de numeração binária é a mesma de um sistema de numeração decimal. Porém, no lugar de usar os dez algarismos de 0 a 9, serão utilizados apenas o 0 e o 1. Além disso, as potências de base 10 são substituídas por potências de base 2.

Assim, o número 101, por exemplo, quando representado em um sistema de numeração binária, é equivalente ao número 5 em um sistema de numeração decimal, pois:

$$\mathbf{1} \cdot 2^2 + \mathbf{0} \cdot 2^1 + \mathbf{1} \cdot 2^0 = 4 + 0 + 1 = 5$$

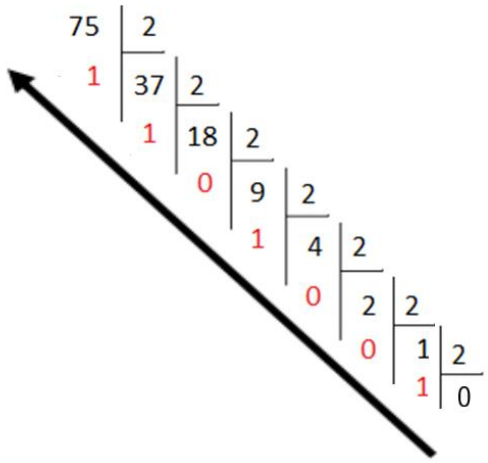
Para não existir confusão entre base binária e decimal, escrevemos $(101)_2 = 5$, onde fica dispensada a indicação da base decimal, por esta ser mais usual.

Perceba, então, que é relativamente simples converter um número representado na base binária para sua representação decimal, como mostram os exemplos abaixo:

a) $(11010)_2 = \mathbf{1} \cdot 2^4 + \mathbf{1} \cdot 2^3 + \mathbf{0} \cdot 2^2 + \mathbf{1} \cdot 2^1 + \mathbf{0} \cdot 2^0 = 16 + 8 + 0 + 2 + 0 = 26.$

b) $(10001001)_2 = \mathbf{1} \cdot 2^7 + \mathbf{0} \cdot 2^6 + \mathbf{0} \cdot 2^5 + \mathbf{0} \cdot 2^4 + \mathbf{1} \cdot 2^3 + \mathbf{0} \cdot 2^2 + \mathbf{0} \cdot 2^1 + \mathbf{1} \cdot 2^0 = 128 + 0 + 0 + 0 + 8 + 0 + 0 + 1 = 137.$

E se quiséssemos converter um número da base decimal para a base binária? Uma das ideias é a divisão euclidiana sucessiva pelo número 2, onde os restos possíveis são 0 e 1. Este processo é realizado até que o dividendo seja menor que 2. Como exemplo, vamos converter o número 75 para a base binária como mostrado abaixo. Os restos, “zeros” e “uns” lidos da direita para esquerda, como indica a seta, são a representação binária do número 75.



Assim, $75 = [1001011]_2$. De fato, $1.2^6 + 0.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 1.2^1 + 1.2^0 = 64 + 8 + 2 + 1 = 75.$

A base binária é importante na utilização de linguagens de programação associada a computadores e *smartphones*, por exemplo. Com isto, é possível, por exemplo, que as letras de nosso alfabeto sejam convertidas em números binários. Para isto, podem ser adotados convenções padronizadas como a Tabela ASCII - do inglês, *American Standard Code for Information Interchange*, ou Código Americano Padrão para Troca de Informações, em tradução livre. Para as letras maiúsculas de A até Z, ela associa os números inteiros de 65 a 90 em sua representação decimal e assim, os correspondentes destes números na base binária. Na tabela ASCII todo número de representação binária apresenta oito dígitos. Parte desta tabela está representada abaixo:

LETRA	DECIMAL	BINÁRIO	LETRA	DECIMAL	BINÁRIO
A	65		N	78	01001110
B	66	01000010	O	79	01001111
C	67		P	80	
D	68	01000100	Q	81	01010001
E	69	01000101	R	82	01010010
F	70	01000110	S	83	01010011
G	71	01000111	T	84	01010100
H	72	01001000	U	85	01010101
I	73	01001001	V	86	01010110
J	74	01001010	W	87	01010111
K	75	01001011	X	88	01011000
L	76	01001100	Y	89	01011001
M	77		Z	90	01011010

Propositalmente, as letras C, M, P e A não apresentam sua representação em binário na tabela acima, pois isto fará parte do nosso exercício. A Tabela ASCII é bem mais completa, com 128 caracteres (outros símbolos além das letras do alfabeto também apresentam representação, inclusive diferenciação das letras minúsculas) além de representação utilizando outras bases como a hexadecimal.

No entanto, é válido nosso exercício para entender como esta tabela é construída. Por uma convenção, a letra B é associado ao número 66 na base decimal. Como $66 = [1000010]_2$, é necessário acrescentar um zero à esquerda para completar o padrão de oito dígitos, ou seja, escrever 01000010.

Exercício 4. Codifique a palavra CMPA utilizando a convenção da tabela ASCII e a representação na base binária.

Resposta: A letra C corresponde ao número 67. Convertendo 67 de decimal para binário, temos $66 = [1000011]_2$. Assim, na tabela ASCII, temos 01000011; da mesa maneira, M que corresponde ao número 77, resulta de $77 = [1001101]_2$ em 01001101; P corresponde a $80 = [1010000]_2$ e assim, temos 01010000; por fim, A que corresponde a $65 = [1000001]_2$, será escrito como 01000001. A mensagem CMPA será codificada como 01000011010011010101000001000001.

Exercício 5. Decodifique a mensagem 010100110100010101010010.

Resposta: Separando a mensagem em grupos de oito dígitos, temos 01010011 – 01000101 – 01010010. Podemos consultar a tabela, ou verificar que: $[01010011]_2 = 83$, $[01000101]_2 = 69$ e $[01010010]_2 = 82$. A mensagem original seria SER.

Exercício 6. De maneira semelhante, você pode representar números em outras bases numéricas, diferentes da base decimal comumente utilizada em sala de aula. A base octal, por exemplo, utiliza oito símbolos, os algarismos 0,1,2,3,4,5,6 e 7. Qual seria a representação na base decimal do número $[607]_8$?

Resposta: Teríamos $[607]_8 = 6 \cdot 8^2 + 0 \cdot 8^1 + 7 \cdot 8^0 = 384 + 0 + 7 = 391$.

APÊNDICE F – NOTA DE AULA 04

AULAS 07 E 08: CIFRAS DE TRANSPOSIÇÃO

1. REVISANDO...

Nas duas primeiras aulas aprendemos técnicas de codificação conhecidas como cifras de substituição. Na aula de hoje, conheceremos as cifras de transposição.

2. CIFRAS DE TRANSPOSIÇÃO

As cifras de transposição consistem em “embaralhar” as letras de uma mensagem, criando anagramas. Anagramas são permutações das letras de uma palavra, formando novas palavras com ou sem sentido. A palavra COR, por exemplo, possui 6 anagramas: COR, CRO, OCR, ORC, ROC e RCO. Uma palavra com letras repetidas, como ABA, por exemplo, possui 3 anagramas: ABA, AAB e BAA.

Obviamente, para codificar um texto inteiro com técnicas de transposição poderia gerar muitas possibilidades. É preciso que o emissor e receptor combinem uma maneira de “embaralhar” estas letras que somente eles conheçam, como nos exemplos abaixo.

Exemplo 1. Suponha que se queira cifrar a mensagem "CRIPTOGRAFIA NO COLÉGIO MILITAR” Se emissor e receptor escolherem CMPA como palavra-chave, o resultado será a criação do quadro abaixo:

ORDEM	**2**	**3**	**4**	**1**
CHAVE	**C**	**M**	**P**	**A**
MENSAGEM ORIGINAL	C	R	I	P
	T	O	G	R
	A	F	I	A
	N	O	C	O
	L	E	G	I
	O	M	I	L
	I	T	A	R

Nesse quadro, o número 2341 é a ordem alfabética que as letras ocorrem dentro da palavra CMPA: A é a primeira letra; C é a segunda, M é a terceira e P a quarta. A mensagem é escrita linha após linha. A cifra é obtida lendo as colunas na ordem numérica. Assim, suprimindo espaços e acento, CRIPTOGRAFIANOCOLEGIOMILITAR resulta em PRAOILRCTANLOIROFOEMTIGICGIA. Para a decodificação, o receptor divide a quantidade de letras da mensagem codificada (no caso 28) por 4 (número de letras da palavra-chave CMPA) e organiza o resultado até também obter a mensagem original.

Exercício 1. Codifique a mensagem TURNO INTEGRAL PARA O COLÉGIO, usando a palavra BANCO como chave e seguindo a mesma técnica explicada no Exemplo 1.

Resposta:

ORDEM	2	1	4	3	5
CHAVE	B	A	N	C	O
MENSAGEM ORIGINAL	T	U	R	N	O
	I	N	T	E	G
	R	A	L	P	A
	R	A	O	C	O
	L	E	G	I	O

Então, TURNOINTEGRALPARAOCOLEGIO fica codificado como UNAAETIRRLNEPCIRTLOGOGAOO.

É interessante que o professor comente que a palavra-chave deve ter um número inteiro de letras que divida a quantidade de letras da mensagem com resto zero em uma divisão euclidiana. Em certas condições, pode-se acrescentar letras que não mudem o sentido da mensagem original, mas que completem a quantidade de letras da mensagem para facilitar a montagem do quadro de codificação.

Exercício 2. Decodifique a mensagem DECRUVEFVODRDOMIICEA, sabendo que a palavra-chave usada foi SORTE, e que a técnica utilizada foi a mesma do Exemplo 1.

Resposta: a palavra SORTE possui cinco letras. Então, dividimos a mensagem DECRUVEFVODRDOMIICEA, de vinte letras por cinco, obtendo palavras com quatro letras cada (pois 20/5=4): DECR – UVEF – VODR – DOMI - ICEA e montamos o Quadro abaixo:

ORDEM	4	2	3	5	1
CHAVE	S	O	R	T	E
MENSAGEM ORIGINAL	D	U	V	I	D
	O	V	O	C	E
	M	E	D	E	C
	I	F	R	A	R

Temos: DUVIDOVOCEMEDECIFRAR (Duvido você me decifrar).

O Exemplo 2, abaixo, traz outro método de cifra de transposição, conhecido como “cerca de ferrovia” (em inglès, é conhecida como *rail fence*).

Exemplo 2. Vamos codificar a mensagem "ENCONTRE-ME ÀS 14H". A ideia consiste de escrever a mensagem alternando as letras em duas linhas diferentes (variações desta técnica podem usar três ou mais linhas). Temos então:

Linha 1	E		C		N		R		M		A		1		H
Linha 2		N		O		T		E		E		S		4	

O texto cifrado fica: ECNRMA1HNOTEES4, onde também foram suprimidos espaços e acento. Para decodificar, é necessário que o receptor saiba em quantas linhas foram codificadas a mensagem. No caso de duas, ele divide a mensagem criptografada em dois grupos e separa em linhas da mesma maneira que na codificação, retornando à mensagem original. Se a mensagem for formada por um número ímpar de letras, o primeiro grupo terá uma letra a mais.

Exercício 3. Codifique a mensagem A RESPOSTA É QUINZE, usando a técnica cerca de ferrovia com duas linhas.

Resposta:

Linha 1	A		E		P		S		A		Q		I		Z	
Linha 2		R		S		O		T		E		U		N		E

O texto cifrado será: AEPSAQIZRSOTEUNE.

Exercício 4. Decodifique a mensagem CFAERNPSCOIRDTASOIA sabendo que foi usada a técnica cerca de ferrovia com duas linhas.

Resposta: Basta dividir a mensagem CFAERNPSCOIRDTASOIA em duas partes: CFAERNPSCO e IRDTASOIA. Como a mensagem possui um número ímpar de letras (dezenove), o primeiro grupo fica com uma letra a mais para compensar). Por fim, basta montar o quadro abaixo:

Linha 1	C		F		A		E		R		N		P		S		C		O
Linha 2		I		R		D		T		A		S		O		I		A	

A mensagem original é CIFRADETRANSPOSICAO (cifra de transposição).

Exemplo 3. Quantos anagramas são possíveis para a palavra ROMA? Escrevendo alguns deles, percebemos que poderíamos ter AMRO, AMOR, MORA, ORAM... Mas quantos? Temos quatro letras distintas. Para formarmos anagramas, temos quatro maneiras de escolher a primeira letra; na escolha da segunda letra, temos três maneiras; na escolha da terceira letra teremos duas possibilidades, enquanto que sobrará apenas uma forma de escolher a última letra. No total, temos: $4 \cdot 3 \cdot 2 \cdot 1 = 24$ anagramas possíveis da palavra ROMA. Com raciocínio semelhante, verifique que a palavra LETRA possui $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ anagramas, enquanto que a palavra ESCOLA possui $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$. Para economizar escrita, podemos usar simplesmente a notação "!". Lê-se este símbolo como "fatorial". Assim: $4! = 4 \cdot 3 \cdot 2 \cdot 1$, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ e $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$, por exemplo.

No entanto, este raciocínio não funciona se a palavra possui letras repetidas. A palavra OVO, por exemplo, com duas letras “O”. São 3 letras, então serão $3! = 3 \cdot 2 \cdot 1 = 6$ anagramas, certo? Errado. Verifique que os anagramas possíveis são OVO, VOO e OOV. De maneira geral, quando temos letras repetidas, uma palavra com n letras, com quantidades α, β, γ ... de letras repetidas, terá número de anagramas calculado por:

$$P^{\alpha,\beta,\gamma\ldots} = \frac{n!}{\alpha!\,\beta!\,\gamma!\ldots}$$

A palavra GARRAFA, por exemplo, com 7 letras, sendo 3 “A” e 2 “R”, terá 420 anagramas, pois:

$$P^{3,2} = \frac{7!}{3!\,2!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 420$$

Exercício 5. Determine o número de anagramas das palavras:

a) ALIMENTO.

Resposta: 8! = 40320 anagramas.

b) CARRO.

Resposta: $\frac{5!}{2!} = 60$ anagramas.

c) FAZER.

Resposta: 5! = 120 anagramas.

d) MATEMÁTICA (não considere a letra A acentuada como uma “letra diferente”).

Resposta: $\frac{10!}{2!3!2!} = 151200$ anagramas.

e) ARGENTINO. (verifique que IGNORANTE é um anagrama possível).

Resposta: $\frac{9!}{2!} = 181440$ anagramas.

f) ANAGRAMA.

Resposta: $\frac{8!}{4!} = 1680$ anagramas.

Exercício 6. Com a palavra MARTELO:

a) Quantos anagramas podemos formar?

Resposta: 5040 anagramas.

b) Quantos anagramas começam por M?

Resposta: 720 anagramas.

c) Quantos anagramas começam por M e terminam por O?

Resposta: 120 anagramas.

d) Quantos anagramas apresentam as letras M, A e R juntas e nessa ordem?

Resposta: 720 anagramas.

e) Quantos anagramas apresentam as letras M, A e R juntas?

Resposta: 4320 anagramas.

Exercício 6. Como sugestão, você pode utilizar os aplicativos para *smartphone* ***Decrypto*** e ***Cryptography***. Ambos são bem intuitivos e permitem codificar e decodificar mensagens por meio de diversas técnicas, inclusive as vistas nas aulas anteriores (cifra do chiqueiro ou *pigpen*, atbash, cifra de César, binária, ASCII e hexadecimal), além da cifra cerca de ferrovia (*rail fence*) trabalhada na aula de hoje.

Sendo assim, escolha uma das técnicas para cifrar e codifique uma mensagem curta. Desafie seus colegas a decifrarem seu código!

Resposta pessoal. No entanto, o uso destes aplicativos é bastante oportuno, fazendo um paralelo com tudo que foi visto anteriormente, além de disponibilizar a análise de frequência e permitir que os alunos compartilhem mensagens criptografadas entre si.

Estes aplicativos são, inclusive, de grande auxílio para o professor na criação das aulas, verificando e corrigindo os códigos.

APÊNDICE G – NOTA DE AULA 05

AULAS 09 E 10: FUNÇÕES MATEMÁTICAS E CRIPTOGRAFIA

1. CONTEXTUALIZANDO

Nesta aula, estudaremos funções associadas a mensagens criptografadas. A ideia básica é a de que emissor e receptor combinem um alfabeto associado a uma sequência de números como na Tabela 1 abaixo:

Tabela 1 – Associando números a letras.

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

Alfabeto original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	14	15	16	17	18	19	20	21	22	23	24	25	26

Depois disso, devem escolher a lei de uma função que será a **chave de codificação**. Vamos escolher, por exemplo, a função $f(x) = 4x + 5$. Com esta escolha, a palavra CMPA fica codificada como 17 ; 57 ; 69 ; 9, pois:

C=3 e $f(3) = 4 \cdot 3 + 5 = 17$;
M=13 e $f(1) = 4 \cdot 13 + 5 = 57$;
P=16 e $f(16) = 4 \cdot 16 + 5 = 69$;
A=1 e $f(1) = 4 \cdot 1 + 5 = 9$.

Agora, com a mensagem codificada, 17 ; 57 ; 69 ; 9, como o receptor voltará à mensagem original CMPA?

Bom, como ele conhece a correspondência entre números e letras da Tabela 1 acima, combinada com o receptor, ele pode determinar a inversa da função de lei $f(x) = 4x + 5$. Relembrando que ele pode fazer isto seguindo os passos abaixo:

1º passo: Tomar $f(x) = 4x + 5$ como $y = 4x + 5$ e trocar x por y.

$$y = 4x + 5 \rightarrow x = 4y + 5.$$

2º passo: Obter da equação anterior, y em função de x.

$$x = 4y + 5 \rightarrow y = \frac{x - 5}{4}$$

Por fim, a função inversa de $f(x) = 4x + 5$ será indicada por $f^{-1}(x) = \frac{x-5}{4}$

Assim, o receptor faz o processo inverso, retornando à mensagem original:

$f^{-1}(17) = \frac{17-5}{4} = 3$ e o número 3 está associado à letra C.
$f^{-1}(57) = \frac{57-5}{4} = 13$ e o número 13 está associado à letra P.
$f^{-1}(69) = \frac{69-5}{4} = 16$ e o número 15 está associado à letra M.
$f^{-1}(9) = \frac{9-5}{4} = 1$ e o número 1 está associado à letra A.

A função $f^{-1}(x) = \frac{x-5}{4}$ será a **chave de decodificação**.

Observação: uma alternativa seria calcular os valores de x quando $f(x) = 17$, $f(x) = 57$, $f(x) = 69$ e $f(x) = 9$. O resultado seria o mesmo.

Exercício 1. Utilizando a Tabela 1 e as leis das funções propostas, **codifique**:

a) A palavra CARRO com a função de lei $f(x) = x + 10$.

Resposta: Como C=3, A=1, R=18 e O=15, calculamos $f(3) = 3 + 10 = 13$; $f(1) = 1 + 10 = 11$, $f(18) = 18 + 10 = 28$ e $f(15) = 15 + 10 = 25$. CARRO fica codificado como 13 ; 11 ; 28 ; 28 ; 25.

b) A palavra SEMPRE com a função de lei $g(x) = -5x + 12$.

Resposta: Como S=19, E=5, M=13, P=16 e R=18, calculamos $g(19) = -5.19 + 12 = -83$; $g(5) = -5.5 + 12 = -13$, $g(13) = -5{,}12 + 12 = -53$; $g(16) = -5.16 + 13 = -67$ e $g(18) = -5.18 + 13 = -77$. SEMPRE fica codificada como -83 ; -13 ; -53 ; -67 ; -77 ; -13.

c) A palavra FÁCIL com a função de lei $h(x) = 9x$ (desconsidere o acento no “A”).

Resposta: Como F=6, A=1, C=3, I=9 e L=12, calculamos $h(6) = 9.6 = 54$; $h(1) = 9.1 = 9$, $h(3) = 9.3 = 27$; $h(9) = 9.9 = 81$ e $h(12) = 9.12 = 108$. FÁCIL fica codificada como 54 ; 9 ; 27 ; 81 ; 108.

Exercício 2. Utilizando a Tabela 1 e as leis das funções propostas, **decodifique**:

a) A mensagem 179 ; 143 ; 116, sabendo que foi codificada com a função $g(x) = 9x + 8$.
Resposta: a função inversa de $g(x) = 9x + 8$ é $g^{-1}(x) = \frac{x-8}{9}$. Assim, $g^{-1}(179) = \frac{179-8}{9} = 19$, $g^{-1}(143) = \frac{143-8}{9} = 15$ e $g^{-1}(116) = \frac{116-8}{9} = 12$. Consultando a Tabela 1, 19=S, 15=O e 12=L. A mensagem original era SOL.

b) A mensagem –12; – 108; – 6; –114; – 54; – 72, sabendo que foi codificada com a função $t(x) = -6x$.

Resposta: a função inversa de $t(x) = -6x$ é $t^{-1}(x) = -\frac{x}{6}$. No entanto, é até mais simples resolver, $-6x = -12$, encontrando $x = 2$; $-6x = -108$ com $x = 18$, $-6x =$

-6 com $x = 1$; $-6x = -114$ com $x = 19$, $-6x = -54$ com $x = 9$ e $-6x = -72$ com $x = 12$. Consultando a Tabela 1, 2=B, 18=R, 1=A, 19=S, 9=I e L=12. A mensagem original era BRASIL.

c) A mensagem $\frac{7}{4}$; $\frac{13}{4}$; $\frac{61}{4}$, sabendo que foi codificada com a função $s(x) = \frac{3}{4}x - \frac{1}{2}$.

Resposta: a função inversa de $s(x) = \frac{3}{4}x - \frac{1}{2}$ é igual a $s^{-1}(x) = \frac{4}{3}x + \frac{2}{3}$. Assim, $s^{-1}\left(\frac{7}{4}\right) = \frac{4}{3}.\frac{7}{4} + \frac{2}{3} = 3$, $s^{-1}\left(\frac{7}{4}\right) = \frac{4}{3}.\frac{13}{4} + \frac{2}{3} = 5$ e $s^{-1}\left(\frac{61}{4}\right) = \frac{4}{3}.\frac{61}{4} + \frac{2}{3} = 21$. Consultando a Tabela 1, 3=C, 5=E e 21=U. A mensagem original era CÉU (onde foi acrescentando o acento).

Até agora, trabalhamos com funções do tipo afim, com lei $f(x) = ax + b$, para $a, b \in \mathbb{R}$ e $a \neq 0$. Os próximos exercícios discutem os cuidados que devemos ter ao trabalhar com funções do tipo quadráticas, $f(x) = ax^2 + bx + c$, para $a, b, c \in \mathbb{R}$ e $a \neq 0$.

Exercício 3. Utilizando a Tabela 1 e a função $f(x) = -2x^2 + 3$, faça o que se pede:

a) Codifique a mensagem GIZ.

Resposta: Como G=7, I=9 e Z=26, temos $f(7) = -2.7^2 + 3 = -95$, $f(9) = -2.9^2 + 3 = -159$ e $f(26) = -2.26^2 + 3 = -1349$, a mensagem fica codificada como -95; -159; -1349.

b) Decodifique a mensagem -797; -47; -645.

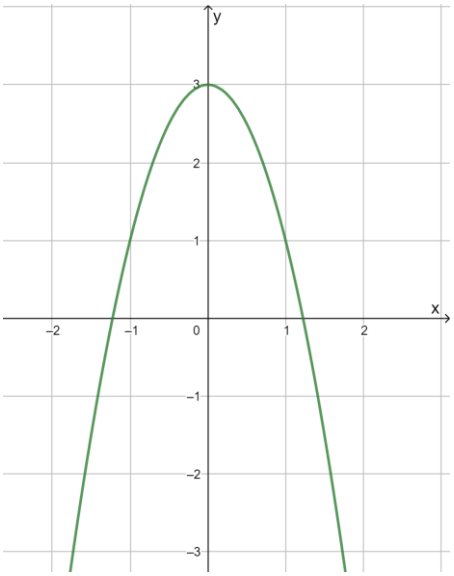
Resposta: Resolvendo -797=-2x²+3, encontramos x'=-20 e x"=20. Consultando a Tabela 1, apenas 20=T apresenta correspondência. Desconsideramos x'=-20. Resolvendo -47=-2x²+3, encontamos x'=-5 e x"=5. Consideramos apenas x"=5 com correspondência E=5. Por fim, -645=-2x²+3, resultando em x'=-18 e x"=18. Consideramos apenas x"=18 com correspondência R=18. A mensagem original era TER.

c) Encontre a chave de decodificação.

Resposta: Sendo $y = -2x^2 + 3$, temos $x = -2y^2 + 3$, com $y = \pm\sqrt{-\frac{x-3}{2}}$. Como $1 \leq y \leq 26$, vamos considerer apenas $y = \sqrt{-\frac{x-3}{2}}$.

d) Esboce o gráfico da função de lei $f(x) = -2x^2 + 3$.

Resposta: Sugere-se que o aluno esboce o gráfico manualmente, em um primeiro momento.



Este exercício é particularmente interessante por permitir discussões sobre domínio, contradomínio, visto que considerando as entradas da Tabela 1 (números naturais entre 1 e 26) deverão ser estudados apenas os pontos que estarão neste intervalo, mas que obedecem a um comportamento quadrático. Outro ponto fundamental que pode ser explorado é a simetria da parabola em relação ao vértice

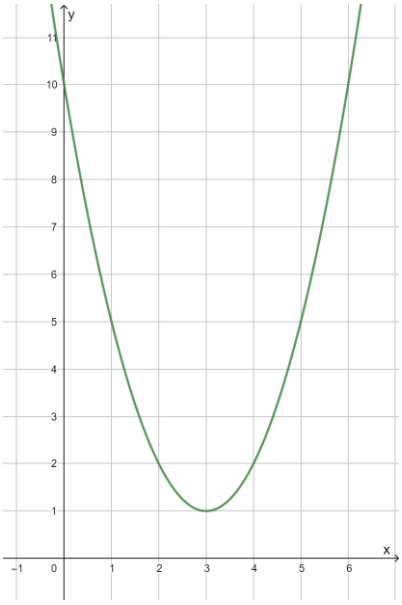
Exercício 4. Utilizando a Tabela 1 e a função $g(x) = x^2 - 6x + 10$:

a) Explique por que existirá ambiguidade na codificação da palavra BODE.

Resposta: da Tabela 1, temos B=2, O=15, D=4 e E=5. Calculando, g(2)=2²-6.2+10=2, g(15)=15²-6.15+10=145, g(4)=4²-6.4+10=2 e g(5)=5²-6.5+10=5. Assim, BODE seria codificado como 2; 145; 2; 5. O receptor da mensagem, na decodificação, não teria certeza se 2 representa B ou D, nem se 5 representa A ou E.

b) Esboce o gráfico da função de lei $g(x) = x^2 - 6x + 10$.

Resposta: Sugere-se que o aluno esboce o gráfico manualmente, em um primeiro momento.



c) Explique por que a chave de codificação $f(x) = -2x^2 + 3$ do exercício anterior não gera ambiguidade, ao contrário da chave de codificação $g(x) = x^2 - 6x + 10$, comparando o esboço de seus gráficos e suas respectivas chaves de decodificação (função inversa).

Resposta: aqui podem ser propostas discussões sobre a injetividade de uma função. A função f é injetiva considerando o intervalo dos naturais entre 1 e 26, o que não ocorre com a função g. Maiores discussões podem ser realizadas com a exploração de *softwares* gráficos. Nesta linha, sugere-se o *Geogebra*.

Exercício 5. Troque uma mensagem curta com um colega, criando uma chave de codificação e um alfabeto cifrado (pode ser o da Tabela 1) convencionado entre vocês.

Resposta pessoal.