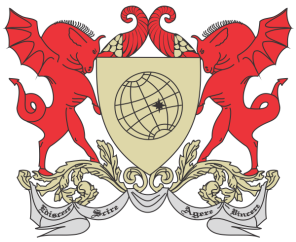
Universidade Federal de Viçosa
Produto Educacional
Produto Educacional



Alexandre Gonçalves Batista

Criptografia no Ensino Básico

FLORESTAL – MINAS GERAIS
2024

ALEXANDRE GONÇALVES BATISTA

Orientador: Luís Felipe Gonçalves Fonseca

FLORESTAL – MINAS GERAIS
2024

Lista de Comandos para o Google Planilhas e Excel

Comando	Função
*	Inserir símbolo da multiplicação
/	Inserir o símbolo da divisão
CIRCUNFLEXO (^)	Inserir símbolo da potenciação
=MMC(A3:A6)	Calcula o mmc dos números inseridos nas células A3 até A6
=MMC(A3;A6) ou =LCM(A3;A6)	Calcula o mmc dos números inseridos nas células A3 e A6
=MDC(A3;A6) ou GCD(A3;A6)	Calcula o mdc dos números inseridos nas células A3 e A6
=PROCV(C2;A$2:B$27;2;0) ou =VLOOKUP(C2;A$2:B$27;2;0)	Procurar o valor C2 na tabela (A2 até B27) e retornar o número da coluna B que está na mesma linha do valor C2, porém na coluna A. O último parâmetro 0 é padrão
=SOMA(C3:C7)	Calcula a soma dos números inseridos nas células C3, C4, C5, C6 e C7.

Lista de Figuras

Sumário

1

Introdução

O presente produto educacional é resultado do trabalho desenvolvido em uma dissertação de mestrado do curso Profmat. O objetivo é apresentar propostas de ensino da matemática, utilizando a criptografia, para professores e alunos da Educação Básica. Assim, são realizadas a codificação e decodificação de mensagens, aplicando alguns métodos criptográficos.

Para facilitar o procedimento e trazer uma abordagem mais tecnológica ao nosso estudo, apresentamos funcionalidades do Google Planilhas, que automatizam o trabalho repetitivo. Em alguns casos, implementamos programações no software, de modo que, ao alterarmos a mensagem ou os parâmetros do método criptográfico adotado, a tarefa seja realizada sem grande esforço. As planilhas são, portanto, automatizadas.

Em algumas situações, utilizamos o programa Wolfram Alpha para realizar cálculos de congruências modulares com números grandes. Esse programa tem menos limitações do que o Google Planilhas, que encontrou dificuldades em alguns desses cálculos.

Por fim, disponibilizamos um plano de aula para cada método de cifra, utilizando os recursos computacionais mencionados, além de atividades de aritmética voltadas ao ensino básico.

O diferencial deste trabalho é a utilização do Google Planilhas como processador de cálculos. Queremos mostrar aos estudantes a importância de conhecer as propriedades matemáticas aplicadas à programação. Portanto, antes de utilizar o Planilhas e o Wolfram Alpha, é essencial que o professor tenha apresentado a teoria, explicado os algoritmos e proposto exercícios práticos. A tecnologia deve ser usada como uma estratégia para consolidar o conteúdo aprendido, além de familiarizar os estudantes com a interpretação de dados em planilhas e com as fórmulas (funções) usadas em ambientes de programação.

Desejamos a todos uma leitura agradável e proveitosa.

2

Google Planilhas e Wolfram Alpha no Ensino de Matemática na Educação Básica

A cada avanço tecnológico, nossa sociedade é transformada. Desse modo, faz-se necessário pensar em processos de ensino e aprendizagem que acompanhem essas transformações.

Conhecer e manipular tecnologias digitais que possam contribuir para o ensino de matemática, tornou-se um dos objetivos do presente trabalho. Sendo assim, buscamos a produção de materiais que sirvam como suporte para docentes que desejam assegurar aos alunos o desenvolvimento de algumas competências relacionadas com o ensino e aprendizagem de matemática, conforme estabelece a BNCC (Base Nacional Comum Curricular) ([1],p.267).

> *Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.*

Inicialmente, apresentaremos algumas funcionalidades do editor **Google Planilhas** enquanto recurso educacional. Este será utilizado para o processamento de cálculos mecânicos. Assim, buscamos que o estudante desenvolva a habilidade de analisar criticamente e aplicar conceitos matemáticos, deixando em segundo plano o papel de mero executor cálculos.

O Google Planilhas é um editor de planilhas eletrônicas online, oferecido pela plataforma Google Workspace. Sua interface e funcionalidades se assemelham com o programa Excel, mostrando-se uma poderosa ferramenta de automação de cálculos, criação e leituras de gráficos e tabelas, além de um ótimo organizador de dados. Para completar, três vantagens do editor Google Planilhas foram determinantes para a escolha da ferramenta. A primeira, foi a gratuidade de editor. Em seguida, sua função de trabalho colaborativo em tempo real. Por fim, sua maior compatibilidade com smartphones e tablets.

Esses editores de planilhas, devido a suas funcionalidades, são bem conhecidos em rotinas administrativas e empresariais. No entanto, buscamos maior utilização no ensino da educação básica.

Seguem descrições de atividades que podem ser utilizadas em sala de aula. Nesse momento, apresentamos com uma maior riqueza de detalhes como o editor pode ser usado no ensino. Para além, o leitor poderá conferir planos de aula na sessão *Aplicação de tecnologias em aulas de matemática* e uma lista de exercícios propostos.

2.1 Descrição de atividades no Google Planilhas

Antes de iniciar as atividades, é importante reservar um tempo e fazer algumas orientações que favoreçam a interação do aluno com o editor. Informações como, acesso ao editor de Planilhas, renomear, salvar e abrir algum trabalho são importantes. O conhecimento da sua interface, bem como a percepção de que cada célula funciona como uma "calculadora"; para isso basta iniciar a inserção dos dados com o sinal de "=", são requisitos fundamentais para as atividades aqui propostas. Essas experiências podem aumentar o interesse do estudante, fazendo com que ele tenha uma noção inicial da ferramenta que utilizará.

O editor pode ser uma ferramenta de aprendizagem para vários conteúdos matemáticos, inclusive para criptografia.

As próximas 11 atividades podem ser acessadas no link https://l1nk.dev/mEcsY. Isso permitirá ao professor leitor a verificação dos resultados. No entanto, esclarecemos que todas as planilhas estão disponíveis apenas para leitura. Para editar uma planilha, o leitor deverá baixá-la ou copiá-la para uma planilha pessoal.

2.1.1 Cálculo de MDC e MMC no Google Planilhas

Para realizar o cálculo do MDC ou do MMC de dois ou mais números, o Google Planilhas possui uma fórmula própria. Trazemos um exemplo de utilização do cálculo de MMC, somente com o objetivo de ambientação com o editor, uma vez que não usaremos esse conteúdo nos processos criptográficos.

Exemplo 2.1.1: Atividade 1.

Propor o cálculo do MMC de quatro números. Para a realização dessa atividade, vamos construir uma tabela.

1) Na célula A1, inserimos o enunciado do exercício: "ENCONTRE O MMC DOS NÚMEROS". Essa célula pode ser mesclada com B1 por motivo estético.

2) Na célula A2, vamos inserir nome da coluna, escolhemos a descrição "Números".

3) Na célula B2, entramos com a descrição "Resultado".

4) Nas células A3 até A6, inserimos os números 7, 12, 15 e 18. Um em cada célula.

5) Na célula A7, inserimos a descrição "MMC". Na célula defronte, B7, inserimos a formula

=MMC(A3:A6).

O resultado, do mmc dos números inseridos nas células A1 até A6, será calculado na célula B7, e os alunos poderão fazer novos testes trocando os números da coluna A. Com isso, a programação realizada possibilitará novos resultados. O professor pode ensinar como formatar a tabela, além de explorar propriedades do MMC e do seu cálculo.

	A	B	C	D	E	F	G	H
1	ENCONTRE O MMC DOS NÚMEROS			ENCONTRE O MMC DOS NÚMEROS			ENCONTRE O MMC DOS NÚMEROS	
2	Números	resultado		Números	resultado		Números	resultado
3	7			7			7	
4	12			9			14	
5	15			16			28	
6	18			25			56	
7	mmc	1260		mmc	25200		mmc	56
8	Produto	22680		Produto	25200		Produto	153664
9	Tabela I			Tabela II			Tabela III	

Figura 2.1: MMC (Autoria própria)

Atividade disponível na página "Atividade 1" em https://l1nk.dev/mEcsY.

Exemplo 2.1.2: Atividade 2.

Encontrar os possíveis restos da divisão de um número inteiro, coprimo com 26, por 26. Nessa atividade, será explorada a propriedade do MDC de dois números coprimos. Trabalharemos também com a construção de uma tabela composta por 15 linhas e 2 colunas. Para a realização da atividade, siga os passos a seguir que pode ser acompanhada na página "Atividade 2" da mesma planilha.

1) Inserir a descrição da atividade nas células A1, que receberá o texto "NÚMEROS COPRIMOS COM". Na célula B1, insira o número a ser analisado. Neste exemplo, será o "26". Agora a tabela deve ser rotulada, começamos pela coluna A. A célula A2 receberá a inscrição: "NÚMERO A". Logo após, a célula B2 deve receber o texto "MDC(A,26)=1".

2) Na coluna A, vamos inserir os números que podem ser coprimos com 26. Inserimos o número 1 na célula A3 e, 2 na célula A4. Na célula A5 inserimos o número 3, e da célula A6 em diante, vamos inserir uma sequência de números ímpares. Para isso, basta entrar com o número 5 na célula A6. Depois, deve-se selecionar as duas últimas células, posicionar o cursor no canto inferior direito da última célula selecionada, e arrastar o cursor para baixo com o botão de clique pressionado, até chegar ao número 25.

3) Na célula B3, insera a fórmula

MDC(A3;B$1)

e conclua teclando em "Enter". Essa função calcula, inicialmente, o MDC do número inserido em A3 e o número inserido em B1. Logo após, use a função arrastar o cursor para baixo, até a linha que tenha um número correspondente na coluna A. Assim, o editor calcula o MDC de cada célula abaixo de A3 e o número inserido em B1 (o símbolo "$" fixa a célula na fórmula, impedindo que a cada linha que descemos seja usada, na fórmula, o valor de cada célula abaixo de B1).

4) Por fim, deve ser feita a análise de quais células, da coluna B, possuem o número 1 como resultado.

A quantidade de números com essa propriedade é, neste caso, igual a 12. São os números da coluna "A" nos quais tem correspondentes iguais a 1 na coluna "B".

	A	B
1	NÚMEROS COPRIMOS COM	26
2	NÚMERO A	MDC (A,26)=1
3	1	1
4	2	2
5	3	1
6	5	1
7	7	1
8	9	1
9	11	1
10	13	13
11	15	1
12	17	1
13	19	1
14	21	1
15	23	1
16	25	1

Figura 2.2: Coprimos com 26 (autoria própria)

Nesta atividade, o que de fato estamos calculando é a função φ de Euler para o número 26. No ensino básico, não é comum realizar atividades com essa denominação.

Fica a cargo do professor mencionar ou não essa aplicação. Ainda neste sentido, torna se interessante escolher números primos aleatórios para realizar os testes dessa atividade. Feito isso, será possível verificar o cálculo da função $\varphi(m)$ para m primo, como pode ser observado em Hefez ([2],p.155-160).

Atividade disponível na página "Atividade 2" em https://l1nk.dev/mEcsY.

2.1.2 Teste de primalidade no Google Planilhas

Testaremos a primalidade de alguns números usando o Google Planilhas. Este material de estudos foi pensado para o Ensino Fundamental Anos finais (6° ano até

9° ano), podendo ser trabalhado em qualquer Ano (Série) dessa etapa de ensino. Nesse sentido, vamos explorar o **Método da Divisão**, visto na seção Testes de Primalidade, aplicado no Google Planilhas.

Exemplo 2.1.3: Atividade 3.
Testar a primalidade de 1117.

1) Abra o Google Planilhas.

2) Estabeleça o número que deseja investigar a primalidade. Por exemplo, ao investigar o número 1117, devemos inseri-ló na célula B2.

3) Vamos construir uma tabela. As linhas 1, 2 e 3 foram destinadas às informações da tabela. Nessa parte, será exibido os rótulos das colunas, o número a ser investigado, bem como o valor aproximado de sua raiz quadrada.

4) Na coluna A, a partir da 4ª linha, inserimos uma lista de números. Vamos iniciar essa lista pelo número 2, e depois vamos inserir todos os números ímpares menores ou iguais do que a parte inteira da raiz quadrada do número avaliado. O programa tem uma fórmula que calcula a raiz quadrada, que será inserida na célula D2

   $$=\text{RAIZ(B2)}.$$

   Essa fórmula devolve a raiz quadrada do número inserido na célula B2. Porém vamos considerar somente a parte inteira do resultado obtido. É importante mostrar para o estudante que, ao inserirmos uma fórmula referente à célula (B2), ao invés do número nela inserido, tem-se procedimento que facilita o cálculo da raiz quadrada de qualquer outro número. Nesse caso, basta trocar o inserido na célula B2 pelo novo número e o editor calcula o valor.

5) Na construção da lista de números, vamos observar a raiz quadrada que encontramos no item anterior. No nosso caso, encontramos um número menor do que 33. Assim, vamos listar os números 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31 e 33. Com essa listagem, vamos utilizar a função autocompletar. O programa facilitou esse processo. Para isso, fizemos o seguinte: inserimos o número 2 na célula A4, nas células A5 e A6 entramos com os números 3 e 5, respectivamente. Logo após, selecionamos as células A5 e A6, em seguida posicionamos o cursor no canto inferior direito da segunda célula selecionada e arrastamos para as células abaixo. Com isso, o programa vai completando a sequência de números ímpares até o número desejado.

6) Na célula B4, devemos inserir a fómula: o quociente da célula B2 (1117) pela célula A4, célula da coluna A na mesma linha de B4. Por exemplo, na célula B4, vamos inserir a fórmula:

   $$=\text{B\$2/A4}.$$

O símbolo "/" é o comando para a operação de divisão, já o símbolo "$" serve para fixar a célula B2. Desse modo, quando arrastarmos o cursor da célula B4 para uma posição para baixo, o programa vai inserir, automaticamente, na célula B5, a fórmula "=B$2/A5". Para encontrarmos todos os valores dessa coluna, basta selecionar a célula B4 e arrastar até a linha desejada.

Verificamos que o número 1117 é primo, uma vez que nenhum dos quocientes encontrados até o número 33 é inteiro.

Feito isso, o professor pode explicar a teoria presente no procedimento, uma vez que as contas foram todas feitas pela máquina. Apesar de não termos feitos nenhum cálculo, nosso conhecimento foi utilizado para programar a plataforma.

	A	B	C	D
1	VERIFICAÇÃO DE PRIMALIDADE			RESULTADO
2	Número	1117	Raiz quadrada	33,42154993
3	N	Quociente de B2 por A(N)		
4	2	558,5		
5	3	372,3333333		
6	5	223,4		
7	7	159,5714286		
8	9	124,1111111		
9	11	101,5454545		
10	13	85,92307692		
11	15	74,46666667		
12	17	65,70588235		
13	19	58,78947368		
14	21	53,19047619		
15	23	48,56521739		
16	25	44,68		
17	27	41,37037037		
18	29	38,51724138		
19	31	36,03225806		
20	33	33,84848485		
21	ANÁLISE:	NÃO ENCONTRADO QUOCIENTE INTEIRO.		
22	CONCLUSÃO:	1117	É PRIMO	

Figura 2.3: Teste de primalidade de 1117 (autoria própria)

O leitor pode acessar esta atividade na página "Atividade 3" por meio do link: https://l1nk.dev/mEcsY.

Exemplo 2.1.4: Atividade 4.

Outra alternativa pode ser a função "MOD" do Google Planilhas que informa o resto de uma divisão. Para isso, podemos seguir os passos 1 até 5 do Exemplo 2.1.3. Já no item 6, basta modificar a fórmula da célula B4 por

$$=\text{MOD}(\text{B\$2;A4}),$$

e fazer a análise dos restos.
Neste caso, devemos observar que nenhum dos quocientes é igual a 0 (zero).
Atividade disponível na página "Atividade 4" em https://l1nk.dev/mEcsY.

2.1.3 Cifras de Substituição no Google Planilhas

Exemplo 2.1.5: Atividade 5

Cifrar a frase "A MATEMÁTICA É BELA", usando cifras de César, com a chave "E".

1) Abra o Google Planilhas.

2) Construir uma tabela com quatro colunas. A célula A1 indicará que se trata da coluna do "Texto Original". É nela que estará o alfabeto original. Para isso, a célula A2 deve conter a seguinte fórmula:

   =ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).

   Essa fórmula "gera" uma sequência de 26 letras do alfabeto, uma em cada linha. O programa insere os caracteres por meio de linguagem de programação, utilizando a tabela ASCII (tabela de códigos binários), apresentada na Figura 5.1 do Apêndice A. Assim, essa lista de caracteres tem início no símbolo 65 da tabela ASCII, que corresponde à letra "A" (maiúscula) e termina no código 90 (65 + 26 - 1), que tem como corresponde a letra "Z"(maiúscula).

3) A célula B1 receberá a descrição: "Cifra". Nessa coluna, estarão presentes os códigos representantes de cada letra do alfabeto original. Dessa forma, vamos inserir na célula B2 a seguinte fórmula:

   =ARRAYFORMULA(CARACT(SEQUENCE(22;1;69))).

   Repare que mudamos o primeiro parâmetro da fórmula para 22. Assim, as quatro últimas células dessa coluna devem ser preenchidas manualmente. O terceiro parâmetro também foi modificado de 65 para 69. Pois desejamos iniciar o alfabeto pela letra "E", quatro letras à frente, logo devemos aumentar quatro unidades nessa fórmula.

4) Na terceira coluna, inserimos a mensagem para ser codificada. Nesse caso, C1 terá "Mensagem Original" como descrição. Cada letra da mensagem deve ser digitada em uma única célula dessa coluna.

5) Por fim, a última coluna nos retornará a "Mensagem Cifrada", texto que colocaremos na célula D1. Já em D2, deve ser inserida a fórmula:

   =PROCV(C2;A$2:B$27;2;1).

Após a inserção dessa fórmula, basta arrastar para baixo a célula onde está a função, a partir da célula D2, até a linha desejada. Feito isso, a mensagem aparecerá na coluna D.

Na fórmula "PROCV", procura-se o valor inserido em C2 na tabela formada pelos valores de A2 até B27 (o "$" mantém a tabela fixa nesses valores). No entanto, ela retorna como resultado o valor da coluna B que está na mesma linha do valor inserido em C2. Por isso, o terceiro parâmetro da fórmula é o número 2. O último parâmetro é padrão, neste caso.

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

Figura 2.4: Cifra de César chave "E" (autoria própria)

A mensagem "A MATEMÁTICA É BELA" é transformada em

E Q E X I Q E X M G E I F I P E.

O leitor pode conferir esta atividade na página "Atividade 5" em https://l1nk.dev/mEcsY.

Exemplo 2.1.6: Atividade 6

Decifrar a mensagem

S P I K E H S H I I V E X S W X I R I W

usando a cifra de César com a chave E.

1) Abra o Google Planilhas.

2) Na coluna A, deve ser colocado o dicionário de cifras. Contudo, o primeiro código é a letra "E", logo devemos inserir o alfabeto começando por essa letra:

   $$=\text{ARRAYFORMULA(CARACT(SEQUENCE(22;1;69))).}$$

   Note que a lista começa na letra E e termina na letra Z, com isso devemos completar mais quatro letras iniciando pela letra A.

3) Na coluna B, deve ser colocado o texto original.

4) Na coluna C, vamos digitar a mensagem codificada inserindo cada letra em uma célula desta coluna.

5) Na coluna D, vamos recuperar cada letra da mensagem original. Para isso, insira, na célula D2, a fórmula:

   $$=\text{PROCV(C2; } A\$2 \text{ :B\$27; 2; 1).}$$

   A mensagem original encontrada será

   O LEGADO DE ERATÓSTENES.

Atividade disponível na página "Atividade 6" em https://l1nk.dev/mEcsY.

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

Figura 2.5: Decodificação pela cifra de César (autoria própria)

2.1.4 Cifra Afim no Google Planilhas

Exemplo 2.1.7: Atividade 7

Criptografar a mensagem "O ALUNO FOI BEM NA PROVA", utilizando a função $f(x) = 7x + 6$.

1) Abra o Google Planilhas.

2) Vamos estabelecer o dicionário de caracteres com 26 letras (na ordem alfabética) que serão substituídas por números inteiros de 10 até 35.

3) O texto original deve estar na coluna A. Na célula A2, digite:

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

4) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo.

5) Na coluna C, digite a mensagem original, com cada letra em uma célula.

6) Na coluna D, busque cada correspondente das letras, no dicionário de Cifras (estamos usando a cifra de substituição). Para isso, basta inserir, em D2 a fórmula:

$$=\text{PROCV(C2;A\$2:B\$27;2;0)}.$$

Depois complete a coluna com a função arrastar, para baixo, o cursor.

7) A coluna E será destinada para encontrar os valores de cada cifra aplicada à função escolhida. Na célula E2, vamos inserir a função:

$$=7*\text{D2}+6.$$

Em seguida, complete a coluna com a função arrastar. A mensagem criptografada será calculada automaticamente. O símbolo "*" representa o sinal de multiplicação.

	A	B	C	D	E
1	TEXTO ORIGINAL	CIFRA	MENSAGEM	PRÉ CODIFICAÇÃO	CIFRA POR f(x)= 7x + 6
2	A	10	O	24	174
3	B	11	A	10	76
4	C	12	L	21	153
5	D	13	U	30	216
6	E	14	N	23	167
7	F	15	O	24	174
8	G	16	F	15	111
9	H	17	O	24	174
10	I	18	I	18	132
11	J	19	B	11	83
12	K	20	E	14	104
13	L	21	M	22	160
14	M	22	N	23	167
15	N	23	A	10	76
16	O	24	P	25	181
17	P	25	R	27	195
18	Q	26	O	24	174
19	R	27	V	31	223
20	S	28	A	10	76
21	T	29			
22	U	30			
23	V	31			
24	W	32			
25	X	33			
26	Y	34			
27	Z	35			

Figura 2.6: Cifra Afim $f(x) = 7x + 6$ (autoria própria)

A mensagem codificada é

174 76 153 216 167 174 111 174 132 83 104 160 167 76 181 195 174 223 76.

Atividade com acesso na página "Atividade 7" em https://l1nk.dev/mEcsY.

Exemplo 2.1.8: Atividade 8

Decifrar o código

22 73 46 79 58 34 79 46 28 22 61 22 28 73 46 67 79 64 40 73 22 37 46 22,

criptografado pela cifras de substituição de chave 10 (alfabeto na sua ordem original) e pela função afim $f(x) = 3x - 8$.

Para resolver essa atividade, o caminho é construir uma tabela com quatro colunas e 27 linhas.

1) Determinar a função inversa de $f(x) = 3x - 8$. Sugerimos que esse cálculo seja feito manualmente pelos alunos.

2) Abrir o Google Planilhas.

3) Inicialmente, vamos rotular a coluna A, inserindo o texto "CIFRA" na célula A1. Da célula A2 até A27, insira a sequência de números inteiros começando pelo número 10. Como o procedimento é o inverso da codificação, devemos inserir primeiro a coluna de Cifras. O procedimento deve ser realizado desse modo para que a função "PROCV" funcione corretamente.

4) Rotular a coluna B, inserindo o texto "TEXTO ORIGINAL" na célula B1 e expandir o alfabeto nessa coluna. Para isso, basta digitar em B2 o comando

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))}.$$

5) Na coluna C, insira as cifras da mensagem secreta, uma em cada célula, iniciando em C2. Rotule essa coluna inserindo o texto "MSG CODIFICADA" em C1.

6) Na coluna D, aplique cada número da coluna C na inversa da função que é expressa por $f^{-1}(x) = \frac{x}{3} + \frac{8}{3}$. Fazemos isso, inserindo em D2 a fórmula

$$=\text{(C2/3)+(8/3)}.$$

Logo após, arraste o curso para completar todos os dados dessa coluna. Rotule essa coluna com a expressão da função inversa determinada.

7) Na coluna E, que recebe em E1 o rótulo "MSG ORIGINAL", faça o processo inverso da pré-codificação. Para isso, vamos procurar (função PROCV) o item da coluna D, na tabela formada pelas colunas A e B, verificando qual é seu correspondente na coluna B. Insira em E2 a seguinte função:

$$=\text{PROCV(D2;A2} : B27;\ 2;\ 0).$$

Logo após, use a funcionalidade arrastar o curso, pra baixo, para completar a tabela.

A mensagem original é revelada:

A R I T M E T I C A N A C R I P T O G R A F I A.

O leitor pode visualizar o resultado final dessa atividade em Figura 2.7 e a planilha produzida pode ser acessada na página "Atividade 8" em https://l1nk.dev/mEcsY.

	A	B	C	D	E
1	CIFRA	TEXTO ORIGINAL	MSG CODIFICADA	f⁻¹(x)=(x/3)+(8/3)	MSG ORIGINAL
2	10	A	22	10	A
3	11	B	73	27	R
4	12	C	46	18	I
5	13	D	79	29	T
6	14	E	58	22	M
7	15	F	34	14	E
8	16	G	79	29	T
9	17	H	46	18	I
10	18	I	28	12	C
11	19	J	22	10	A
12	20	K	61	23	N
13	21	L	22	10	A
14	22	M	28	12	C
15	23	N	73	27	R
16	24	O	46	18	I
17	25	P	67	25	P
18	26	Q	79	29	T
19	27	R	64	24	O
20	28	S	40	16	G
21	29	T	73	27	R
22	30	U	22	10	A
23	31	V	37	15	F
24	32	W	46	18	I
25	33	X	22	10	A
26	34	Y			
27	35	Z			

Figura 2.7: Decodificação por Cifra Afim (autoria própria)

2.1.5 Cifra RSA no Google Planilhas e Wolfram Alpha

Exemplo 2.1.9: Atividade 9

Criptografar a mensagem "SOMA OU TOTAL", utilizando a chave pública (91,5), com alfabeto de pré-codificação começando na cifra 10 e terminando em 35.

Antes de iniciarmos o trabalho no editor de planilhas, vamos reelembrar a construção de alguns elementos essenciais no processo de encriptação RSA. O estudo completo pode ser acessado no site: https://profmat-sbm.org.br/dissertacoes/ dissertação: "Criptografia no Ensino Básico", seção "Contexto Histórico da Criptografia", subseção "Sistema RSA de Criptografia", cujo autor é o mesmo deste produto. Primeiramente, o remetente deve conhecer a chave pública do destinatário. Essa chave é composta por dois números (n,e), que são chamados de parâmetros da chave. Para além, n é o produto de números primos e distintos p e q. Já o parâmetro e pode ser escolhido livremente, com a condição de ser coprimo com $\varphi(n)$, em que $\varphi(n) = (p-1)(q-1)$.

1) Abra o Google Planilhas.

2) Na célula A1, insira o texto "**p**". A célula B1 deve ser nomeada por "**q**". Já C1, deve ser rotulada com "**n=p.q**" e D1 deve receber o texto "**e**".

3) Nas células E1, F1 e G1, insira os respectivos textos:

"**(p-1)(q-1)**", "**mdc(e,(p-1)(q-1)** " e "**d**".

4) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Comece pela célula A2 que recebe o valor 7. B2 recebe o valor 13. Em C2, insira a fórmula "**=A2 * B2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p e q. Em seguida, insira em D2 o valor 5, como indicado na chave pública.

5) Agora, vamos programar a célula E2 com a fórmula "**=(A2 - 1)*(B2 - 1)**". F2 receberá a fórmula "**=MDC(D2;E2)**", e G2 será preenchida com o número 29, que representa o valor de "**d**", parâmetro da chave privada $(n,d) = (91,29)$.

6) O cálculo do valor de "**d**" geralmente é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir.

"**d**" é um número inteiro definido pelas duas condições,

$$ed \equiv 1(\ (\text{mod } (p-1)(q-1)) \text{ e } 1 \leq d < (p-1)(q-1).$$

Dessa forma, as condições podem ser reescritas como:

$$5d \equiv 1\ (\text{mod } 72) \text{ e } 1 \leq d < 72.$$

Nesse sentido, resolver a primeira condição equivale a solucionar a equação:

$$5d - 1 = 72x, \text{ em que } x \text{ é inteiro.}$$

Logo

$$d = \frac{72x+1}{5} = \frac{2x+1}{5} + 14x.$$

Interessa-nos encontrar um valor para x, de modo que a primeira parcela da equação acima, represente um número inteiro. Ao testar a expressão $2x + 1$, para $x \in \{0, 1, 2, 3, 4\}$, verifica-se que $2x + 1$ é divisível por 5 quando $x = 2$ (apenas ele). Temos:

$$d = \frac{2.2+1}{5} + 14.2 = 29.$$

Devemos observar que esse número atende à condição

$$1 \leq d < 72.$$

7) Voltando para a planilha, vamos estabelecer o dicionário de caracteres com 26 letras (na sua ordem natural) que serão substituídas por números inteiros de 10 até 35. Sendo assim, na célula A4, inserimos "**TEXTO ORIGINAL**" e em A5 digitamos a fórmula:

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

8) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo. Com isso, a célula B4 será rotulada com o texto "**CIFRA**" e da célula B5 em diante, colocaremos a sequência de números.

9) Na célula C4, insira o rótulo "**MENSAGEM ORIGINAL**". Nas células abaixo, vamos digitar a mensagem original, lembrando de inserir uma letra em cada célula.

10) Na coluna D, vamos "buscar" cada correspondente das letras, no dicionário de Cifras (estamos usando a cifra de substituição). Estamos pré-codificando a mensagem original. O rótulo de D4 será "**PRÉ-CODIFICAÇÃO**" e em D5 inserimos a fórmula:

$$=\text{PROCV(C5; } A\$5 : \text{B\$30; 2; 0).}$$

Em seguida, devemos completar a coluna com a função arrastar o cursor baixo.

11) A coluna E será destinada para a inserção dos "Blocos". São eles que serão codificados e seguem três exigências de formação, como observamos em Hefez ([2],p.218-219) e Shokranian ([3],p.46-48). Os blocos são números formados a partir da mensagem pré-codificada e para formá-los, devemos primeiramente, visualizar a mensagem pré-codificada como um único número. Assim, visualizaremos um número com muitos algarismos. Logo após, devemos "quebrar" os algarismos, desse número, em numerais menores B_1,B_2...B_r, com $1, 2, ..., r$ números naturais, de modo que cada numeral atenda às condições:

- $B_r < pq$;
- $B_r \not\equiv 0 \pmod{p}$ e $B_r \not\equiv 0 \pmod{q}$;
- Nenhum bloco pode iniciar com o algarismo zero.

Dessa maneira, vamos rotular a coluna E, inserindo na célula E5 o texto "**BLOCOS B ($<$ pq)**", em seguida apenas copiamos os pré-códigos da coluna D para serem colados na célula E5. Precisaremos avaliar essa coluna, no entanto, faremos isso com auxílio do editor de planilhas. Nesse sentido, caminhamos ao passo seguinte para facilitar a avaliação.

12) Na coluna F, vamos verificar quais Blocos são incongruentes a zero módulo p. A célula F4 terá a inscrição: "$\mathbf{B} \not\equiv \mathbf{0} \pmod{p}$". Na célula F5, inserimos a fórmula:

$$=\text{MOD(E5;A\$2)}.$$

Em seguida, usamos a função autocompletar. Para isso, selecionamos essa célula e posicionamos o cursor no canto direito inferior dessa célula. Ao aparecer uma cruz, arrastamos para baixo. Não analisaremos os resultados ainda, sigamos para o próximo passo.

13) Repetimos o passo anterior com algumas adaptações. A primeira é rotular a coluna G, inserindo em G4 o texto "$\mathbf{B} \not\equiv \mathbf{0} \pmod{q}$". Em seguida, na célula G5 inserimos a fórmula:

$$=\text{MOD(E5;B\$2)}.$$

14) Nesse passo, analisaremos simultaneamente as colunas F e G para que atendam às três condições do Item 11). Começaremos pela segunda condição, verificando que nenhum valor dessas colunas seja 0 (zero). Se isso ocorrer, passamos para a próxima análise. Caso contrário, voltamos à coluna dos blocos (Coluna E) e modificamos os valores que não atendem às condições das colunas F e G. A modificação de um bloco será realizada por meio da separação de seus algarismos, criando dois novos blocos que serão vizinhos na coluna. Da mesma forma, dois blocos vizinhos podem ser unidos formando um único bloco. No entanto, o valor do bloco deve ser menor do que n, isso satisfaz a primeira condição. Para finalizar, devemos observar que um bloco não pode ter o algarismo inicial igual a zero, como estabelece a terceira condição.

Esse procedimento é realizado por meio de tentativa e erro. Como já programamos as colunas F e G para apresentarem os resultados que nos interessam, cada modificação feita nas colunas de blocos reflete nas colunas F e G.

15) Sigamos para o passo final. Rotulamos a coluna H, inserindo em H4 a inscrição "$C = B\hat{}e \pmod{pq}$". Na célula H5, devemos inserir a fórmula:

$$=\text{MOD(E5 \^{}D\$2;C\$2)}.$$

Essa fórmula devolve o resto da divisão por "n" (na célula C2) de cada bloco, da coluna E, elevado (símbolo circunflexo) ao valor de "e" (presente na célula D2). Após isso, basta usar a função autocompletar, arrastando o cursor da célula selecionada para baixo.

Dessa forma, a mensagem "SOMA OU TOTAL" é transformada na mensagem criptografada

	A	B	C	D	E	F	G	H
1	p	q	p x q	e	(p -1)(q-1)	mdc(e, (p -1)(q-1	d	
2	7	13	91	5	72	1	29	
3								
4	TEXTO ORIGINAL	CIFRA	MENSAGEM ORIGINAL	PRÉ-CODIFICAÇÃO	BLOCOS B (< pxq)	B ≡/0 (mod p)	B ≡/0 (mod 13)	C=B ^e (mod pq)
5	A	10	S	28	2	2	2	32
6	B	11	O	24	8	1	8	8
7	C	12	M	22	24	3	11	33
8	D	13	A	10	22	1	9	29
9	E	14	O	24	10	3	10	82
10	F	15	U	30	24	3	11	33
11	G	16	T	29	30	2	4	88
12	H	17	O	24	29	1	3	22
13	I	18	T	29	24	3	11	33
14	J	19	A	10	29	1	3	22
15	K	20	L	21	10	3	10	82
16	L	21			2	2	2	32
17	M	22			1	1	1	1
18	N	23						
19	O	24						
20	P	25						
21	Q	26						
22	R	27						
23	S	28						
24	T	29						
25	U	30						
26	V	31						
27	W	32						
28	X	33						
29	Y	34						
30	Z	35						
31								

Figura 2.8: RSA chave (91,5) (autoria própria)

32 8 33 29 82 33 88 22 33 22 82 32 1,

utilizando a chave pública (91,5).

A planilha pode ser acessada na página "Atividade 9" em https://l1nk.dev/mEcsY.

Exemplo 2.1.10: Atividade 10

Decifrar a mensagem

32 8 33 29 82 33 88 22 33 22 82 32 1,

criptografada com a chave pública (91,5) e o alfabeto de substituição com cifras de 10 a 35.

Como o receptor da mensagem codificada foi o responsável por construir a chave pública usada na codificação, somente ele conhece a chave privada. É nesse momento que o sistema de criptografia RSA mostra sua segurança, uma vez que, para encontrarmos o parâmetro d (da chave privada), necessitamos conhecer os números primos p e q que formam o parâmetro n da chave pública.

Atualmente, procedimentos que envolvem a criptografia RSA utilizam dois números primos com mais de uma centena de algarismos. Consequentemente, o número n se torna um número muito grande, tornando sua decomposição em fatores primos trabalhosa e demorada até para as máquinas e/ou programas mais tecnológicos.

Nesse sentido, o receptor autorizado a ler a mensagem é aquele que definiu ou tem conhecimento das duas chaves.

1) Abra o Google Planilhas.

2) Na célula A1, insirimos o texto "**n**". A célula B1 será rotulada com "**d**".

3) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Começamos por A2 que receberá o valor 91. Já B2, será preenchida com 29. Esses valores foram determinados no Exemplo 2.1.9.

4) Vamos construir uma tabela para melhor visualização do processo. Como iremos descriptografar uma mensagem, realizaremos o caminho inverso da codificação. Começando pela inserção do dicionário de cifras na coluna A.

   Nesse sentido, a célula A4 será rotulada com o texto "**CIFRA**". Da célula A5 em diante, colocaremos a sequência de cifras, que inicia no número 10 e termina em 35. A automatização desse procedimento pode ser realizada da seguinte maneira: digite os dois primeiros números da sequência e use a função arrastar o cursor para baixo.

5) Criaremos o dicionário de caracteres com 26 letras, posicionadas na sua ordem alfabética. Dessa forma, a célula B4 será rotulada por "**TEXTO ORIGINAL**" e em B5 digitaremos a fórmula:

   $$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

6) A célula C4 receberá a inscrição "**MENSAGEM CRIPTOGRAFADA (C)**". Nas células de baixo, digitaremos a mensagem codificada, lembrando de inserir um código em cada célula.

7) Na coluna D, rotularemos D4 com o texto "$C = B \,\hat{}\, d \,(mod\, n)$". Na célula D5, devemos inserir a fórmula:

   $$=\text{MOD(C5 ⌃ B\$2;A\$2).}$$

   Essa fórmula devolve o resto da divisão por "n" (na célula A2) de cada cifra, da coluna C elevado ao valor de "d" (presente na célula B2). Após isso, basta usar a função autocompletar, arrastanto o cursor da célula selecionada para baixo.

   Ao executarmos os passos acima, esperávamos encontrar como resultados, nas células da coluna D, números inteiros. No entanto, o editor de planilhas devolveu, nessas células, a indicação de erros com a descrição **#NUM!**. Isso ocorreu devido à limitação do Google Planilhas ao trabalhar com números grandes.

	A	B	C	D	E	F	G	H
1	n	d						
2	91	29						
3								
4	CIFRA	MSG ORIGINAL	MSG CODIFICADA (C)	RESTO DE (C elev 29) : 91				
5	10	A	32	#NUM!				
6	11	B	8	#NUM!				
7	12	C	33	#NUM!				
8	13	D	29	#NUM!				
9	14	E	82	#NUM!				
10	15	F	33	#NUM!				
11	16	G	88	#NUM!				
12	17	H	22	#NUM!				
13	18	I	33	#NUM!				
14	19	J	22	#NUM!				
15	20	K	82	#NUM!				
16	21	L	32	#NUM!				
17	22	M	1	1				
18	23	N						
19	24	O						
20	25	P						
21	26	Q						
22	27	R						
23	28	S						
24	29	T						
25	30	U						
26	31	V						
27	32	W						
28	33	X						
29	34	Y						
30	35	Z						

Erro

Os parâmetros em MOD causaram um erro de valor fora do intervalo. O erro ocorre quando o seguinte é verdadeiro: (o divisor * 1125900000000) é menor ou igual ao dividendo.

Figura 2.9: RSA com chave privada (91,29). Autoria própria

8) Utilizaremos o programa **Wolfram alpha** para fazer esses cálculos. Ele pode ser acessado no site: https://www.wolframalpha.com. Esse programa possui um amplo conjunto de funcionalidades matemáticas envolvendo números e menor limitação que o Google Planilhas ao trabalhar com números grandes. Sendo assim, mostra-se como uma ferramenta apta para trabalhos acadêmicos e também para uso profissional. Apresenta características que viabilizam seu uso, dentre elas destacamos: sua interface intuitiva e de fácil utilização, além de ser muito rápido no processamento dos cálculos e apresentação das respostas.

9) O programa possui uma caixa de entrada para os cálculos que desejamos realizar. Como exemplo, apresentaremos o cálculo de decifragem da primeira cifra. Os demais cálculos devem ser feito de maneira análoga. Nesse sentido, basta digitarmos, na caixa de entrada do site, a seguinte expressão:

$$32 \hat{} \ 29 \ (\text{mod } 91).$$

Dentro de poucos instantes, a ferramenta nos apresenta na caixa "*Result*" o valor 2. Assim, o primeiro bloco foi encontrado.

Importante apontar que o Wolfram Alpha disponibiliza para seus usuários duas versões. Uma delas é paga, apresentando funcionalidades adicionais, com

explicações acerca das resoluções. De forma mais limitada, porém efeciente, temos a versão gratuita. Foi por meio dela que este trabalho foi elaborado.

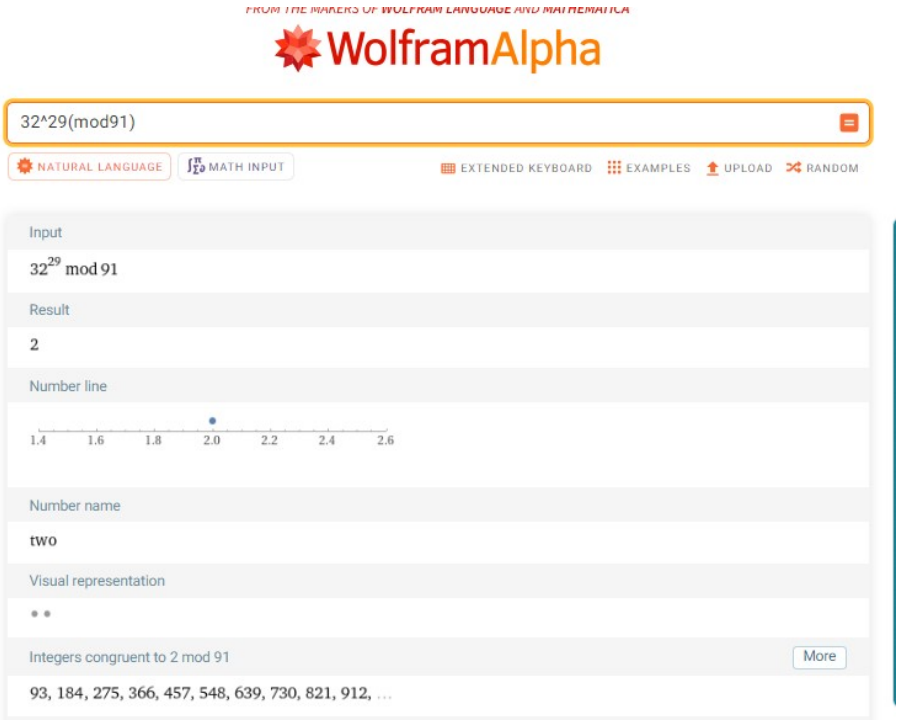


Figura 2.10: Interface do Wolfram Alpha

Os valores calculados através do Wolfram Alpha são:

2 8 24 22 10 24 30 29 24 29 10 2 1

10) À medida que vamos realizando os cálculos no Wolfram Alpha, devemos inserir esses resultados na nossa planilha. Apesar de sua limitação, com a resolução dos cálculos de congruências, o Google Planilhas ainda tem um papel importante na finalização desse trabalho. Nesse sentido, rotulamos a célula E4 com o texto: **BLOCOS B (< pxq) WOLFRAM**. Logo após, inserimos, nessa coluna, os dados obitos no programa. Iniciamos a lista pela célula E5.

11) No item anterior, os números encontrados representam os blocos relativos às cifras pré-codificadas. Sendo assim, necessitamos encontrar as cifras, nas quais a mensagem foi pré-codificada. Para isso, rotulamos a célula F5 com **CIFRA DIGITAL**. Em seguida, juntamos os números da coluna E, menores do que 10, por justaposição, sem exceder o número 35. Temos que digitar todos esses números na coluna F, começando pela célula F5.

12) Para recuperarmos a mensagem original, usaremos a funcionalidade do editor de planilhas. Iniciamos rotulando a célula G4 com: **MENSAGEM ORIGINAL**. Feito isso, na célula G5, inserimos a fórmula:

$$=\text{PROCV}(\text{F5};\text{A5} : B30;2;0).$$

A mensagem **SOMA OU TOTAL** foi recuperada.

A planilha pode ser acessada na página "Atividade 10" em https://l1nk.dev/mEcsY.

2.1.6 RSA (Assinado) no Google Planilhas e Wolfram Alpha

Exemplo 2.1.11: Atividade 11

Criptografar a mensagem "UM BOM ALUNO", em que o remetente utiliza as chaves pública e privada iguais a (187,7) e (187,23), respectivamente. Já o destinatário possui as chave pública e privada iguais a (299,5) e (299,53), respectivamente. Admitamos que o alfabeto de cifras usado na comunicação esteja pré-codificado com números naturais de 10 a 35.

Para a assinar a mensagem, será utilizado o caso 1, apresentado por Shokranian ([3],p.54-56). Nesse sentido, o parâmetro n' (do remetente) é menor do que o parâmetro n (do destinatário). Importante salientar que: **nenhuma das partes envolvidas na troca da mensagem conhece a chave privada da outra**.

1) Abra o Google Planilhas.

2) Defina o remetente e o destinatário da mensagem. Logo após, vamos inserir os parâmetros das chaves dos envolvidos na troca de mensagem. Começaremos pelo destinatário. Na célula A1, insira o texto "**p**". A célula B1 deve ser renomeada por "**q**". Já C1 deve ser rotulada com "**n=p.q**" e D1 deve receber o texto "**e**".

   Nas células E1, F1 e G1, insira os respectivos textos:

   "**(p-1)(q-1)**", "**mdc(e,(p-1)(q-1)** " e "**d**".

3) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada na linha 1. Comece pela célula A2 que recebe o valor 23. B2 recebe o valor 13. Em C2, insira a fórmula "**=A2 * B2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p e q. Em seguida, insira em D2 o valor 5, como indicado na chave pública.

4) Agora, vamos programar a célula E2. Para isso, inserimos a fórmula:

   "**=(A2 - 1)*(B2 - 1)**".

   F2 receberá a fórmula "**=MDC(D2;E2)**", e G2 será preenchida com o número 53 que representa o valor de "**d**", parâmetro da chave privada $(n,d) = (299,53)$.

5) O cálculo do valor de "**d**" geralmente é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir. "**d**" é um número inteiro definido pelas duas condições:

$$ed \equiv 1(\ (\text{mod}\ (p-1)(q-1)) \text{ e } 1 \leq d < (p-1)(q-1).$$

Dessa forma, as condições podem ser reescritas como:

$$5d \equiv 1\ (\text{mod}\ 264) \text{ e } 1 \leq d < 264.$$

Nesse sentido, resolver a congruência equivale solucionar a equação:

$$5d = 264x + 1, \text{ em que } x \text{ é inteiro.}$$

Daí

$$d = \frac{264x+1}{5} = \frac{4x+1}{5} + 52x.$$

O interessante é encontrar um valor para x, de modo que a primeira parcela da equação acima represente um número inteiro. Ao testar a expressão $4x + 1$, para $x \in \{0, 1, 2, 3, 4\}$, verifica-se que $4x + 1$ é divisível por 5 quando $x = 1$ (apenas ele). Temos:

$$d = \frac{4.1+1}{5} + 52.1 = 53.$$

Devemos observar que esse número satisfaz a condição

$$1 \leq d < 264.$$

Agora devemos inserir os dados do remetente, cujas chaves pública e privada são (187,7) e (187,23), respectivamente.

Na célula H1, insira o texto "**p'**" e em I1 a inscrição: "**q'**". A célula J1 será rotulada com "**e'**", enquanto K1 receberá "**n'=p'.q'**".

Nas células L1, M1 e N1, insira os respectivos textos:

"**(p'-1)(q'-1)**", "**mdc(e',(p'-1)(q'-1)** " e "**d'**".

6) Na linha 2, vamos inserir os valores equivalentes a cada célula rotulada anteriormente. Começamos por H2 que recebe o valor 17. I2 será preenchida com 11. Em J2, entramos com o valor 7. K2 receberá a fórmula "**=H2*I2**". Dessa forma, estamos programando essa célula que será modificada, automaticamente, caso modifiquemos os números p' e q'.

7) Agora programaremos a célula L2 com a fórmula "**=(H2-1)*(I2-1)**". M2 receberá a fórmula "**=MDC(J2;L2)**", e N2 será preenchida com o número 53, que representa o valor de "**d'**", parâmetro da chave privada.

8) O cálculo do valor de d', geralmente, é realizado por meio de resolução de equações diofantinas. No entanto, esse cálculo pode ser adaptado para o ensino médio, como veremos a seguir. d' é um número inteiro definido pelas duas condições,

$$e'd' \equiv 1(\ (\text{mod}\ (p'-1)(q'-1)) \text{ e } 1 \leq d' < (p'-1)(q'-1).$$

Dessa forma, as condições podem ser reescritas como,

$$7d' \equiv 1\ (\text{mod}\ 160) \text{ e } 1 \leq d' < 160.$$

Nesse sentido, resolver a primeira condição equivale solucionar a equação:

$$7d' = 160x' + 1, \text{ em que } x' \text{ é inteiro.}$$

Segue que

$$d' = \frac{160x+1}{7} = \frac{6x+1}{7} + 22x.$$

A meta é encontrar um valor para x', de modo que a primeira parcela da equação acima represente um número inteiro. Ao testar a expressão $6x'+1$, para $x' \in \{0,1,2,3,4,5,6\}$, verifica-se que $6x'+1$ é divisível por 7 quando $x'=1$ (apenas ele). Temos:

$$d' = \frac{6.1+1}{7} + 22.1 = 23.$$

Devemos observar que esse número atende à condição

$$1 \leq d' < 160.$$

9) Voltando para a planilha, vamos estabelecer o dicionário de caracteres com 26 letras (na ordem alfabética) que serão substituídas por números inteiros de 10 até 35. Sendo assim, na célula A4, inserimos "**TEXTO ORIGINAL**" e em A5 digitamos a fórmula

$$=\text{ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).}$$

10) Na coluna B, adicione o dicionário de cifras, iniciando no número 10 e terminando em 35. Basta digitar os dois primeiros números da sequência e usar a função arrastar o cursor para baixo. Com isso, a célula B4 será rotulada com o texto "**CIFRA**" e da célula B5 em diante, colocaremos a sequência de números.

11) Na célula C4, insira o rótulo "**MENSAGEM ORIGINAL**". Nas células abaixo, vamos digitar a mensagem original, lembrando de inserir uma letra em cada célula.

12) Na coluna D, vamos "buscar" cada correspondente das letras no dicionário de cifras (estamos usando a cifra de substituição). Estamos pré-codificando a mensagem original, o rótulo de D4 será "**PRÉ-CODIFICAÇÃO**" e em D5 inserimos a fórmula:

$$=\text{PROCV(C5; } A\$5 :\text{B\$41; 2; 0).}$$

Em seguida, devemos completar a coluna com a função arrastar o cursor para baixo.

13) A coluna E será destinada para a inserção dos "Blocos". São eles que serão codificados e seguem três exigências de formação, como observamos em Hefez ([2],p.218-219) e Shokranian ([3],p.46-48). Os blocos são números formados a partir da mensagem pré-codificada e para formá-los, devemos primeiramente, visualizar a mensagem pré-codificada como um único número. Assim, visualizaremos um número com muitos algarismos. Logo após, devemos "quebrar" os algarismos, desse número, em numerais menores B_1,B_2...B_r, com $1, 2, ..., r$ números naturais, de modo que cada numeral atenda às condições:

(a) $B_r < n'$;

(b) B_r deve ser coprimo tanto com n' quanto com n;

(c) Nenhum bloco pode inciar com o algarismo zero.

Dessa maneira, vamos rotular a coluna E, inserindo na célula E5 o texto "**BLOCOS B (< n')**", em seguida, apenas copiaremos os pré-códigos da coluna D para serem colados na célula E5. Precisaremos avaliar essa coluna, no entanto, faremos isso com auxilio do editor de planilhas. Nesse sentido, passamos ao passo seguinte para facilitar a avaliação.

14) Na coluna F, vamos verificar quais blocos são coprimos com n. A célula F4 terá a inscrição: "**mdc(B,n)=1**". Na célula F5, inserimos a fórmula:

$$=\text{MDC(E5;C\$2).}$$

Em seguida, usamos a função autocompletar.

15) Repetimos o passo anterior com algumas adaptações. A primeira é rotular a coluna G, inserindo em G4 o texto "**mdc(B,n')=1**". Em seguida, na célula G5, inserimos a fórmula:

$$=\text{MDC(E5;K\$2).}$$

16) Nesse passo, analisaremos simultaneamente as colunas F e G para que atendam às três condições do item 13). Começaremos pela segunda condição, verificando todos os valores dessas colunas que são iguais a 1. Se isso ocorrer, passamos para a próxima análise. Caso contrário, voltamos à coluna dos blocos (Coluna E) e modificamos os valores que não atendem às condições das colunas F e G. A modificação de um bloco será realizada por meio da separação de seus algarismos, criando dois novos blocos que serão vizinhos na coluna. De mesma forma, dois blocos vizinhos podem ser unidos formando um único bloco. No entanto, o valor do bloco deve ser menor do que n', isso satisfaz a primeira condição. Para finalizar, devemos observar que um bloco não pode ter o algarismo inicial igual a zero, como estabelece a terceira condição.

    Esse procedimento é realizado por meio de tentativa e erro. Como já progamamos as colunas F e G para apresentarem os resultados que nos interessam, cada modificação feita na colunas de blocos reflete nas colunas F e G.

    Nesse exemplo, copiamos os pré-códigos:

    $$30\ 22\ 46\ 11\ 24\ 22\ 46\ 10\ 21\ 30\ 23\ 24,$$

    para a coluna de blocos (coluna E). Imediatamente, algumas células das colunas F e G apresentaram valores diferentes de 1. Assim, os blocos dessas linhas devem ser modificados.

17) Neste momento, vamos mostrar a assinatura da mensagem, em que o remetente usa a sua chave privada para tal procedimento. Rotulamos a coluna H, inserindo em H4 a inscrição "**C = B ^d' (mod n')**". Na célula H5, devemos inserir a fórmula:

    $$=\text{MOD(E5 ^M\$2;K\$2)}.$$

    Essa fórmula devolve o resto da divisão por "n'" (na célula K2) de cada bloco, da coluna E, elevado (símbolo circunflexo) ao valor de "d'" (presente na célula N2). Após isso, basta usar a função autocompletar, arrastanto o cursor da célula selecionada para baixo.

    Ao executarmos os passos acima, esperávamos encontrar como resultados, nas células da coluna H, números inteiros. No entanto, o editor de planilhas devolveu, na maioria das dessas células, a indicação de erros com a descrição **#NUM!**. Isso ocorreu devido à limitação do Google Planilhas ao trabalhar com números grandes.

18) Utilizaremos o programa **Wolfram alpha** para fazer esses cálculos.

19) Basta digitarmos, na caixa de entrada do site, a seguinte expressão:

    $$30\ \hat{}\ 23 \bmod 187.$$

Dentro de poucos instantes, a ferramenta nos apresenta na caixa "*Result*" o valor 72. Assim, o primeiro bloco foi encontrado. Os valores calculados através do Wolfram Alpha são:

72 162 63 73 177 168 63 150 175 98 72 162 76 64.

20) Vamos inserir esses resultados na nossa planilha, a partir de I5 e rotulamos a célula I4 com o texto: "**C WOLFRAM**".

21) Até esse momento, a mensagem já foi assinada e agora só resta ao remetente criptografar. Para isso, ele usará a chave pública do destinatário. Sendo assim, criamos a coluna de códigos "T". Na célula J4, digitamos o texto "**T = C ^ e (mod n)**". Na célula J5, inserimos a fórmula:

=MOD(I5 ^ D$2;C$2).

Para finalizar, basta usar a função autocompletar do editor de planilhas. Logo a mensagem criptografada será:

128 93 228 242 190 155 228 271 15 232 128 93 293 233.

Em resumo, o remetente usou o parâmetro de sua chave privada para assinar e a chave pública do destinatário para codificar. De maneira análoga, o destinatário usará a sua chave privada para decodificar, inicialmente a mensagem, logo após, usa a chave pública do remetente para ter acesso à mensagem original.

Acesso da planilha na página "Atividade 11" em https://l1nk.dev/mEcsY.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	p	q	n = p x q	e	(p -1)(q-1)	mdc(e, (p -1)(q-1))	d	p'	q'	e'	n' = p' x q'	(p'-1)(q'-1)	mdc(e', (p'-1)(q'-1))	d'
2	23	13	299	5	264	1	53	17	11	7	187	160	1	23
3														
4	TEXTO ORIGINAL	CIFRA	MENSAGEM ORIGINAL	PRÉ-CODIFICAÇÃO	BLOCOS B (< n')	mdc(B, n)=1	mdc(B,n')=1	C=B ^d' (mod n')	C (Wolfram)	T=C ^e (mod n)				
5	A	10	U	30	30	1	1	#NUM!	72	128				
6	B	11	M	22	2	1	1	162	162	93				
7	C	12	_	46	24	1	1	#NUM!	63	228				
8	D	13	B	11	61	1	1	#NUM!	73	242				
9	E	14	O	24	12	1	1	#NUM!	177	190				
10	F	15	M	22	42	1	1	#NUM!	168	155				
11	G	16	_	46	24	1	1	#NUM!	63	228				
12	H	17	A	10	6	1	1	#NUM!	150	271				
13	I	18	L	21	10	1	1	#NUM!	175	15				
14	J	19	U	30	21	1	1	#NUM!	98	232				
15	K	20	N	23	30	1	1	#NUM!	72	128				
16	L	21	O	24	2	1	1	162	162	93				
17	M	22			32	1	1	#NUM!	76	293				
18	N	23			4	1	1	64	64	233				
19	O	24												
20	P	25												
21	Q	26												
22	R	27												
23	S	28												
24	T	29												
25	U	30												
26	V	31												
27	W	32												
28	X	33												

Figura 2.11: Cifra RSA com assinatura (autoria própria)

3

Aplicações de tecnologias em aulas de matemática

Para acessar as planilhas com as aulas propostas clique em:

https://l1nk.dev/4pQI1.

3.0.1 Aula 1

1) **Tema**: Cálculo do MMC e MDC.

2) **Problematização**: No primeiro momento, encontre o MMC dos seguintes números:

   (a) 11, 14, 21 e 36.

   (b) 11, 14, 25 e 27.

   (c) 11, 22, 44 e 88.

   Logo após, encontre todos os números menores do que 36 que são coprimos com 36.

3) **Público Alvo**: Turmas dos Anos finais do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

   - Multiplicação e divisão de números naturais.

5) **Objetivo**: Trabalhar conceitos básicos acerca dos números inteiros (múltiplos e divisores, divisão euclidiana, definição de números primos). Esse roteiro foi construído pela compilação das ideias apresentadas nos Exemplos 2.1.1 e 2.1.2.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- O professor deve explicar a dinâmica da aula, orientando que a aula terá dois momentos. No primeiro, será explorado conteúdos relacionados ao cálculo de MMC. No segundo momento, será investigado uma aplicação para o MDC.
- Definir o conceito de múltiplo e divisor de um número natural.
- Apresentar o conceito de mínimo múltiplo comum e máximo divisor comum.
- Definir número primo e mostrar a importância desses números e suas várias aplicações como visto ao longo deste trabalho. Além disso, definir os números coprimos.
- Apresentar o Google Planilhas, mostrar sua localização, interface e funcionalidades.
- Orientar na construção de uma tabela, como fizemos no Exemplo 2.1.1. O professor preenche sua tabela com os 4 números, aplica a fórmula de cálculo do mmc deles. Paralelamente, em outra célula, entrar com fórmula para o produto desses números.
- Analisar os resultados da tabela. Explorar propriedades do cálculo do MMC.
- Iniciar o segundo momento. Agora devemos encontrar números inteiros positivos menores do que 36 que são coprimos com o próprio 36. Ver referência no Exemplo 2.1.2.
- Analisar os resultados da tabela. Explorar propriedades do cálculo do MDC.
- Investigar a percepção de que a lista de resultados fornece também todos os divisores do número 36. Lembramos que para isso, basta observar que o MDC, apresetando na segunda coluna, deve ser igual ao número da primeira coluna. Deve ser observado que, o número 1 e o próprio 36 não aparecerão nessa lista, ainda assim, eles são, respectivamente, o menor e o maior divisor de 36. Com isso, é possível determinar a quantidade de divisores desse número.
- Sugerir que os alunos testem outros números e analisem os cálculos quando os números envolvidos são coprimos e no caso em que não são coprimos.
- Para além, investigar a relação da tabela com a escrita do número 36 como o produto de seus fatores primos. Essa relação fica mais evidente com decomposição, em fatores primos, dos dois divisores de 36 cuja a diferença entre eles seja a menor possível.

9) **Conclusão**:

- Pedir para que os alunos produzam uma análise de resultados. Nessa análise, é importante que seja apresentada explicação acerca do algoritmo utilizado e análise do uso da tecnologia, comparando-a com o trabalho manual.
- Solicitar "feedback" da aula, com apontamentos de pontos positivos e negativos.

3.0.2 Aula 2

1) **Tema**: Números primos.

2) **Problematização**: Teste primalidade dos números 1129 e 1141. Caso encontre um número composto, determine seus divisores.

3) **Público Alvo**: Turmas dos Anos Finais do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

   - Multiplicação e divisão de números naturais.

5) **Objetivos**: Trabalhar conceitos básicos acerca dos números inteiros (múltiplos e divisores, definição de números primos). O objetivo principal é testar a primalidade de números inteiros com a utilização de método da divisão.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Trinta minutos.

8) **Desenvolvimento**:

   - Definir o conceito de número primo. Explicar a necessidade de encontrar, no mínimo, um divisor do número que seja diferente dele mesmo e do número 1.
   - Explicar o método da divisão utilizado no teste de primalidade, destacando a importância da operação de radiciação para eficiência do método.
   - Apresentação do Google Planilhas. Mostrar funcionalidades do editor que poupam o trabalho manual.
   - Orientar na construção de uma tabela, como fizemos no Exemplo 2.1.3.
   - Analisar os resultados da tabela e concluir de acordo com os números obtidos com as divisões.
   - Sugerir que os alunos testem outros números (observar o aumento de dados da tabela à medida que o número a ser analisado fica maior).

9) **Conclusão**:

- Solicitar aos alunos a análise do processo, por meio de explicação do algoritmo e opinião acerca do uso da tecnologia, comparando-a com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

3.0.3 Aula 3

1) **Tema**: Criptografia pelo método da Substituição.

2) **Problematização**: Criptografar e descriptografar a mensagem "TUDO É NÚMERO", utilizando a Cifra de César com chave "D".

3) **Público Alvo**: Turmas dos Anos finais do Ensino Fundamental e Ensino Médio.

4) **Objetivos**: Trabalhar a relação biunívoca e o contexto histórico da Cifra de César. Interpretação de tabelas. Noções de programação.

5) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

6) **Duração**: Cinquenta minutos.

7) **Desenvolvimento**:

   - Apresentação da Cifra de César, mostrando contexto histórico.
   - Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Nesse sentido, oriente na criação de uma coluna com o alfabeto e outra com as cifras. Ver Exemplo 2.1.5 fazendo adaptações das fórmulas, quando necessário.
   - Crie uma coluna para ser a entrada da mensagem original.
   - Determine a coluna, na qual aparecerá a mensagem criptografada, inserindo a função "PROCV" como feito no Exemplo 2.1.5
   - Analisar, mesmo que superficialmente, o resultado da codificação.
   - Inicar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.
   - Criar uma tabela com quatro colunas, como feito no Exemplo 2.1.6. Inicie inserindo o dicionário de cifras (adaptar fórmula) na primeira coluna. Na segunda coluna, deve ser preenchida com o texto original (alfabeto original).
   - Crie a coluna para ser a entrada da mensagem codificada, inserindo cada cifra em uma única célula.
   - Determine a coluna na qual aparecerá a mensagem criptografada, inserindo a função "PROCV" como feito no Exemplo 2.1.6

- Verificar se a mensagem decodificada confere com a mensagem do primeiro momento.

8) **Conclusão**:

- Solicitar aos alunos a análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

3.0.4 Aula 4

1) **Tema**: Criptografia por Cifra Afim.

2) **Problematização**: Criptografar e descriptografar a mensagem "ESTUDAR VALE A PENA", utilizando a Cifra Afim com chave $f(x) = 2x + 6$.

3) **Público Alvo**: Nono Ano do Ensino Fundamental e Ensino Médio.

4) **Pré-requisitos**:

- Multiplicação e divisão de números naturais.
- Noção de resolução de uma equação polinomial do primeiro grau com uma variável.
- Noções do estudo de função polinomial do primeiro grau.

5) **Objetivos**: Trabalhar com o estudo de funções polinomiais do primeiro grau. Criptografia por substituição. Noções de programação de planilhas eletrônicas. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- Breve revisão do conteúdo de função polinomial do primeiro grau, com maior ênfase no cálculo da imangem de um elemento da função com a determinação da sua função inversa. Contextualização com funções do 1º grau.
- Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Nesse sentido, oriente na criação de uma coluna com o alfabeto e outra com a sequência de números inteiros. Ver Exemplo 2.1.7, fazendo adaptações das fórmulas, quando necessário.

- Crie na coluna A uma lista para o texto original (alfabeto original), usando a fórmula de inserir alfabeto.
- Na coluna B, insira o dicionário de caracteres, ou seja, as cifras. Lista de números de 10 a 35.
- Na coluna C, digite a mensagem original, com cada letra em uma célula.
- Na coluna D, busque cada correspondente das letras no dicionário de Cifras (estamos usando a cifra de substituição). Use a função "PROCV". Terminado esse procedimento, a mensagem estará pré-codificada.
- A coluna E será destinada para encontrar os valores das imagens dos pré-codigos aplicados à função. É nessa coluna que está o resultado de todo processo.
- Iniciar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.
- Determinar a função inversa, manualmente.
- Criar uma tabela com quatro colunas, como feito no Exemplo 2.1.8. Inicie inserindo o dicionário de cifras na primeira coluna. Na segunda coluna, deve ser preenchida com o texto original (alfabeto original).
- A terceira coluna será a entrada da mensagem codificada, inserindo cada cifra em uma única célula.
- Na quarta coluna, devemos aplicar o valor de cada código da coluna anterior na inversa da função. Assim, chegamos até a mensagem pré-codificada.
- Na última coluna, inserimos a função "PROCV" como feito no Exemplo 2.1.8 chegando ao texto original.
- Verificar se a mensagem decodificada confere com a mensagem do primeiro momento.
- Solicitar que os alunos façam testes, trocando a mensagem original e verifiquem a codificação e pré-codificação.

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos

10) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

3.0.5 Aula 5

1) **Tema**: Criptografia RSA.

2) **Problematização**: Criptografar e descriptografar a mensagem

"PROFMAT_2024",

utilizando o RSA com chave pública (187,7) e chave privada (187,23).

3) **Público Alvo**: Alunos do Ensino Médio.

4) **Pré-requisitos**:

- Multiplicação e divisão no conjunto dos números inteiros.
- Noção de resolução de uma equação polinomial do primeiro grau com duas variáveis.

5) **Objetivos**: Trabalhar com criptografia RSA. Noções de programação de planilhas eletrônicas. Segurança da informação. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cem minutos.

8) **Desenvolvimento**:

- Na primeira parte da aula, o trabalho é voltado para a codificação da mensagem. Comece com a apresentação do Google Planilhas. Enfatize as funcionalidades do editor que poupam o trabalho manual. Inicie inserindo os parâmetros das chaves. Nesse sentido, rotule as células da primeira linha (A1,...,G1) com os respectivos rótulos p, q, $p.q$, e, $(p-1)(q-1)$, $mdc(e,(p-1)(q-1))$ e d. Na linha 2, vamos inserir os respectivos valores das células rotuladas, são eles: 11, 17, 187, 7, 160, 1 e 23. Nessa segunda linha, pode ser feita a programação dos cálculos nas células C2 (=A2*B2), E2 (=(A2-1)*(B2-1)) e F2 (=MDC(D2;E2)). Ver Exemplo 2.1.9.
- Crie na coluna A uma lista para o texto original, usando a fórmula de inserir alfabeto, ver Exemplo 2.1.9. Nessa mesma coluna, logo após o alfabeto, insira os algarismos de 0 até 9. Na célula abaixo do algarismo 9, entre com o símbolo _ (underline). Ele representará o espaço entre as palavras na mensagem original.
- Na coluna B, insira o dicionário de caracteres, ou seja, as cifras. Lista de números de 10 a 46.
- Na coluna C, digite a mensagem original, com cada letra em uma célula. Lembre-se que o espaço deve ser preenchido pelo símbolo *underline*.

- Na coluna D, busque cada correspondente das letras no dicionário de Cifras (estamos usando a cifra de substituição). Use a função "PROCV", inserindo em D5 a fórmula:

  $$=\text{PROCV(C5; A5} : B41; 2; 0).$$

  Terminado esse procedimento, a mensagem estará pré-codificada.

- A coluna E será destinada para encontrar os blocos dos pré-codigos. São eles que serão codificados no final do processo.

- A célula F4 será rotulada com "B $\not\equiv 0 \pmod{p}$". Na célula abaixo, insira a fórmula:

  $$=\text{MOD(E5;A\$2)}$$

  e use a funcionalidade autocompletar.

- Faça o procedimento análago ao item anterior. As modificações são que a célula G4 recebe "B $\not\equiv 0 \pmod{q}$" e em G5 insira:

  $$=\text{MOD(E5;B\$2).}$$

  Use a funcionalidade autocompletar.

- Na coluna H, vamos encontrar o resultado do procedimento. A célula H4 será rotulada com

  "C=B $\widehat{}$ e (mod pq)".

  O símbolo circunflexo ($\widehat{}$) realiza a exponencial. Na célula H5 insira a fórmula:

  $$=\text{MOD(E5} \widehat{} \text{ D2;}C2).$$

  Logo após use a função autocompletar, nas células dessa coluna, aparecerá as cifras codificadas:

  $$185\ 124\ 29\ 93\ 128\ 128\ 175\ 160\ 7\ 47\ 9\ 47\ 116.$$

- Iniciar o segundo momento da aula, ou seja, o processo de decodificação da mensagem.

- Rotule a célula J4 com "CIFRA". Na célula abaixo, insira o dicionário de cifras. Copie da coluna B.

- Rotule a célula K4 com "TEXTO ORIGINAL", na célula abaixo insira o alfabeto. Copie da coluna A.

- Na coluna L, vamos inserir a mensagem criptografada. Para isso, rotule L4 com o texto "MENSAGEM CRIPTOGRAFADA" e na célula abaixo, cole a mensagem obitida na coluna H. Cole somente os valores.

- Na coluna M, vamos fazer o processo inverso da codificação. Para isso, rotulamos a célula M4 com o texto "RESTO DE (C $\widehat{}$ 29) : 187". Na célula abaixo, digite a expressão responsável pela codificação;

$$=\text{MOD}(\text{L5} \hat{} \text{G\$2;C\$2}).$$

Use a função autocompletar.

O programa Google Planilhas não é capaz de realizar esses cálculos. Sendo assim, devemos usar o programa Wolfram Alpha para realizá-los.

- Abra o site no navegador de internet. Para isso, basta digitar ou clicar no endereço:

  https://www.wolframalpha.com.

- Na caixa de entrada da tela principal do site, digite o comando que necessitamos, ou seja,

  $$185 \hat{} \ 23 \ (\text{mod } 187).$$

  Na tela, um pouco mais abaixo, será possível visualizar o resultado, 25.

- Prossiga realizando o passo anterior para cada cifra da coluna L. Cada valor encontrado deve ser digitado na planilha, na coluna N, a partir da célula N5. Para melhor entendimente e estética, rotule a célula N4 com o texto "BLOCOS B ($< p.q$) WOLFRAM". A coluna será composta pelos números:

  $$25\ 27\ 24\ 15\ 2\ 2\ 10\ 29\ 46\ 38\ 36\ 38\ 40.$$

- Perceba que dois elementos não fazem parte do dicionário de cifras. Sendo assim, escrevemos essa sequência de números, tomando cuidado para que nenhum deles seja menor do que 10 e ou maior do que 46. As modificação devem ser feitas por união de números por justaposição.
- Na coluna O, vamos escrever as cifras que foram encontradas com os blocos da etapa anterior. Rotulamos a célula O4 com "CIFRA DIGITAL", e a partir de O5, encontraremos a sequência

  $$25\ 27\ 24\ 15\ 22\ 10\ 29\ 46\ 38\ 36\ 38\ 40.$$

- O processo final se dará pela substituição dessas cifras. Nesse sentido, rotule a célula P4 com o texto "MENSAGEM ORIGINAL" e, na célula P5, insira a fórmula:

  $$=\text{PROCV(O5;J\$5:K\$41;2;0)}.$$

  Ao usar a função autocompletar, deve aparecer a mensagem:

  $$\text{PROFMAT\_2024}.$$

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo, opinião acerca do uso da tecnologia em comparação com o trabalho manual.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

3.0.6 Aula 6

1) **Tema**: Criptografia RSA com assinatura.

2) **Problematização**: Descriptografar a mensagem

$$128\ 93\ 228\ 242\ 190\ 155\ 228\ 271\ 15\ 232\ 128\ 93\ 293\ 233,$$

utilizando o RSA com assinatura do remetente que possui a chave pública (187,7) e (187,23) como chave privada, e o destinatário da mensagem tem em mãos as chaves pública e privada, respectivamente, iguais a (299,5) e (299,53).

3) **Público Alvo**: Alunos do Ensino Médio.

4) **Pré-requisitos**:

- Possuir noção de criptografia RSA.

5) **Objetivos**: Trabalhar com criptografia RSA com assinatura de mensagem. Noções de programação de planilhas eletrônicas. Construção e interpretação de tabelas.

6) **Recursos didáticos**: Lousa, pincel, aparelho de Data Show (se possível), computador, ou *tablet* ou *smartphone* com acesso à internet.

7) **Duração**: Cinquenta minutos.

8) **Desenvolvimento**:

- Inicie inserindo os parâmetros das chaves. Nesse sentido, rotule as células A1 até E1, da primeira linha, com os respectivos rótulos $n = pq$, e, d, $n' = p'q'$ e e'. Na linha 2, vamos inserir os respectivos valores das células rotuladas, são eles: $n = 299$, $e = 5$, $d = 53$, $n' = 187$ e $e' = 7$.
- A célula A4 será rotulada com o texto "**CIFRA**". Da célula A5 em diante, colocaremos a sequência de cifras que inicia no número 10 e termina em 46. Para isso, digite os dois primeiros números da sequência e use a função arrastar o cursor para baixo.
- Criaremos o dicionário de caracteres com 26 letras, posicionadas na sua ordem alfabética. Dessa forma, na célula A4, será rotulada por "**TEXTO ORIGINAL**" e em A5 digitaremos a fórmula:

  =ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))).

  Na célula A31, inicie a sequência dos algarismos (de 0 até 9). Por fim, insira o símbolo "*underline*" na célula A41. Esse símbolo representará os espaços que podem haver entre as palavras na mensagem recebida.

- A célula C4 receberá a inscrição "**MENSAGEM CRIPTOGRAFADA**". Nas células de baixo, digitaremos a mensagem codificada, lembrando de inserir um código em cada célula.
- Na coluna D, rotularemos D4 com o texto "$C = B \hat{} d\,(mod\, n)$". Na célula D5, devemos inserir a fórmula:

  $$=\text{MOD(C5 ⌃ C\$2;A\$2)}.$$

  Na sequência, use a função autocompletar do editor de planilhas. O programa retornará o erro **#NUM!** na fórmula. Dessa forma, esses cálculos podem ser feitos pelo programa Wolfram Alpha, no endereço eletrônico:

  https://www.wolframalpha.com.

- Na coluna E, insira os resultados dos cálculos realizados pelo Wolfram Alpha. Na célula E4, rotule com a inscrição "**U (wolfram)**". Os dados serão inseridos da célula E5 em diante.

  Até esse momento, o destinatário fez a primeira parte da decodificação da mensagem. Ele usou a chave privada.

- Agora vamos verificar a assinatura do remetente. Sendo assim utilizaremos a fórmula:

  $$=\text{MOD(E5 ⌃ E\$2;D\$2)},$$

  que deve ser insirida em F5. Essa coluna receberá o rótulo de "**B=U ⌃ e' (mod n')**" em F4. Após a inserção da fórmula, use a função autocompletar do editor de planilhas. Essa coluna apresentará erros. Isso novamente ocorrerá devido à limitação desse programa. Use novamente o programa Wolfram Alpha para realizar os cálculos que não foram realizados até o momento.
- Na coluna G, insira em G4 a descrição "**B (Wolfram)**". Insira todos os cálculos da coluna anterior. Com essa coluna completa, o destinatário possui os blocos que foram codificados.
- Rotule a célula H4 com "**CIFRA**". Da célula H5 em diante, insira, manualmente, os blocos originais formados a partir da coluna anterior. Logo devemos ter números que variam de 10 até 46. Na ordem que aparecem e utilizando união por justaposição.
- Para finalizar, vamos procurar cada cifra encontrada na coluna anterior no nosso dicionáio de cifras. Iniciamos, rotulando a célula I4 com "**TEXTO ORIGINAL**". Em I5, insira a fórmula:

  $$=\text{PROCV(H5;A\$5:B\$41;2;0)}.$$

  Ao utilizar a função autocompletar, a mensagem irá sendo revelada.

UM_BOM_ALUNO.

9) **Conclusão**:

- Solicitar aos alunos uma análise do processo, apresentando explicação do algoritmo.
- Solicitar "feedback" da aula com indicação de pontos positivos e negativos.

4

Lista de Exercícios Propostos

4.0.1 Atividades propostas

Apresentaremos alguns exercícios contextualizados envolvendo o mdc e o mmc. Para facilitar o planejamento das aulas disponibilizamos planilhas com as resoluções dos exercícios. Para acessar clique em https://acesse.one/uZniz .

Exercício 4.0.1: Em uma empresa, os cinco gerentes de produção precisam definir o número de funcionários a serem contratados para iniciar a sua operação. Eles poderão distribuir o número total de os funcionários em setores iguais, todos com 608 funcionáios, ou todos com 416, ou todos com 247 funcionários, sem que haja sobra de funcionários. Desse modo, qual é o número mínimo de funcionários que essa empresa precisa ter para entrar em operação, incluindo os gerentes?

Solução:

Para resolver esse problema, devemos primeiramente encontrar o mmc dos números de funcionários que os setores podem conter. Para isso, vamos construir uma tabela no Google Planilhas.

- Mescle as células A1 e B2 e coloque o título da sua tabela.
- Na célula A2, inclua a descrição *FUNCIONÁRIOS*. Já em B2, inclua: *RESULTADO*
- Entre com os valores de funcionários que os setores podem ter nas células A3, A4 e A5.
- Na célula A7, introduza o texto: *mmc*.
- Na célula B7, insira uma das fórmulas:

$$=\text{MMC(A3;A4;A5) ou } =\text{MMC(A3:A5).}$$

O programa nos retorna como valor o número 7904. Com mais os cincos gerentes, concluímos que o total de funcionários é 7909. Esse passo pode ser automatizado, para isso, em qualquer célula vazia do editor, por exemplo em B8, insira:

=B6+5.

Nota: A construção e formatação de tabelas no Google Planilhas são habilidades que podem ser trabalhadas a critério do professor.

Exercício 4.0.2: Uma árvore de natal possui luzes que acendiam e imediatamente apagavam nas seguintes frequências: as luzes amarelas piscavam de 15 em 15 segundos. Já as vermelhas faziam o mesmo procedimento de 19 em 19 segundos. As luzes azuis piscavam de 21 e 21 segundos. Por último, as verdes piscavam de 27 em 27 segundos. Ao ligar a árvore, todas as luzes piscam juntas. Depois de quanto tempo elas tornarão a piscar todas ao mesmo tempo?

Solução:

Esse problema é resolvido, diretamente, pelo cálculo do mmc dos números 15, 19, 21 e 27, que representam o intervalo que cada lâmpada demora para piscar. Sendo assim, entramos com esses valores nas células da coluna A. No final dessa coluna, inserimos uma das fórmulas:

=MMC(A1:A4) ou =MMC(A1;A2;A3;A4).

O programa nos retorna como valor o número 17 955 segundos.

Exercício 4.0.3: Ilda está estudando o resultado com testes dos medicamentos A, B e C em cobaias. O medicamento A está sendo ministrado a 162 cobaias. Outro grupo formado por 270 cobaias é testado com o medicamento B. Por fim, um terceiro grupo com 306 animais recebem o medicamento C. Para uma análise, ela precisa que as cobaias sejam divididas em grupos com o mesmo número de indivíduos, sendo que o número de indivíduos por grupo seja o maior possível e que os grupos possuam somente cobaias que receberam o mesmo medicamento. Após essa separação, cada grupo é enviado para uma gaiola que deve ser identificada. Quantas gaiolas serão necessárias para acolher todos os novos grupos?

Solução:

Esse problema é resolvido pelo cálculo do mdc dos números 162, 270 e 306. Sendo assim, construíremos uma tabela com seis linhas e três colunas. Na primeira, vamos inserir cada medicamento (A, B e C). Na segunda coluna, será inserido os números de cobais que receberam cada um dos medicamentos (162, 270, 306). Na terceira, vamos encontrar o número de grupos após as divisões das cobaias. Todos os dados devem ser inseridos a partir da 3ª célula de cada coluna. Dessa forma, basta inserir na coluna B, de frente para o texto "mdc", a fórmula:

=MDC(B3:B5).

Na célula C3, vamos inserir a fórmula:

=B3/B$7.

Logo após, usamos a função autocompletar, arrastando o cursor, da célula selecionada, para baixo. O programa retornará, nessa coluna, as quantidades relativas de cada um dos grupos. Para finalizar, basta aplicar a função soma nos resultados encontrados. Na célula C8, insira a fórmula:

$$=\text{SOMA(C3:C7)}.$$

O número de gaiolas necessárias para acolher todos os grupos é 41.

Exercício 4.0.4: Uma máquina produz peças de ferragem de dois comprimentos diferentes, uma com 156 metros e outra com 180 metros. Para atender a uma obra na construção de uma ponte, essa empresa precisa partir essas ferragens em pedaços iguais, de maior tamanho possível, sem que haja desperdício nas peças que a máquina produz.

Nesse sentido, qual deve ser o tamanho de cada pedaço vendido pela empresa?

Solução:

Esse problema é resolvido pelo cálculo direto do mdc dos números 156 e 180. Sendo assim, construa uma tabela e inserira os dois números nas duas primeiras células da coluna B. Na terceira célula dessa coluna, insira a fórmula:

$$=\text{MDC(B3;B4)}.$$

O programa nos retornará 12 metros.

Exercício 4.0.5: Considere dois intervalos de números inteiros. O primeiro é formado pelos números de 1 a 100, o segundo de 101 a 200. Encontre a quantidade de números primos contidos em cada intervalo. Logo após, encontre a diferença das quantidades de números primos encontrados em cada intervalo.

Solução:

Sugererimos a construção de uma tabela no Google Planilhas. Na coluna A, vamos inserir o número 2 e todos os números ímpares menores do que 100. Siga os passos:

1. Na linha 1, vamos mesclar as três primeiras células dessa linha (A1, B2,C3) e inserir o título da tabela,

   “VERIFICAÇÃO DE PRIMALIDADE de 1 a 100”.

2. Na célula A2, insira o texto:

   “NÚMERO”.

3. Na célula A4, insira o número 2. Nas células A5 e A6, insira, respectivamente, 3 e 5. Logo após, selecione os dois números e arraste o curso para baixo até chegar ao número 99.

4. A célula B2 será destinada aos números que vamos testar. Observe que só precisamos testar números ímpares. Se o aluno conhecer todos os produtos da tábua de múltiplicação de 2 até 9 mais os critérios de divisibilidade por 3 e 5, o trabalho será reduzido significativamente. Além disso, podemos informar os 5 primeiros números primos (2, 3, 5, 7 e 11) que não precisarão ser testados. Começaremos testando o número 13 que deve ser digitado em B2.

5. Na célula B3, entre com o título:

   "Resto de B2 por A(N)".

6. Na célula B4, inicie a programação. Nessa célula, será calculado o resto da divisão do número inserido em B2 pelo número inserido em A4, que na fórmula acima é representado por A(N). Para isso, insira na célula a seguinte fórmula:

   =MOD(B$2;A4).

7. Agora use a função "arrastar", na célula B4 até o final da tabela.

8. Verifique se algum número da coluna B é igual a zero. Se apareçer apenas um número zero, o número é divisível somente por ele mesmo, logo é primo. Caso contrário, ele é não primo.

9. Agora é só testar os outros números, inserindo-os na célula B2 e analisando essa coluna.

10. Crie uma coluna, fora da tabela, na coluna E, por exemplo, para inserir os números primos encontrados.

    Nota: Para facilitar a análise do item anterior, podemos colocar um destaque em todos os números zeros que por ventura aprareçam nessa coluna. Para isso, use a formatação condicional:

    - Selecione as células B4 até B53.
    - Acesse na barra superior do menu, do Google Planilhas a função **Formatar**. Logo após, clique em **Formatação condicional**.
    - Verifique se o intervalo esta correto. Logo após, no subitem **Regras de formatação**, escolha a opção: "*O texto é exatamente*".
    - Na caixa de dialógo, logo abaixo, digite "0".
    - No subitem **Estilo de formatação**, escolha a cor vermelha, por exemplo, clicando no balde de tinta. Clique em **Concluído**. Pronto, todos os números zeros, no intervalo selecionado ficarão com o fundo da célula vermelho. Veja ilustração.

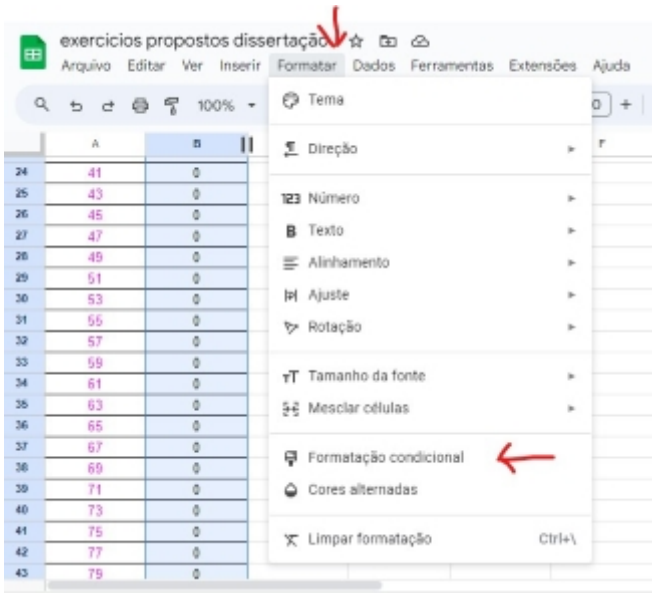


Figura 4.1: Formatação 1, Autoria própria

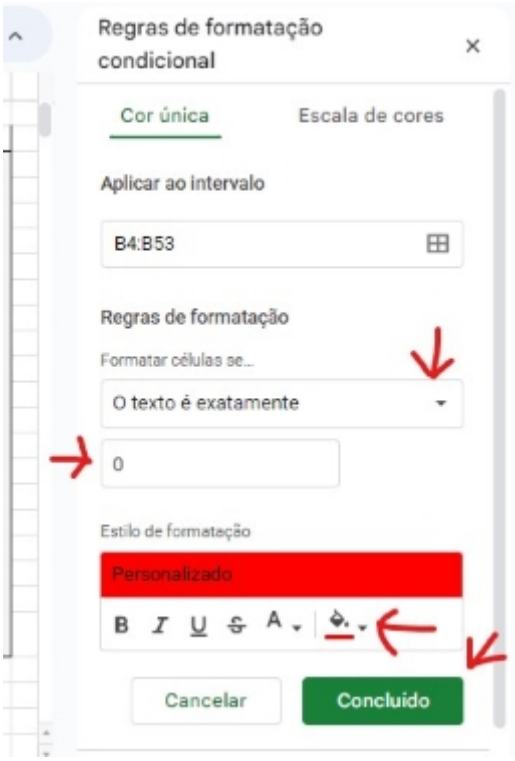


Figura 4.2: Formatação 2, Autoria própria

Para obter a quantidade de números que inserimos nas colunas dos números primos, contaremos com ajuda do programa. Para isso, selecione todos os números dessa coluna. Observe que, no canto direito da barra inferior da planilha, aparece a expressão "soma:" seguida de um número. Ao lado direito desse número, há uma seta preta, apontada para baixo. Ao clicar na seta, surgirá uma mini guia com várias opções, uma delas será a opção: "contagem", que nesse caso estará representado pela expressão: "contagem:25". Dessa forma,

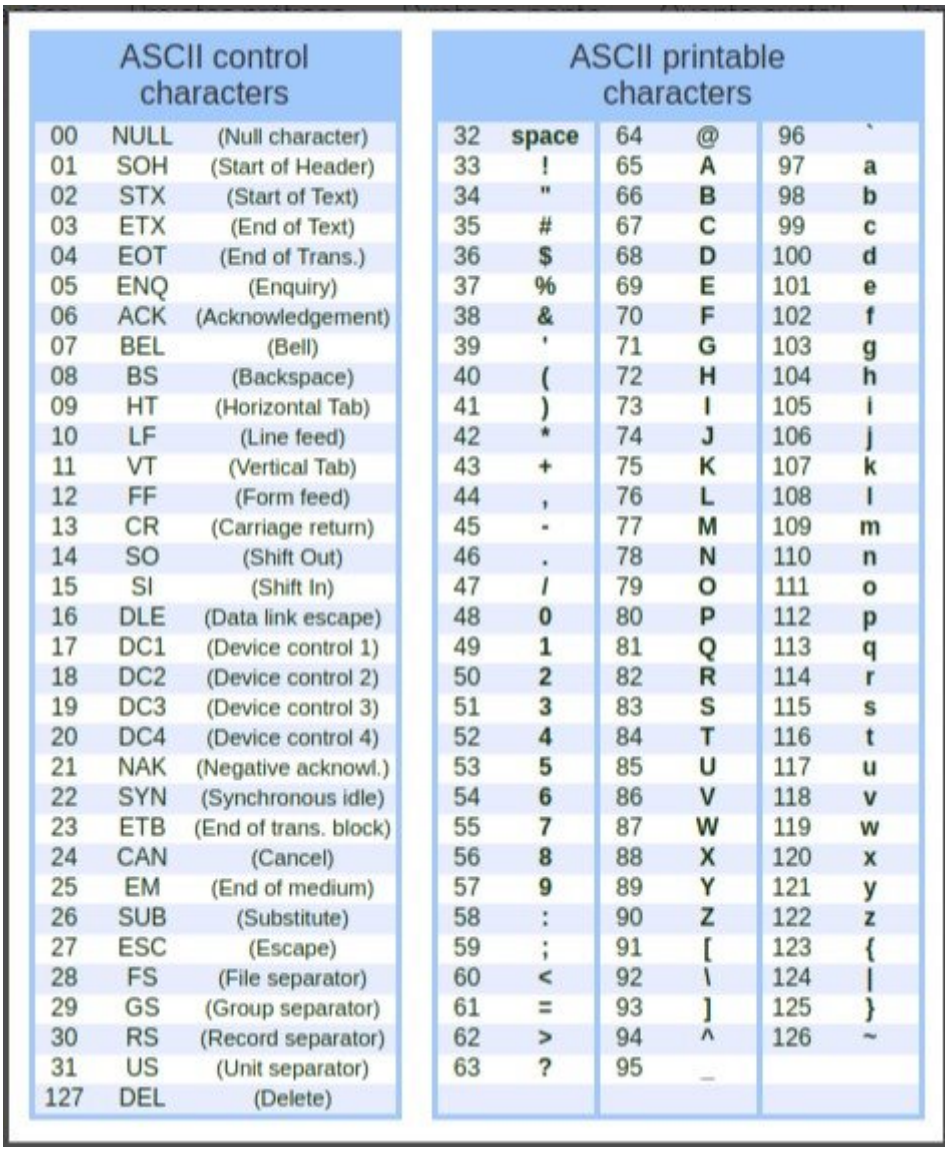
indicará 25 números inseridos na coluna selecionada. Segue ilustração.

Figura 4.3: Contagem, Autoria própria

Para concluir o exercício, repita o procedimento para os números de 101 a 200. Nesse passo, crie uma coluna de primos ao lado da coluna anterior (coluna F). Serão, 21 números primos neste intervalo. A diferença entre as quantidades será de 4 números.

5

Apêndice A



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Figura 5.1: Fonte: //www.treinaweb.com.br/blog/uma-introducao-a-ascii-e-unicode acesso 26/04/24.

Bibliografia

[1] Brasil. “Base Nacional Comum Curricular”. Ministério da Educação (20 de dez. de 2017). Portaria 1570. Estabelece as diretrizes e bases da educação nacional. URL: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf (acesso em 25 de jul. de 2023).

[2] Hefez, A. Aritmética. 3ª edição. Rio de Janeiro: SBM: Sociedade Brasileira de Matemática, 2022.

[3] Shokranian, S. Criptografia para Iniciantes. 2ª edição. Editora Ciência Moderna Ltda, 2012.