Criptografia no Ensino Básico

Alexandre Gonçalves Batista[1]
Luís Felipe Gonçalves Fonseca [2]
UFV, Florestal, MG

Resumo.Este trabalho aborda a criptografia com foco no ensino de matemática na educação básica. Apresentamos o processo de codificação RSA, utilizando as ferramentas Google Planilhas e Wolfram Alpha.

Palavras-chave. Aritmética; Criptografia; Planilhas eletrônicas; RSA; Wolfram Alpha.

1 Introdução

Desde a invenção da escrita, os historiadores têm documentado diferentes formas de comunicação secreta. Algumas delas se relacionam à esteganografia, a arte de ocultar mensagens, enquanto outras estão ligadas à criptografia, que trata da codificação de mensagens.

Um dos métodos criptográficos mais conhecidos é a Cifra de César, uma cifra de substituição usada pelo ditador romano Júlio César. Outro exemplo é a cifra polialfabética, introduzida por Leone Battista Alberti no século XV. No século XX, surgiu o RSA, um dos primeiros sistemas de criptografia com chave assimétrica, cuja base teórica está na aritmética.

Atualmente, a criptografia é essencial para a segurança de dados e informações, sendo amplamente utilizada em aplicativos bancários e de mensagens, como o WhatsApp e o Telegram.

Objetivos

O objetivo geral do projeto é desenvolver estudos sobre criptografia para estudantes do Ensino Fundamental II e Médio, utilizando programas computacionais. Além disso, busca-se proporcionar um primeiro contato com uma linguagem de programação, o Google Planilhas.

2 Metodologia

A pesquisa incluiu a leitura de trabalhos sobre métodos criptográficos, a utilização do Google Planilhas e do Wolfram Alpha, além de uma revisão bibliográfica focada em aritmética. Os autores se reuniam semanalmente para analisar os resultados e estruturar o estudo em tópicos aplicáveis ao ensino básico.

Os livros [1] , [2] , [3] compõem o referencial teórico básico deste trabalho.

[1]alexandre.batista@ufv.br
[2]luisfelipe@ufv.br
[3]Este template foi baseado no modelo de trabalho completo do CNMAC 2024, disponível no Overleaf.

3 Resultados e Discussão

Nesta seção, apresentaremos dois exemplos que ilustram parte do trabalho "Criptografia no Ensino Básico". Embora seja apenas um recorte parcial, ele é suficiente para destacar o foco deste estudo: o uso de tecnologias no ensino da matemática, com ênfase no Google Planilhas e no Wolfram Alpha.

O primeiro exemplo é teórico. O segundo é numérico. O principal referencial teórico desta seção é [3]. As obras [1] e [2] são complementares.

Nos dois exemplos, faremos a seguinte associação entre as letras do alfabeto e os números de 10 a 35.

Tabela 1: Tabela de substituição para o algoritmo RSA

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

Exemplo 1

Alice enviará uma mensagem para Bob. Bob possui uma chave pública (n, e), usada para codificar a mensagem, e uma chave privada (n, d), usada para decodificar a mensagem. O número n é o produto de dois números primos p e q com centenas de algarismos. Os inteiros e, d são maiores que 1, menores que $\varphi(n)$, invertíveis módulo $\varphi(n)$ e, além disso, satisfazem a identidade

$ed \equiv 1 \ \ mod\ \varphi(n)$, sendo φ a função de Euler.

Mesmo que uma fonte não autorizada tenha acesso à chave pública, ainda será necessário descobrir os números p e q para determinar a chave privada. No entanto, a fatoração de números muito grandes em fatores primos é extremamente difícil e demorada, mesmo para os sistemas computacionais mais avançados.

Bob informará à Alice a sua chave-pública. A partir dela, Alice começará a codificação da mensagem que deseja enviar para Bob.

Etapas

1. Alice faz a pré-codificação da mensagem.
2. Em seguida, ela enfileira todos os códigos, transformando-os em um único número. Logo após, o número é dividido em blocos $T_1, T_2, ..., T_r$ de forma que todos sejam menores do que n e não iniciem com o algarismo zero. Além disso, o comprimento de cada bloco não deve ser múltiplo de p ou q.
3. Para codificar sua mensagem, Alice define

$$C_i \equiv T_i^e \pmod{n}, \tag{1}$$

para todo $i = 1, 2, 3, .., r$. Então a mensagem recebida por Bob será:

$$C_1 C_2 C_3 ... C_r. \tag{2}$$

Para decodificar a mensagem, Bob utiliza sua chave privada formada pelo par (n, d).

$$T_i \equiv C_i^d \pmod{n} \tag{3}$$

para cada $i = 1, 2, 3, .., r$. Assim, ele decodifica a mensagem original $T_1, T_2, ..., T_r$.

Comentários sobre o Exemplo 1

Ao iniciarmos o processo matemático, definimos

$$C_i \equiv T_i^e \pmod{n} \text{ para cada } \ i = 1, 2, 3, .., r. \tag{4}$$

Decorre que

$$C_i^d \equiv (T_i^e)^d \equiv T_i^{ed} \pmod{n}. \tag{5}$$

Como $ed \equiv 1 \pmod{\varphi(n)}$, existe um $k \in \mathbb{N}$ tal que $ed = k\varphi(n) + 1$. Dessa forma:

$$C_i^d \equiv T_i^{ed} \equiv T_i^{k\varphi(n)+1} \equiv T^{k\varphi(n)}.T_i. \tag{6}$$

Para finalizar, segue do Teorema de Euler e da propriedade da potenciação de congruências que:

$$T^{k\varphi(n)} \equiv 1 \pmod{n}. \tag{7}$$

Ou seja:

$$T^{k\varphi(n)}.T_i \equiv T_i \tag{8}$$

No próximo exemplo, exploraremos o Google Planilhas e o Wolfram Alpha como recurso computacional.

Exemplo 2

Decifrar a mensagem

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

criptografada com a chave pública $(n, e) = (91, 5)$ e decodificada com a chave privada $(n, d) = (91, 29)$.

Etapas Iniciais

1. Abra o Google Planilhas.
2. Na célula A1, insira o texto "**n**". A célula B1 será rotulada com "**d**".
3. Na linha 2, apresente os valores equivalentes a cada célula rotulada na linha 1, quer dizer, $n = 91$ e $d = 29$.
4. O objetivo é descriptografar a mensagem, processo inverso à codificação. Nesse sentido, rotule a célula A4 com o texto "**CIFRA**". Da célula A5 em diante, coloque a sequência de cifras.
5. Posicione as 26 letras do alfabeto em ordem. Rotule a célula B4 por "**TEXTO ORIGINAL, abreviado aqui por MSG ORIGINAL**" e, em B5, digite a fórmula:

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

   O comando ARRAYFORMULA(CARACT(SEQUENCE(26;1;65))) permite que o cálculo seja feito em uma matriz, retornando todas as letras de A a Z em uma única fórmula, sem precisar arrastar ou repetir a fórmula em várias células.
6. A célula C4 deverá receber a inscrição "**MENSAGEM CRIPTOGRAFADA (C), abreviada por MSG CODIFICADA (C)**". Nas células de baixo, digite a mensagem codificada, lembrando de inserir um código em cada célula.
7. Na coluna D, rotule D4 com o texto $C = B \hat{} \, d \, (mod \, n)$. Na célula D5, insira a fórmula:

=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).

Limitação do Google Planilhas

Após executar os passos descritos, espera-se obter números inteiros nas células da coluna D. No entanto, o editor de planilhas exibiu, nessas células, o erro #**NUM!**. Isso ocorreu devido à limitação do Google Planilhas ao lidar com números muito grandes. O Google Planilhas usa a especificação de números do tipo "double" com 64 bits para os cálculos numéricos.

A	B	C	D
n	d		
91	29		
CIFRA	MSG ORIGINAL	MSG CODIFICADA (C)	RESTO DE (C elev 29) : 91
10	A	32	#NUM!
11	B	8	#NUM!
12	C	33	#NUM!
13	D	29	#NUM!
14	E	82	#NUM!
15	F	33	#NUM!
16	G	88	#NUM!
17	H	22	#NUM!
18	I	33	#NUM!
19	J	22	#NUM!
20	K	82	#NUM!
21	L	32	#NUM!
22	M	1	1

Figura 1: RSA com chave privada (91,29). Planilha parcial. Fonte: Autoria Própria

O **Wolfram Alpha** pode realizar esses cálculos e está disponível tanto na Web quanto em aplicativo, acessível pela App Store e Google Play.

O Wolfram Alpha possui um campo de entrada para os cálculos desejados e não tem um limite rígido de bits para cálculos numéricos. A precisão pode ser aumentada dinamicamente, permitindo trabalhar com números de qualquer tamanho ou com a quantidade de dígitos necessária, dentro das capacidades do hardware disponível.

Como exemplo, apresentaremos o cálculo da decifragem da primeira cifra, sendo que os demais cálculos devem ser realizados de forma análoga. Para isso, basta digitar a seguinte expressão no campo de entrada do site: 32 ^ 29 (mod 91)

A ferramenta nos apresenta, na caixa "*Result*", o valor 2. Assim, o primeiro bloco foi encontrado. Todos estes cálculos foram feitos com a versão gratuita do Wolfram Alpha.

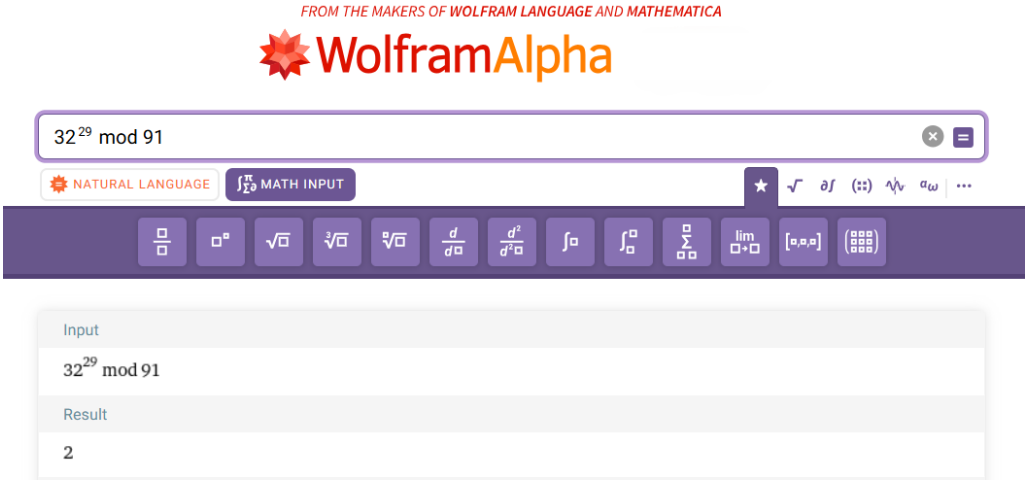

Figura 2: Interface do Wolfram Alpha

Os valores calculados a partir do Wolfram Alpha são:

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

Etapas finais

1. À medida que os cálculos no Wolfram Alpha são realizados, insira esses resultados na planilha. Rotule a célula E4 com o texto: **BLOCOS B (< p x q) WOLFRAM**. Logo após, insira, nessa coluna, os dados obtitos no programa. Inicie a lista pela célula E5.

2. No item anterior, os números encontrados representam os blocos relativos às cifras pré-codificadas. Sendo assim, é preciso encontrar as cifras. Cifras nas quais a mensagem foi pré-codificada. Para isso, rotule a célula F5 com **CIFRA DIGITAL**. Em seguida, junte 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.

3. Para recuperar a mensagem original, deve-se usar a funcionalidade do editor de planilhas. Inicie rotulando a célula G4 com: **MENSAGEM ORIGINAL**. Feito isso, na célula G5, insira a fórmula:

   $$=\text{PROCV(F5;A\$5:B\$30;2;0)}.$$

   O comando PROCV(F5;A\$5:B\$30;2;0) executa uma busca vertical na tabela para encontrar um valor exato na coluna A dentro do intervalo $A5 : B30$ e retorna o valor correspondente da coluna B.

   A mensagem decodificada é **SOMA OU TOTAL**.

A	B	C	D	E	F	G
n	d					
91	29					
CIFRA	MSG ORIGINAL	MSG CODIFICADA (C)	RESTO DE (C elev 29) : 91	BLOCOS B (< pxq) WOLFRAM	CIFRA DIGITAL	MSG ORIGINAL
10	A	32	#NUM!	2	28	S
11	B	8	#NUM!	8	24	O
12	C	33	#NUM!	24	22	M
13	D	29	#NUM!	22	10	A
14	E	82	#NUM!	10	24	O
15	F	33	#NUM!	24	30	U
16	G	88	#NUM!	30	29	T
17	H	22	#NUM!	29	24	O
18	I	33	#NUM!	24	29	T
19	J	22	#NUM!	29	10	A
20	K	82	#NUM!	10	21	L
21	L	32	#NUM!	2		
22	M	1	1	1		

Figura 3: Google Planilhas. Planilha parcial. Fonte: Autoria Própria

4 Considerações Finais

Este trabalho explorou a criptografia RSA, com ênfase em sua aplicação por meio do Google Planilhas e do Wolfram Alpha. Destacamos que o uso de planilhas não apenas facilita o aprendizado de informática, elemento essencial para a formação profissional dos alunos, mas também introduz os alunos às linguagens de programação, ao mesmo tempo que reforça sua compreensão matemática.

Esperamos que este estudo sirva como referência e fonte de inspiração para futuras pesquisas educacionais no campo da matemática.

Agradecimentos

O primeiro autor agradece à Capes pelo apoio financeiro durante o seu mestrado.

Referências

[1] Framílson José Ferreira Carneiro. **Criptografia e Teoria dos Números**. 1a. ed. Rio de Janeiro: Editora Ciência Moderna, 2016. ISBN: 8539908204.

[2] José Laudelino de Menezes Neto. **Primeiros passos em criptografia [recurso eletrônico]**. 1a. ed. João Pessoa: Editora UFPB, 2021. ISBN: 978-65-5942-143-5.

[3] Salahoddin Shokranian. **Criptografia para Iniciantes**. 2a. ed. Rio de Janeiro: Editora Ciência Moderna, 2021. ISBN: 8539902753.