PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.2, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo811

Criptografia na educação básica: das escritas ocultas ao código RSA

Igor Nascimento da Silva Christine Sertã Costa

Resumo

Este trabalho, fruto de uma dissertação de conclusão de curso do Profmat PUC-Rio apresentada em 2016, propõe a introdução nas aulas de matemática da escola básica de um tema que agrega significado e interesse ao alunado. A partir dele, é possível desenvolver conteúdos novos e clássicos de matemática pertinentes a esse nível de escolaridade. O tema em questão é a criptografia, e esta escolha possibilitou o desenvolvimento de uma abordagem histórica da sua evolução até o código RSA, a promoção de discussões sobre a relevância atual do assunto até os nossos dias e o trabalho com conteúdos importantes da matemática básica. Com o intuito de aprimorar e avaliar a proposta, uma pequena aplicação numa escola pública foi feita, através de uma oficina, com resultados bastante satisfatórios. Pretende-se que este trabalho seja mais uma fonte para auxiliar professores na construção de novas propostas pedagógicas adaptadas à realidade de cada sala de aula com olhar motivador, significativo e contemporâneo.

Palavras-chave: Aritmética modular; Criptografia na educação básica; RSA.

Abstract

This work, the result of a dissertation dissertation by Profmat PUC-Rio presented in 2016, proposes the introduction in mathematics classes of the basic school of a theme that adds meaning and interest to the students. From it, it is possible to develop new and classic mathematics content relevant to this level of education. The subject in question is cryptography and this choice enabled the development of a historical approach to its evolution to the RSA code, the promotion of discussions on the current relevance of the subject to the present day and the work with important contents of basic mathematics. In order to improve and evaluate the proposal, a small application in a public school was made, through a workshop, with very satisfactory results. It is intended that this work is another source to assist teachers in the construction of new pedagogical proposals adapted to the reality of each classroom with a motivating, meaningful and contemporary look.

Keywords: Modular arithmetic; Encryption in basic education; RSA.

1. Introdução

O presente artigo é fruto do trabalho de conclusão de curso (TCC) do Profmat PUC-Rio apresentado em 2016 e intitulado CRIPTOGRAFIA NA EDUCAÇÃO BÁSICA: DAS ESCRITAS

OCULTAS AO CÓDIGO RSA (Silva, 2016). O trabalho original constrói uma trajetória histórica que retrata a evolução de alguns sistemas criptográficos desde os mais rudimentares até o código RSA; apresenta, descreve e demonstra conceitos matemáticos que fundamentam esses sistemas; propõe uma sequência didática de aplicações práticas sobre o tema, pertinentes para uma sala de aula da educação básica e, finalmente, analisa alguns resultados das aplicações realizadas numa escola pública do estado do Rio de Janeiro.

Todo o estudo foi pensado procurando aliar pesquisa e fundamentação teórica e prática ao chão da escola básica, com a pretensão de trazer significado e motivação ao alunado. Objetivou-se contribuir para o desenvolvimento do pensamento matemático lógico e crítico e para a ampliação do repertório histórico e cultural de cada aluno de modo que ele se torne, cada vez mais, um cidadão capaz de, com autonomia, construir suas estratégias, argumentações e conclusões. No presente texto, um recorte com um enfoque mais conceitual do trabalho original é apresentado.

2. Justificativa e motivação

Procurar um assunto contemporâneo, relevante e carregado de significado para os alunos foi um dos desafios primordiais do trabalho desenvolvido. Com esse olhar, a criptografia foi o tema escolhido, uma vez que, além de ser um assunto com avanços significativos e relevantes na história mundial e estar presente em importantes aplicações do mundo moderno, permite o desenvolvimento de conteúdos matemáticos interessantes e possíveis de serem abordados na escola básica.

Constatamos que muitos alunos desse nível de escolaridade ainda desconhecem o significado da palavra criptografia mas ficam curiosos sobre o tema assim que o mesmo lhes é apresentado. Por outro lado, outros já experimentaram algum contato com o tema através de séries, filmes, livros ou notícias. Fazer uso dessas associações que partem das vivências dos alunos facilita o trabalho do professor, amplia o arcabouço cultural e acadêmico do alunado e, especialmente, o aproxima da Matemática.

Para trabalhar o tema, fez-se necessário desenvolver o estudo da aritmética modular, assunto esse que não consta no currículo mínimo da educação básica, mas que é pertinente e viável de ser trabalhado neste nível de escolaridade e certamente auxilia e traz significado a outros conteúdos, como os sistemas de numeração, critérios de divisibilidade, estudos sobre números primos e resolução de equações.

O fato de que uma comunicação possa se estabelecer entre duas pessoas, de modo que uma terceira pessoa não consiga compreender o significado da mensagem encaminhada, aliado à notória fascinação desta geração pela tecnologia encanta e desperta o interesse e curiosidade de crianças e adolescentes, possibilitando um solo fértil para o aprendizado.

3. Um passeio histórico por alguns sistemas criptográficos

Segundo SINGH (2007), um dos primeiros relatos de escrita oculta foi encontrado no livro *As histórias de Heródoto* (485 a.C–420 a.C). Singh relata que Demarato, um grego que teria sido expulso de sua terra natal, sabendo dos planos de uma possível invasão de Xerxes, imperador Persa de 486 a.C até a data de seu assassinato em 465 A.C, à Grécia, mandou uma mensagem ao seu povo, raspando a cera de um par de tabuletas, escrevendo os planos de Xerxes nessas madeiras e em seguida cobrindo-as novamente com cera. Sua mensagem chegou aos gregos de forma segura e deixou-os preparados para a invasão. Este artifício de ocultar fisicamente uma mensagem recebe o

nome de esteganografia, derivado do grego *steganos*, que significa coberto, e *graphein*, que significa escrever.

Com o surgimento da criptografia, do grego *kriptos* que significa oculto, as mensagens não precisavam mais ser ocultadas fisicamente. Outras estratégias para que uma mensagem enviada por um remetente a um destinatário não fizesse sentido para uma terceira pessoa, passaram a ser utilizadas. De modo geral, essas estratégias dividiram-se em dois grandes grupos de sistemas criptográficos: a cifra da transposição e a da substituição.

Na transposição, as letras do texto original são misturadas com um determinado critério previamente combinado entre remetente e destinatário, formando anagramas que, especialmente para textos longos, tornam-se difíceis de serem decifrados. A Cerca de Ferrovia (Figura 1) e o Citale Espartano (Figura 2) são exemplos de criptografias da categoria transposição.

Na primeira, escreve-se as letras da mensagem original de forma alternada em duas linhas, e a mensagem cifrada é escrita com as letras da primeira linha seguida das letras da segunda linha.

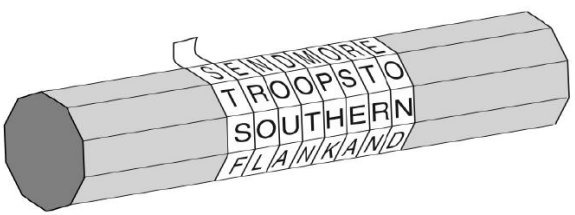
V		U		E		T		A		A		U		P		U		O
	O		M		A		R		S		R		M		O		C	

Mensagem original: VOU ME ATRASAR UM POUCO

Mensagem cifrada: VUETAAUPUOOMARSRMOC

Figura 1: Cerca de Ferrovia

Já na criptografia do tipo Citale Espartano, remetente e destinatário precisam possuir um bastão (citale) de madeira idêntico. Uma fita de couro é enrolada neste bastão pelo destinatário e a mensagem é escrita ao longo do comprimento do bastão. A fita então é desenrolada e enviada ao destinatário que só consegue decifrar a mensagem quando enrola novamente a fita no bastão idêntico ao do remetente.



Mensagem original:

SEND MORE TROOPS TO SOUTHERN FLANK...

Mensagem cifrada:

STSF...

Figura 2: Citale Espartano

A cifra da substituição consiste em trocar cada letra da mensagem original por outra letra do alfabeto, seguindo um determinado padrão preestabelecido. Segundo SINGH (2007), uma das

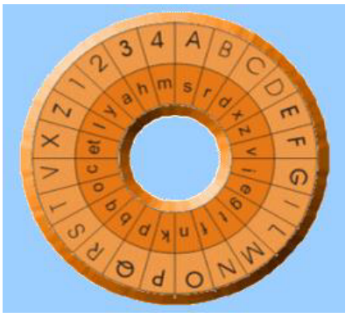
primeiras descrições da substituição data do século IV a.C. A principal fraqueza desse tipo de codificação é que, com uma análise de frequência das letras do idioma aliada a um conhecimento da sua estrutura, é possível decifrar a mensagem.

A Cifra de César, muito utilizada pelo imperador Júlio Cesar na Roma Antiga, é um exemplo de uma cifra de substituição que utilizava um deslocamento de 3 posições no alfabeto, conforme mostra a Figura 3.

alfabeto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cifra	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Original:	atacar ao meio dia																									
Cifrada:	DWDFDU DR PHLR GLD																									

Figura 3: Cifra de Cesar

O disco de Alberti (Figura 4), formado por dois discos concêntricos com diâmetros distintos presos por um pino, foi criado em 1466. É também um sistema de substituição em que destinatário e remetente precisam possuir discos idênticos e combinar uma letra de cada disco para alinhá-las nos discos e servir de base do sistema. A Figura 4 retrata uma situação em que as letras V, do disco maior, e c, do disco menor, foram alinhadas. Neste sistema, também, foi incorporado uma espécie de dicionário de códigos que associa algumas palavras a números, dificultando ainda mais a decodificação.



Mensagem original: MATAR O REI LOGO

Mensagem cifrada: tsosb n yam gngn

Obs.: Supondo que, no dicionário de códigos, a palavra REI esteja associada ao numeral 124

Figura 4: Disco de Alberti

Por volta de 1518, um grande passo para a criptografia é dado com o surgimento de sistemas de cifragem que utilizam a chamada Tabula Recta – uma tabela que possui o mesmo número de linhas e colunas e onde na primeira linha escreve-se o alfabeto na ordem normal e em cada linha seguinte escreve-se o alfabeto da linha anterior deslocado de uma posição, conforme a Figura 5. A cifragem de uma mensagem tem a primeira linha como referência para as substituições, e a primeira letra da mensagem é transformada na letra correspondente na segunda linha, a segunda letra é transformada na letra correspondente na terceira linha e assim sucessivamente.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Mensagem original: CHEGO NA SEGUNDA
Mensagem cifrada: DJHKT TH ANQFZQO

Figura 5: A Tabula Recta e uma cifragem

A Cifra de Vigenère é um exemplo de um sistema de substituição mais sofisticado que foi apresentado por volta de 1586. Também utiliza a Tabula Recta mas agrega o **conceito de chave** – usada para cifrar e/ou decifrar mensagens. Nesse sistema, a chave inicial é uma letra que é usada para cifrar a primeira letra da mensagem original. Em seguida, a primeira letra da mensagem original torna-se a chave para cifrar a segunda letra da mensagem e assim sucessivamente. O procedimento para a cifragem consiste em substituir cada letra da mensagem original pela letra correspondente ao par ordenado (letra da chave, letra da mensagem original) na Tabula Recta.

Por exemplo, na Figura 6 a seguir, a chave inicial foi a letra b e a mensagem a ser codificada é ATACAR HOJE. Assim, consultando na Tabula Recta (Figura 5) o par ordenado (chave inicial, primeira letra da mensagem original)= (b, A), vemos que esse par está relacionado à letra B, que se torna a primeira letra da mensagem cifrada. O próximo par ordenado a ser pesquisado (primeira letra da mensagem original, segunda letra da mensagem original)= (A, T) corresponde na TabuRecta à letra T, que é portanto a segunda letra da mensagem cifrada. Seguindo com esse procedimento, os próximos pares da mensagem exemplificada são (T, A) = T, (A, C) = C, (C, A) = C, (A, R) = R, (R, H) = Y, (H, O) = V, (O, J) = Xe(J, E) = N, finalizando a mensagem cifrada BTTCCRYVXN.

Chave	b	A	T	A	C	A		R	H	O	J
Mensagem original	A	T	A	C	A	R		H	O	J	E
Mensagem cifrada	**B**	**T**	**T**	**C**	**C**	**R**		**Y**	**V**	**X**	**N**

Figura 6: Cifra de Vigenere

Durante a segunda guerra mundial, diversas máquinas cifradoras foram construídas, entre elas a japonesa Purple e as alemãs Enigma e Lorenz SZ40. Nessa época, havia também um grande esforço em construir máquinas decifradoras. Para isso, os britânicos contaram com a ajuda de um dos pais da computação, Alan Turing, que em 1938 fazia parte de uma organização do governo britânico responsável por quebrar códigos e enigmas, chamada Government Code and Cypher School. Com o começo da guerra em 1939, Turing ingressou no Bletchley Park, a instalação que reuniu grandes matemáticos e criptógrafos e que teve papel fundamental na interceptação de mensagens trocadas pelos exércitos da Itália, Alemanha e Japão. Nessa instalação houve uma intensa cooperação de cientistas ingleses, franceses e poloneses para decifrar o código utilizado pelos alemães e seus aliados.

Por meio dos estudos de Turing e dos demais pesquisadores desse grupo, foi concebida uma máquina decifradora conhecida como "bomba eletromecânica" (The Bombe, em inglês), que decifrou o código da máquina Enigma e permitiu que os Aliados tivessem acesso a informações privilegiadas ao longo da guerra. A cada mês, cerca de 84 mil mensagens enviadas pelos alemães via Enigma eram decifradas. Os britânicos, por exemplo, conseguiram mapear a posição de embarcações alemãs, e, dessa forma, desviar a rota das embarcações inglesas com antecipação.

Os estudos de Turing também serviram de base para que a cifra da Lorenz fosse quebrada em 1943, com a máquina Colossus, que se tornou a precursora do computador digital.

Todas essas máquinas trabalhavam com o conceito de chaves simétricas, ou seja, a mesma chave que era usada para cifrar mensagens também era usada para decifrá-las. O principal empecilho, por muito tempo, para o desenvolvimento da criptografia foi a questão da troca de chaves, um problema que chegou a ser considerado sem solução. Ou a chave deveria ser trocada diretamente entre os correspondentes, o que nem sempre era uma tarefa simples, ou tal tarefa deveria ser delegada outra pessoa, o que nem sempre era uma tarefa segura.

4. Sobre a aritmética modular

Para os sistemas criptográficos apresentados a partir de agora é importante o entendimento de algumas definições, propriedades e resultados relativos à aritmética modular que apresentamos a seguir.

Sejam a, b e m inteiros com m não nulo.

Definição 1. Dizemos que dois números inteiros a e b são congruentes módulo m, se m é um divisor de a – b. Utilizamos a notação: a ≡ b mod m.

Corolário 1. *Dizemos que dois números inteiros* a *e* b *são congruentes módulo* m*, se* a *e* b *deixam o mesmo resto na divisão euclidiana por* m.

Para efeito de simplificação vamos considerar $m > 1$ uma vez que:

1. É fato que $a \equiv b \bmod m$ sempre que $m = 1$ e

2. Se $a \equiv b \bmod m$ então $a \equiv b \bmod -m$.

Decorre naturalmente da definição de congruência módulo m, as propriedades enunciadas a seguir. Considere a, b, c, d e m inteiros com m não nulo e n um natural.

Propriedade 1. *A congruência módulo* m *é uma relação de equivalência sobre o conjunto* Z *dos números inteiros uma vez que satisfaz às seguintes propriedades:*

1. $a \equiv a \bmod m$ *(Reflexiva)*

2. Se $a \equiv b \bmod m$ *então* $b \equiv a \bmod m$ *(Simétrica)*

3. Se $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$ *então* $a \equiv c \bmod m$ *(Transitiva)*

Propriedade 2. *Se* $a \equiv b \bmod m$ *e* $0 \leqslant b < m$ *então* b *é o resto da divisão de* a *por* m. *(Observe que sempre existe um único* $0 \leqslant b < m$ *tal que* $a \equiv b \bmod m$.*)*

Propriedade 3. *Se* $a \equiv b \bmod m$ *então* $a + c \equiv b + c \bmod m$.

Propriedade 4. *Se* $a \equiv b \bmod m$ *então* $ac \equiv bc \bmod m$.

Propriedade 5. *Se* $a \equiv b \bmod m$ *então* $ac \equiv bc \bmod mc$.

Propriedade 6. *Se* $a \equiv b \bmod m$ *então* $a^n \equiv b^n \bmod m$.

Propriedade 7. *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$ *então* $a + c \equiv b + d \bmod m$.

Propriedade 8. *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$ *então* $ac \equiv bd \bmod m$.

A definição de inverso multiplicativo e alguns teoremas que envolvem congruências e números primos também são necessários para um completo entendimento do funcionamento dos sistemas apresentados nas próximas seções, e estão listados a seguir.

Definição 2. Se existe um inteiro b tal que $ab \equiv 1 \bmod m$ diz-se que b é o inverso multiplicativo de a módulo m.

Teorema 1. *Se* a *e* m *são primos entre si, então existe o inverso multiplicativo de* a *módulo* m.

Teorema 2. *Se* p *é primo então* $(a + b)^p \equiv a^p + b^p \bmod p$. *(Teorema Binomial Fácil)*

Teorema 3. *Se* p *é primo então* $a^p \equiv a \bmod p$. *(Pequeno Teorema de Fermat)*

Teorema 4. *Se* p *é primo e* a *não é múltiplo de* p *então* $a^{p-1} \equiv 1 \bmod p$.

Teorema 5. *Sejam* $m_1, m_2, ..., m_k$ *números inteiros positivos, dois a dois primos entre si. O sistema de congruências* $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ ... \\ x \equiv a_k \bmod m_k \end{cases}$ *admite uma solução simultânea, que é única módulo o inteiro* $m = m_1 m_2 ... m_k$. *(Teorema Chinês do Resto - TCR)*

5. Uma troca de chaves mais eficiente: o sistema DHM

Em 1976, foi apresentado por Whitfield Diffie, Martin Hellman e Ralph Merkle uma função de mão única que resolvia de forma simples o problema da troca de chaves. Eles desenvolveram uma função matemática fácil de ser calculada mas difícil de ser revertida. O sistema ficou conhecido como sistema DHM, em homenagem a seus criadores, e possibilitou que duas pessoas distintas conseguissem calcular a chave de um sistema criptográfico de forma independente. Essa função, de mão única, tem por base conceitos da aritmética modular e possibilita que dois interlocutores calculem a chave, sem necessidade de compartilhá-la diretamente.

Seja α a chave a ser calculada. Os passos a seguir explicam o procedimento para esse cálculo.

Suponha que duas pessoas, M e G, desejem calcular uma chave α de um sistema criptográfico pelo sistema DHM.

1. M e G precisam conhecer dois números naturais, Y e P, públicos.
2. G escolhe um número α_{G}, calcula o número β_{G} como sendo o resto da divisão de $\mathrm{Y}^{\alpha_{\mathrm{G}}}$ por P e envia β_{G} para M.
3. M escolhe um número α_{M}, calcula o número β_{M} como sendo o resto da divisão de $\mathrm{Y}^{\alpha_{\mathrm{M}}}$ por P e envia β_{M} para G.
4. De posse de β_{M}, G pode calcular o resto da divisão de $\beta_{\mathrm{M}}^{\alpha_{\mathrm{G}}}$ por P. Mas, $\beta_{\mathrm{M}} \equiv \mathrm{Y}^{\alpha_{\mathrm{M}}} \bmod \mathrm{P} \Rightarrow \beta_{\mathrm{M}}^{\alpha_{\mathrm{G}}} \equiv \mathrm{Y}^{\alpha_{\mathrm{M}}\alpha_{\mathrm{G}}} \bmod \mathrm{P}$.
5. De modo análogo, M pode calcular o resto da divisão de $\beta_{\mathrm{G}}^{\alpha_{\mathrm{M}}}$ por P. Mas, $\beta_{\mathrm{G}} \equiv \mathrm{Y}^{\alpha_{\mathrm{G}}} \bmod \mathrm{P} \Rightarrow \beta_{\mathrm{G}}^{\alpha_{\mathrm{M}}} \equiv \mathrm{Y}^{\alpha_{\mathrm{G}}\alpha_{\mathrm{M}}} \bmod \mathrm{P}$.
6. A chave α procurada portanto pôde ser calculada tanto por G quanto por M.

A Figura 7 a seguir resume e apresenta um exemplo numérico para os passos do cálculo da chave pelo sistema DHM.

PASSOS	EXEMPLO
G e M escolhem dois números naturais em comum acordo, Y e P, que podem ser públicos.	Y = 53 e P = 170
G escolhe, sem divulgar, um número natural α_G e calcula $\beta_G < P$ tal que $Y^{\alpha_G} \equiv \beta_G \bmod P$. G envia β_G a M.	α_G = 7. O resto da divisão de 53^7 por 170 é $\beta_G = 77$
M escolhe, sem divulgar, um número natural α_M e calcula $\beta_M < P$ tal que $Y^{\alpha_M} \equiv \beta_M \bmod P$. M envia β_M a G.	α_M = 5. O resto da divisão de 53^5 por 170 é $\beta_M = 83$
G calcula $\alpha < P$ como o resto da divisão de $\beta_M{}^{\alpha_G}$ por P. Como $\beta_M \equiv Y^{\alpha_M} \bmod P$, $\beta_M{}^{\alpha_G} \equiv (Y^{\alpha_M})^{\alpha_G} \equiv Y^{\alpha_M \alpha_G} \equiv \alpha \bmod P$.	O resto da divisão de 83^7 por 170 é 127
M calcula $\alpha < P$ como o resto da divisão de $\beta_G{}^{\alpha_M}$ por P. Como $\beta_G \equiv Y^{\alpha_G} \bmod P$, $\beta_G{}^{\alpha_M} \equiv (Y^{\alpha_G})^{\alpha_M} \equiv Y^{\alpha_G \alpha_M} \equiv \alpha \bmod P$.	O resto da divisão de 77^5 por 170 é 127

Figura 7: O sistema DHM

Observe que o sistema é útil quando se trata da comunicação entre duas pessoas por vez, o que nem sempre é satisfatório. Além disso, o cálculo da chave depende do envio a M do número β_G e do envio a G do número β_M. Embora esses números possam ser enviados de forma pública, esse procedimento possivelmente torna o processo mais lento.

6. Um sistema criptográfico importante: o sistema RSA

Em 1977, Ron Rivest, Leonard Adleman e Adi Shamir, pesquisadores do laboratório de ciência da computação do Massachusetts Institute of Technology, sofisticaram o DHM incluindo características necessárias para seu funcionamento com chaves assimétricas (chaves distintas para cifrar e decifrar). Surgia assim o sistema RSA, em homenagem a seus criadores, e que se tornaria a cifra mais influente da criptografia moderna.

O RSA ficou conhecido como criptografia de chave pública, onde parte dessa chave é um número N, cujo valor é obtido pelo produto de dois números primos (bem grandes), p e q. Nesse caso, o valor de N pode ser divulgado amplamente, pois tal chave é utilizada para cifrar as mensagens, mas os valores de p e q devem ser mantidos em sigilo, pois sem esses valores fica impossível obter a chave de decifragem. Cabe ressaltar que, teoricamente, conhecendo-se o valor de N é possível deduzir os valores de p e q, mas, na prática, essa não é uma tarefa fácil. Quando p e q são dois números primos muito grandes, nem mesmo os computadores mais modernos conseguem obtê-los a partir de N, e é aí que se encontra a segurança do RSA.

Segundo COUTINHO (2015), o RSA Laboratory, que pertence à empresa detentora dos direitos do sistema, propôs desafios que consistiam em fatorar possíveis chaves públicas (N). Ainda segundo o autor, a última fatoração até então, anunciada em 2005, de um número com 193 algarismos,

utilizou 80 computadores de 2.2GHz cada e, ainda assim, foram necessários 5 meses para que todas as contas fossem finalizadas. Mais recentemente, em 2019, foi anunciado um novo maior número primo descoberto, que é composto por 24.862.048 algarismos. Esse número é o 51º primo de Mersenne e denominado no meio matemático por M82589933. Tais considerações deixam clara a magnitude da dificuldade da fatoração, garantindo assim a segurança do RSA.

Voltando aos personagens M e G, suponha agora que M (remetente) deseje encaminhar uma mensagem X cifrada para G (destinatário), utilizando o sistema RSA. Os passos a seguir explicam o funcionamento desse código.

1. O destinatário (G) escolhe dois números primos grandes p e q e calcula N = pq.
2. G escolhe um número α (chave de codificação) tal que mdc(α, ϕ(N)) = 1 onde ϕ(N) = (p–1)(q–1).
3. G divulga N e α (números que compõe a chave pública). Qualquer um que queira encaminhar uma mensagem para G precisa dessa chave e pode obtê-la, já que é pública.
4. De posse de N e de α, o remetente (M) calcula o número Y que é o resto da divisão de X^{α} por N. Y é o número X codificado.
5. M divulga Y.
6. De posse de Y, apenas G consegue decodificá-lo, já que apenas G conhece p e q. G calcula o número β (chave de decodificação) resolvendo a equação de congruência $\alpha\beta \equiv 1 \mod \phi(N)$.
7. De posse de β, G consegue decodificar Y obtendo X já que X é o resto da divisão de Y^{β} por N.

A Figura 8 abaixo resume e apresenta um exemplo numérico para os passos da codificação (cifragem – transformar X em Y) e decodificação (decifragem – transformar Y em X) pelo sistema RSA.

PASSOS	EXEMPLO
G escolhe dois números primos suficientemente grandes p e q e obtém N=p.q. O valor de N é amplamente divulgado, mas os valores de p e q são mantidos em sigilo.	p=13 e q=11. Portanto N=143
G escolhe um número α, chave de codificação, tal que mdc(α,φ(N)) = 1 onde φ(N) = (p – 1).(q – 1). α também é amplamente divulgado.	α=7. Observe que mdc(7,120)=1
M tem acesso a N e a α e, então, calcula $Y \equiv (X)^{\alpha} \mod N$ e envia Y para G.	Supondo X=19, tem-se que o resto da divisão de 19^7 por 143 é Y=46
G conhece p e q e, portanto, pode calcular a chave de decodificação β tal que . $\alpha.\beta \equiv 1 \mod \varphi(N)$	β = 103 é solução de $7\beta \equiv 1 \mod 120$
G decodifica Y, obtendo X, calculando $(Y)^{\beta} \equiv X \mod N$.	X=19 é o resto da divisão de 46^{103} por 143

Figura 8: O código RSA

Por que funciona?

Observe que inicialmente G escolhe dois números primos suficientemente grandes p e q e calcula N = pq. O valor de N então é amplamente divulgado (público), mas os valores de p e q são mantidos em sigilo. Apenas o destinatário G (que vai decodificar a mensagem) o conhece. Em seguida G escolhe também um número α, chave de codificação, com a única restrição que $\text{mdc}(\alpha, \phi(N)) = 1$, onde $\phi(N) = (p-1)(q-1)$. O valor de α também é amplamente divulgado (público).

Um destinatário (M), interessado em enviar uma mensagem criptografada para G, deve obter os valores públicos de N e α. E, para codificar uma mensagem X transformando-a na mensagem codificada Y, basta calcular o resto da divisão de X^α por N, ou seja, basta resolver a equação de congruência $Y \equiv X^\alpha \mod N$. M assim envia a mensagem Y, que está codificada, para G.

G precisa decodificar Y, ou seja, G precisa encontrar a mensagem original X que satisfaz $X^\alpha \equiv Y \mod N$. Para isso, G vai precisar da chave β de decodificação que só ele pode encontrar, uma vez que só ele conhece os valores de p e de q e, portanto, só G conhece o valor de $\phi(N)$. Como $\text{mdc}(\alpha, \phi(N)) = 1$, sabe-se que existe o inverso multiplicativo de α módulo $\phi(N)$ (teorema 1). Esse número é justamente a chave β de decodificação, uma vez que:

$\alpha\beta \equiv 1 \mod \phi(N) \Rightarrow \alpha\beta - 1 = k(p-1)(q-1)$, k inteiro $\Rightarrow \alpha\beta = 1 + k(p-1)(q-1) \Rightarrow X^{\alpha\beta} = X^1 X^{k(q-1)(p-1)} \Rightarrow (X^\alpha)^\beta = X^1 (X^{k(p-1)})^{q-1}$ ou $(X^\alpha)^\beta = X^1 (X^{k(q-1)})^{p-1}$.

Mas sabe-se que $X \equiv X \mod p$ e $X \equiv X \mod q$.

Além disso p e q são primos, logo $(X^{k(q-1)})^{p-1} \equiv 1 \mod p$ e $(X^{k(p-1)})^{q-1} \equiv 1 \mod q$. (teorema 4)

Logo, tem-se que $(X^\alpha)^\beta = X^1 (X^{k(q-1)})^{p-1} \equiv X \mod p$ e $(X^\alpha)^\beta = X^1 (X^{k(p-1)})^{q-1} \equiv X \mod q$. Logo, pelo teorema 5, tem-se que $Y^\beta \equiv X^\alpha)^\beta \equiv X \mod pq$.

Portanto, depois de obter β, G só precisa calcular o resto da divisão de Y^β por N.

7. Considerações finais

A apresentação da evolução histórica da criptografia e do funcionamento dos sistemas DHM e RSA permitem o desenvolvimento de uma série de atividades lúdicas com alunos da escola básica de diversos níveis que, além de fundamentações matemáticas importantes, permitem associações interessantes e o desenvolvimento do raciocínio lógico. Questões sobre mensagens sigilosas usando as cifras de substituição ou que envolvam a aritmética do relógio ou dos calendários são alguns exemplos interessantes que podem ser trabalhados desde as séries inciais do fundamental II e permitem propostas criativas e inovadoras. Além disso, a aritmética modular propicia uma riqueza de questões mais elaboradas envolvendo o estudo de números primos, a codificação e decodificação de mensagens, números binários, divisibilidade e diversos outros temas que podem ser entrelaçados e organizados de forma contemporânea e significativa para o alunado.

Convidamos o leitor a consultar o texto original (SILVA,2016) para que possa observar algumas atividades construídas nesse sentido e, especialmente, analisar a visão dos alunos frente às propostas pedagógicas que puderam ser aplicadas.

Embora a criptografia seja uma realidade do mundo moderno e tema constante de estudos e publicações, ainda é assunto desconhecido por grande parte dos alunos da educação básica. No entanto, a simples introdução de conceitos básicos do tema gera motivação, interesse e envolvimento dos alunos. O presente trabalho, então, pretende ser mais uma semente para que projetos engenhosos e transformadores estejam cada vez mais presentes na sala de aula da educação básica.

Referências

[1] Coutinho, Severino. *Criptografia*. Rio de Janeiro, Impa, 2015.

[2] Hefez, Abramo. *Aritmética*. Coleção Profmat. Rio de Janeiro, Editora SBM, 2013.

[3] Silva, Igor Nascimento da. *Criptografia na Educação Básica: das escritas ocultas ao código RSA*. Dissertação de Mestrado. Rio de Janeiro: PUC-Rio, 2016. Disponível em https : //sca.profmat−sbm.org.br/sca$_v$2/get$_t$cc3.php?id = 94676. Acesso em 13 set. 2018.

[4] Singh, Simon. *O Livro dos Códigos*. São Paulo, Editora Record, 2007.

Igor Nascimento da Silva
Escola Municipal Joaquim da Silva Gomes
<igor_etfq@yahoo.com.br>

Christine Sertã Costa
Pontifícia Universidade Católica do Rio de Janeiro
Colégio Pedro II
<cserta@globo.com>

Recebido: 15/08/2019
Publicado: 10/04/2020