Pontifícia Universidade Católica
do Rio de Janeiro

Igor Nascimento da Silva

Criptografia na educação básica: das escritas ocultas ao código RSA

Dissertação de Mestrado

Dissertação apresentada ao Programa de Pós-graduação em Matemática da PUC-Rio como requisito parcial para obtenção do título de Mestre em Matemática (opção profissional).

Orientadora: Profa. Christine Sertã Costa

Rio de Janeiro

Junho de 2016

Pontifícia Universidade Católica
do Rio de Janeiro

Igor Nascimento da Silva

Criptografia na educação básica: das escritas ocultas ao código RSA

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Matemática do Departamento de Matemática do Centro Técnico Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Profa. Christine Sertã Costa
Orientador
Departamento de Matemática – PUC-Rio

Prof. Sinésio Pesco
Departamento de Matemática – PUC-Rio

Profa. Patrícia Erthal de Moraes
Colégio Pedro II

Profa. Renata Martins da Rosa
Departamento de Matemática – PUC-Rio

Prof. Márcio da Silveira Carvalho
Coordenador Setorial do Centro
Técnico Científico – PUC-Rio

Rio de Janeiro, 28 de junho de 2016

Igor Nascimento da Silva

Graduou-se em Licenciatura em Matemática pela Universidade do Estado do Rio de Janeiro (UERJ) em 2005. Atualmente professor da rede municipal de ensino do Rio de Janeiro.

Ficha Catalográfica

Silva, Igor Nascimento da

Criptografia na educação básica: das escritas ocultas ao código RSA / Igor Nascimento da Silva; orientadora: Christine Sertã Costa. – 2016.

59 f. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Matemática, 2016.

Inclui bibliografia

1. Matemática – Teses. 2. Aritmética modular. 3. Criptografia na educação básica. 4. RSA. I. Costa, Christine Sertã. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Matemática. III. Título.

CDD: 510

Dedico esta dissertação à minha família que sempre esteve presente e me apoia em todos os meus projetos. Em especial aos meus filhos, Gabriela e Matheus, que com seus sorrisos me alegram a cada dia.

Agradecimentos

A Deus por ter me dado força e saúde durante esta jornada.

Aos meus pais por me darem a melhor educação que eles puderam. Tudo que alcancei até hoje devo a eles.

À minha esposa que me apoiou desde o exame de acesso até o final do curso, me dando suporte para conseguir vencer os momentos mais difíceis desta caminhada.

À direção da Escola Municipal Joaquim da Silva Gomes por facilitar a realização da oficina.

Aos alunos que participaram da oficina de forma voluntária. Sem eles o trabalho ficaria comprometido.

À minha orientadora pela paciência, por estar sempre disposta a ajudar e pelas respostas rápidas.

Aos colegas de turma pelos bons momentos que passamos durante o curso e pelas palavras de incentivo nos momentos mais difíceis.

A toda equipe do PROFMAT por ter dividido seus conhecimentos conosco da melhor forma possível.

A CAPES e à PUC–Rio pelo auxílio que foi fundamental para a conclusão do mestrado.

Resumo

Silva, Igor Nascimento da; Costa, Christine Sertã (Orientadora). **Criptografia na educação básica: das escritas ocultas ao código RSA.** Rio de Janeiro, 2016. 59p. Dissertação de Mestrado - Departamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro.

Essa dissertação se propõe a introduzir nas aulas de matemática da escola básica um tema que traga significado e interesse ao alunado e que, a partir dele, seja possível desenvolver conteúdos novos e clássicos da disciplina, pertinentes a esse nível de escolaridade. O tema escolhido foi a criptografia que 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. 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 diversos 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

Silva, Igor Nascimento da; Costa, Christine Sertã (Advisor) **Encryption in basic education: from the hidden code written to RSA.** Rio de Janeiro, 2016. 59p. MSc Dissertation – Departamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro.

This dissertation proposes to introduce in the math class of the elementary school a theme that brings meaning and interest to the students and, from it, it is possible to develop new and classic content, relevant discipline at this level of education. The theme chosen was the encryption that made possible the development of a historical approach of its development until the RSA code, the promotion of discussions on the current relevance of the subject until our days and working with important content of mathematics. In order to improve and evaluate the proposal, a small application in a public school was made, through a workshop, with results quite satisfactory. It is intended that this work is more a source to assist several teachers in the construction of new pedagogical proposals adapted to the reality of each classroom with motivating, meaningful and contemporary look.

Keywords

Modular arithmetic; Encryption in basic education; RSA.

Sumário

Lista de figuras

1
Introdução

Um questionamento muito comum dos alunos da educação básica é: “qual a aplicação desta matéria?”. Procurar um tema atual que trouxesse significância para os alunos foi um dos desafios do presente trabalho. Com esse olhar, criptografia foi o tema escolhido uma vez que possibilita o desenvolvimento de muitas aplicações importantes do cotidiano, permite o desenvolvimento de conteúdos matemáticos interessantes e possíveis de serem desenvolvidos na escola básica além de ser um assunto com avanços significativos e relevantes na história mundial. Todos esses fatores, acreditamos, despertam o interesse dos alunos e os aproxima da Matemática.

A maioria dos alunos da educação básica desconhece o significado da palavra criptografia, mas ficam curiosos sobre o tema assim que ele é apresentado. Além disso, sempre conhecem algum exemplo de filme ou livro que de alguma forma enfocam este conteúdo. Fazer uso dessas aproximações facilita o trabalho do professor e amplia o arcabouço tanto cultural como acadêmico do aluno.

Para trabalhar a criptografia, outros tópicos que também não constam do currículo escolar podem e precisam ser abordados. É o caso da aritmética modular. Esse assunto inclusive já apareceu em alguns concursos que só exigem o ensino fundamental, tais como provas de seleção para o colégio naval e para o colégio militar, e, certamente seu conhecimento facilitaria a resolução de algumas dessas questões. Cabe ressaltar que a introdução deste conteúdo é absolutamente pertinente e viável na educação básica além de poder auxiliar e dar significado, por exemplo, ao estudo de sistemas de numeração, de critérios de divisibilidade, de estudos de números primos e de resolução de equações, temas que fazem parte do currículo mínimo da escola básica.

Destacamos também que, no ensino fundamental, o aluno estuda sistemas de numeração, e, entre eles tem destaque o sistema binário. Operações básicas neste sistema e procedimentos para mudanças de base são algumas vezes trabalhados, porém, estes cálculos parecem não ter utilidade para o aluno, pois, ao

longo de toda a sua trajetória na educação básica ele não utiliza mais este conteúdo e nem percebe sua aplicabilidade. Mais uma vez, a criptografia pode dar sentido a esses aprendizados. Atualmente, na maior parte das vezes, apenas os alunos que optam por cursos voltados à informática têm algum contato com essas aplicações sendo apresentado à tabela ASCII[1], que também será abordada ao longo desse trabalho.

O fato de se comunicar com alguém de forma que uma terceira pessoa não consiga compreender o significado da mensagem e a notória fascinação desta geração pela tecnologia desperta o interesse e curiosidade dos adolescentes pelo assunto e possibilita um solo fértil para a aprendizagem. No presente trabalho sugerimos diferentes técnicas para enviar uma mensagem criptografada, pontuando onde estão as falhas de algumas delas e trazemos o assunto para a atualidade destacando que, no nosso cotidiano, estamos sempre utilizando a criptografia quando utilizamos a internet.

Assim esse trabalho apresenta a evolução da criptografia até o surgimento do código RSA e constrói uma proposta de aplicação dos fundamentos e funcionamentos deste código, de forma superficial, para alunos da educação básica. O estudo de aritmética modular e uma breve explanação sobre a tabela ASCII servem de base para os desenvolvimentos apresentados. A proposta de aplicação construída foi feita numa escola pública do estado do Rio de Janeiro e os resultados, muito satisfatórios. É claro que os exemplos apresentados foram simples, mas debates importantes como a questão de fatoração de números bem grandes e o uso de computadores puderam ser realizados levando os alunos participantes a se aproximarem mais da realidade. Todo o trabalho foi construído tentando estimular no discente o pensamento lógico matemático e fornecendo embasamento teórico e repertório para que ele construa suas próprias argumentações e conclusões.

[1]American Standard Code for Information Interchange (Código Padrão Americano para o Intercâmbio de Informação).

2
Contexto histórico

Segundo SINGH (2007), um dos primeiros relatos de escrita oculta foi encontrado no livro *As histórias* de Heródoto (485 a.C – 420 a.C), onde são narrados conflitos entre a Grécia e a Pérsia. Neste livro Heródoto conta que Demarato, um grego que teria sido expulso de sua terra natal, sabendo dos planos de uma possível invasão de Xerxes[2] à Grécia, mandou uma mensagem raspando a cera de um par de tabuletas, escreveu os planos de Xerxes na madeira e em seguida cobriu novamente com cera, assim sua mensagem chegou aos gregos de forma segura, deixando-os preparados para a invasão. Demarato utilizou um artifício para ocultar a mensagem fisicamente, qualquer artifício que tenha esta característica recebe o nome de *esteganografia*, derivado do grego *steganos*, que significa coberto, e *graphein*, que significa escrever. Com o estudo da criptografia, do grego *kriptos*, que significa oculto, as mensagens não precisavam mais ser ocultadas fisicamente, bastava usar alguma estratégia para que a mensagem fosse enviada ao destinatário de forma que, quando lida por uma terceira pessoa, não fizesse sentido algum, ficando assegurado que apenas o remetente e o destinatário conseguissem entender o teor da mensagem original. Podemos dividir a criptografia em dois ramos, a transposição e a substituição.

2.1
Transposição

Na transposição as letras são misturadas formando anagramas, sendo assim, em uma palavra curta é simples descobrir a palavra original a partir de um anagrama, porém quando se trata de textos longos, torna-se praticamente impossível a sua decifragem. Porém há um problema, as letras não podem ser misturadas ao acaso, senão, nem mesmo o destinatário, que deveria compreender

[2] Xerxes (518 a.C – 465 a.C) foi imperador Persa, de 486 a.C até a data de seu assassinato.

a mensagem, conseguirá decifrá-la. Assim, o padrão do rearranjo das letras deve ser algo previamente combinado.

Há um padrão conhecido como "cerca de ferrovia", que consiste em escrever as letras da mensagem de forma alternada em duas linhas, ou seja, a primeira letra na primeira linha, a segunda letra na segunda linha, a terceira letra na primeira linha e assim sucessivamente. A mensagem cifrada é escrita com as letras da primeira linha seguida das letras da segunda linha. Veja um exemplo:

Mensagem original: **VOU ME ATRASAR UM POUCO**

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

Mensagem cifrada: **VUETAAUPUOOMARSRMOC**

Outra forma utilizada para enviar mensagens utilizando a transposição era o uso do *citale espartano*, que consiste em um bastão de madeira, onde era enrolada uma fita de couro. Nesta fita a mensagem era escrita ao longo do comprimento do bastão. Quando a fita fosse desenrolada, as letras estariam misturadas e poderia ser levada ao destinatário. Para decifrar a mensagem o destinatário deveria possuir um *citale* idêntico ao do remetente, então bastava enrolar a fita em seu *citale* e o texto original aparecia escrito para ele. Na *Figura 1* temos um exemplo deste equipamento, onde parte do texto original é **SEND MORE TROOPS TO SOUTHERN FLANK AND[3],** cuja mensagem cifrada é **STSF**... .

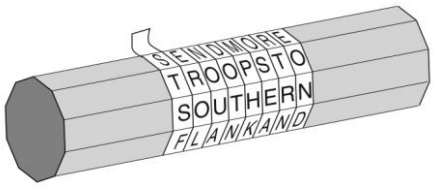


Figura 1 – Citale espartano.
(Fonte: Singh, 2007, p.24).

[3]Tradução: Enviar mais tropas ao sul do flanco e.

Uma alternativa para a transposição é a substituição. Segundo SINGH (2007), uma das primeiras descrições desta categoria data do século IV a.C no Kama-sutra, livro escrito pelo indiano Vatsyayana[4]. O Kama-sutra recomenda que as mulheres devam estudar 64 artes, entre elas a escrita secreta, para ajudá-las a esconder os detalhes de seus relacionamentos e uma das técnicas recomendadas é a substituição simples. A seguir descreveremos alguns métodos de substituição.

2.2
Cifra de César

A substituição simples consiste em trocar cada letra da mensagem original por outra letra do alfabeto, seguindo um padrão. Na Roma antiga este método foi muito utilizado por Júlio César[5] e ficou conhecido como *cifra de César*, onde cada letra da mensagem original era substituída pela letra correspondente na linha abaixo da tabela, como mostra a *Figura 2*. Observe que César utilizava um deslocamento de 3 posições no alfabeto para cifrar suas mensagens, porém o padrão a ser seguido pode ser outro, desde que seja de conhecimento do destinatário. A seguir, um exemplo do uso da cifra de César:

Mensagem original: **ATACAR AO MEIO DIA**

Mensagem cifrada: **DWDFDU DR PHLR GLD**

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*

Figura 2 – Cifra de César.
(Fonte: Hefez, 2013, p.311).

A principal fraqueza deste método é que com uma simples análise de frequência das letras do idioma e um bom conhecimento da sua estrutura, uma pessoa consegue decifrar a mensagem. No caso do português, por exemplo, sabemos que a letra **Q** sempre vem seguida da letra **U** e, segundo a análise de

[4] Filósofo indiano que viveu entre os séculos IV e VI antes de Cristo.

[5] Ditador da República Romana de 49 a.C a 44 a.C.

frequência das letras, a letra **A** é a que aparece com maior frequência no nosso idioma (veja a tabela completa na *Figura 3*).

Letra	Freq.%	Letra	Freq.%
A	14.63	N	5.05
B	1.04	O	10.73
C	3.88	P	2.52
D	4.99	Q	1.20
E	12.57	R	6.53
F	1.02	S	7.81
G	1.30	T	4.34
H	1.28	U	4.63
I	6.18	V	1.67
J	0.40	W	0.01
K	0.02	X	0.21
L	2.78	Y	0.01
M	4.74	Z	0.47

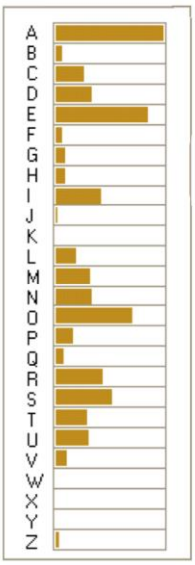


Figura 3 – Tabela de frequência das letras do nosso alfabeto.
(Fonte: http://www.numaboa.com.br/criptologia).

Ainda segundo SINGH(2007), no século XVI a rainha da Escócia Maria Stuart (1542 – 1587) planejava matar sua prima, a rainha Elizabeth I da Inglaterra. Ela enviava mensagens para seus aliados substituindo letras e algumas palavras recorrentes por símbolos. Devido à fragilidade do método já citada anteriomente, as mensagens foram interceptadas e decifradas servindo como prova contra a rainha da Escócia, que acabou condenada à morte por decaptação.

2.3
Disco de Alberti

Conhecido como pai da criptologia ocidental, o arquiteto italiano *Leone Battista Alberti*, em 1466, criou um sistema de substituição polialfabética. Nesse sistema não era usado apenas um alfabeto cifrado, uma letra poderia ser cifrada de diferentes formas. Sendo assim, este método era mais seguro que a cifra de César ou qualquer outro método de substituição monoalfabética conhecido. O sistema consistia no uso de um objeto chamado *disco de Alberti* (F*igura 4*), que era formado por dois discos concêntricos com diâmetros distintos presos por um pino central, sendo que o disco menor era móvel e o disco maior, fixo. Ambos eram divididos em 24 setores iguais distribuídos da seguinte forma: no disco maior, no

sentido horário, eram escritas as 20 letras A, B, C, D ,E ,F ,G, I, L, M, N, O, P, Q, R, S, T, V, X, Z e os numerais 1, 2, 3, 4 e no disco menor, em ordem aleatória, as letras minúsculas do alfabeto (exceto as letras j, u e w) mais a palavra do latim *et* (que significa e).

Para utilizar o sistema o remetente e o destinatário devem possuir discos idênticos e a partir de uma posição previamente determinada do disco, por exemplo a letra **V** do disco maior alinhada com a letra **c** do disco menor, cada letra da mensagem original no disco maior é substituída pela sua correspondente no disco menor. Os numerais servem para inserir na mensagem original números entre 11 (inclusive) e 4444 (inclusive), utilizando apenas os algarismos constantes no disco, ou seja, 336 números onde cada um representa uma palavra ou frase contida em um dicionário de códigos previamente produzido em duas cópias, estes números são cifrados de acordo com a posição préviamente determinada dos discos. A fim de obter mais segurança nas mensagens, a cada grupo de algumas palavras o disco é girado aleatoriamente e a nova letra, no disco menor, correspondente à letra **V** do disco maior, que foi nosso exemplo, é inserida no texto indicando que esta é a nova posição do disco menor em relação ao disco maior, a ser seguida.

Suponha que deseja-se mandar a seguinte mensagem **MATAR O REI LOGO**, utilizando o disco da *Figura 4* na posição citada no parágrafo anterior. Suponha ainda que, no dicionário de códigos, a palavra REI é representada pelo numeral 124. No exemplo não utilizaremos a técnica de girar o disco aleatoremente para determinar uma nova posição. Assim a mensagem cifrada é **tsosb n yam gngn**.

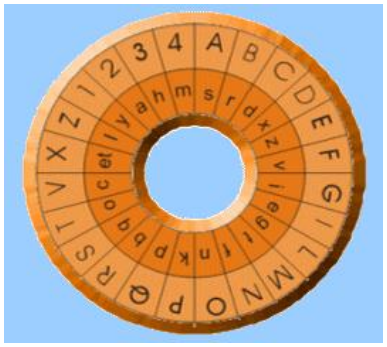


Figura 4 – Disco de Alberti.
(Fonte: http://www.rexposta.com.br).

2.4
Tabula recta

Johannes Trithemius foi um alemão que viveu de 1462 a 1516 e, em seu livro, *Poligrafia*, que só foi publicado em 1518, propõe um novo sistema de codificação que seria um grande passo para a criptografia. Neste sistema as mensagens são cifradas utilizando a *tabula recta*, que é 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, como mostra a *Figura 5*. A cifragem de uma mensagem procedia da seguinte forma: o alfabeto da primeira linha serve como referência para as substituições, sendo assim 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 até chegar à última linha onde, na próxima letra retorna para a segunda linha. Segue um exemplo:

Mensagem original: **CHEGO NA SEGUNDA**

Mensagem cifrada: **DJHKT TH ANQFZQO**

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

Figura 5 – Tabula recta

(Fonte: Elaborada pelo autor)

2.5
Cifra de Vigenère

Antes de falarmos da cifra de Vigenère propriamente dita vamos dar crédito ao italiano *Giovanni Battista Bellaso*, que em 1553, no livro *La cifra del Sig Giovan Batista Belaso*, acrescenta ao método anterior o uso de uma chave que é usada para cifrar e decifrar a mensagem. Se uma pessoa deseja mandar uma mensagem para outra, eles devem compartilhar uma chave que pode ser uma letra, uma palavra ou até mesmo uma frase. A cifragem da mensagem é descrita da seguinte forma: escreve-se a mensagem e acima se escreve a chave, letra sobre letra, repetindo-se essa chave tantas vezes quantas sejam necessárias. Na tabula recta a primeira linha representa as letras da chave e a primeira coluna representa as letras da mensagem original, sendo assim cada letra é substituída pela letra correspondente na coluna que se encontra a letra da chave e na linha que se encontra a letra da mensagem, fazendo uma analogia com pares ordenados obtemos: **letra cifrada = (letra da chave; letra da mensagem original)**. Para decifrar a mensagem basta fazer o caminho inverso. Por exemplo, suponhamos que uma pessoa queira mandar a mensagem **MATEM A RAINHA** para outra e ambos compartilham da chave **morte**:

Chave	m	o	r	t	e		m		o	r	t	e	m	o
Mensagem original	M	A	T	E	M		A		R	A	I	N	H	A
Mensagem cifrada	**Y**	**O**	**K**	**X**	**Q**		**M**		**F**	**R**	**B**	**R**	**T**	**O**

A grande revolução do método proposto por Bellaso era o uso da chave, dificultando assim que outra pessoa que não saiba qual é a chave consiga decifrar a mensagem mesmo utilizando técnicas de análise de frequência e estrutura do idioma.

Em 1586, o Francês *Blaise Vigenère*, com base nos estudos de Alberti e Trithemius, publicou no livro *Traicté des Chiffe* o método proposto por Bellaso que ficaria conhecido como sistema de Vigenère e no mesmo livro apresentou o conceito da autochave. Este conceito tem o seguinte funcionamento: cada correspondente compartilha uma chave que é uma letra, esta chave é utilizada para cifrar a primeira letra da mensagem, utilizando o método já descrito proposto por

Bellaso, a primeira letra da mensagem original é a chave para cifrar a segunda e assim sucessivamente, conforme o exemplo a seguir.

Suponha que um general deseje mandar a mensagem **ATACAR HOJE** para um de seus oficiais, sabendo que a chave escolhida é a letra **b**. Assim a mensagem cifrada fica **BTTCCR YVXN**.

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**

Este sistema não foi muito utilizado não só por ser extremamente trabalhoso para decifrar mensagens longas, mas também porque se um erro fosse cometido na cifragem, a recuperação da mensagem ficava muito comprometida.

Por aproximadamente 300 anos a cifra de Vigenère foi considerada inquebrável, mas no século XIX o inglês Charles Babbage mostrou que a fraqueza do sistema está na periodicidade que o uso da chave acarreta em mensagens muito longas, assim era possível descobrir a chave e consequentemente decifrar a mensagem.

2.6
Criptografia na segunda guerra mundial

Durante a segunda guerra mundial as cifras polialfabéticas foram de bastante utilidade para a construção das máquinas cifradoras, entre elas a japonesa Purple e as alemães Enigma, inspirada no disco de Alberti, e a Lorenz SZ40. A Purple e a Enigma operavam de formas parecidas, mas a Lorenz SZ40 era mais complicada e tida como mais difícil de ter seu código quebrado. Nesta época havia um grande esforço em construir máquinas decifradoras, para isso os britânicos contaram com a ajuda de um dos pais da computação, Alan Turing, que ajudou a decifrar as mensagens da Enigma. Parte da inspiração de Alan Turing veio dos trabalhos realizados por Marian Rejewski, um jovem matemático polonês que durante a década de 1930 se empenhou em quebrar a cifra da máquina Enigma, obtendo sucesso, porém nos anos posteriores a máquina foi aperfeiçoada dificultando, mas não tornando impossível, o trabalho dos criptoanalistas. Os

estudos de Alan Turing serviram de base para que a cifra Lorenz fosse quebrada. Em 1943 ficava pronta a máquina Colossus que quebrou a cifra Lorenz e se tornaria o percursor do computador digital. Mas, com o fim da guerra, a máquina Colossus e seu projeto foram destruídos e todos os envolvidos no projeto foram proibidos de dar qualquer depoimento sobre o assunto.

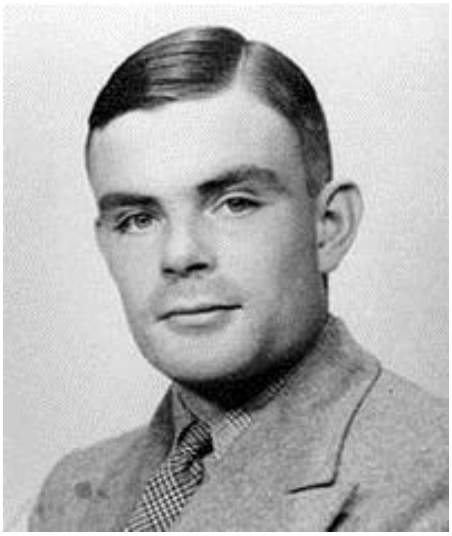


Figura 6 – Alan Turing.
(Fonte: https://pt.wikipedia.org).

2.7
O problema da troca das chaves

Todas estas máquinas trabalhavam com o uso de chaves simétricas, ou seja, a mesma chave que é usada para cifrar as mensagens é usada para decifrar e o principal empecilho por muito tempo no estudo 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 é uma tarefa simples, ou deveria delegar esta tarefa à outra pessoa, o que nem sempre é seguro.

Graças à persistência de Whitfield Diffie, Martin Hellman e Ralph Merkle foi apresentada uma solução para este problema.

Whitfield Diffie, um matemático graduado em 1965 no Massachusetts Institute of Technology, tinha a certeza que quem descobrisse a solução de tal problema entraria para a história. Em 1974 Diffie foi convidado para dar uma palestra sobre suas estratégias para lidar com a questão da distribuição das chaves

no laboratório Thomas J. Watson da IBM, onde Alan Konhein, um dos principais especialistas em criptografia da IBM trabalhava. Nesta ocasião, Alan contou a Diffie que Martin Hellman, um professor da Universidade de Stanford na Califórnia, havia visitado o laboratório para abordar esta mesma questão. Diffie então procurou Hellman e ambos passaram a trabalhar juntos na busca da solução do problema da distribuição das chaves. Mais tarde esta parceria ainda receberia a adesão de Ralph Merkle, um matemático vindo de um grupo que não simpatizava com o sonho de resolver esta questão aparentemente impossível.

O trio buscou atacar o problema procurando uma função de mão única, ou seja, uma função matemática que é facilmente calculada, mas a sua reversão é uma tarefa muito mais complicada, ou até mesmo impossível. Em 1976, Hellman percebeu que a aritmética modular poderia ser uma solução para a sua procura, e, quando apresentou os resultados obtidos a seus companheiros, esses prontamente reconheceram que a questão da distribuição das chaves estava solucionada.

O sistema ficou conhecido como DHM, em homenagem aos seus criadores, e a sua simplicidade é espantosa, como veremos mais adiante.

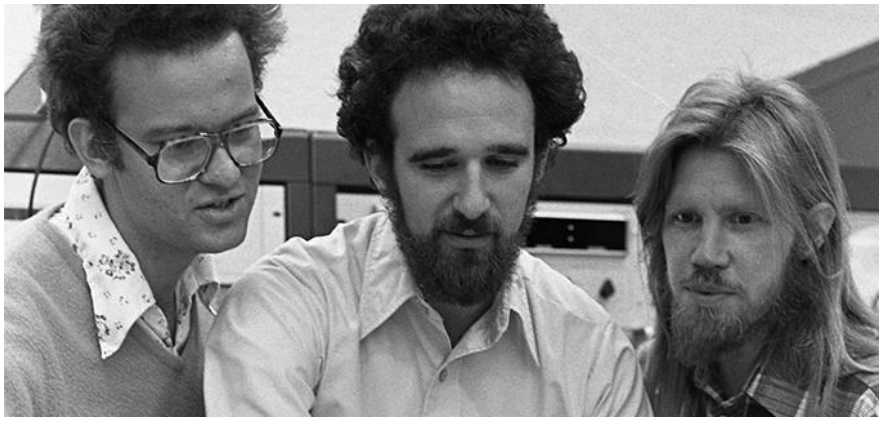


Figura 7 – Ralph Merkle, Martin Hellman e Whitfield Diffie (da esquerda para a direita). (Fonte: http://engineering.stanford.edu).

2.8
O surgimento do RSA

Embora Diffie, Hellman e Merkle tivessem solucionado o problema da distribuição das chaves, fato que revolucionou o estudo da criptografia, o sistema não era prático e ainda trabalhava com chaves simétricas. No capítulo 4, quando

for mostrada a matemática que envolve o DHM, veremos mais claramente as suas deficiências.

As descobertas de Diffie, Hellman e Merkle encorajou outro trio a solucionar a questão das chaves assimétricas. Ron Rivest, Leonard Adleman e Adi Shamir eram pesquisadores do laboratório de ciência da computação do Massachusetts Institute of Technology e também buscavam uma função de mão única que resolvesse esta questão. Ron Rivest e Adi Shamir eram dois cientistas da computação que formularam várias ideias, mas o matemático Leonard Adleman logo encontrava falhas e as derrubava. Porém, em 1977 Rivest teve uma espécie de visão, já era tarde da noite quando ele começou a formular suas ideias, uma função de mão única baseada na aritmética modular que aparentemente tinha as características necessárias para o funcionamento da chave assimétrica. Quando amanheceu Rivest entregou o trabalho para Adleman que por sua vez tentou encontrar falhas como fez em todos os outros casos, mas desta vez não as encontrou. O sistema RSA, em homenagem a seus criadores, surgia e se tornaria a cifra mais influente da criptografia moderna.

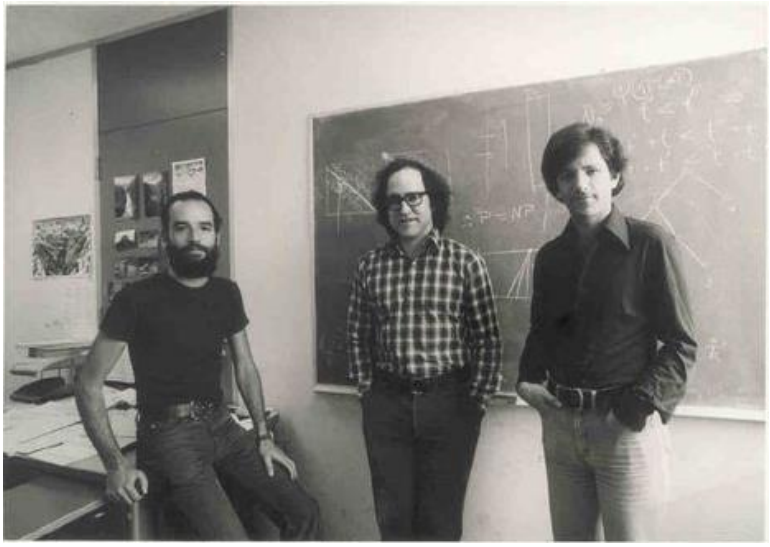


Figura 8 – Adi Shamir, Ron Rivest e Leonard Adleman (da esquerda para a direita). (Fonte: https://chessprogramming.wikispaces.com).

O RSA ficou conhecido como criptografia de chave pública, onde parte desta chave é um número N, cujo valor é obtido pelo produto de dois números primos bem grandes, p e q. Neste caso, o valor do N pode ser divulgado amplamente, pois esta 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. Teoricamente, conhecendo o valor de N é fácil deduzir os valores de p e q, mas na prática 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. Os detalhes do funcionamento do RSA serão vistos do capítulo 4.

3
Aritmética Modular

Neste capítulo abordaremos o conceito de aritmética modular, alguns teoremas que são importantes para o objetivo do trabalho e apresentaremos algumas questões de concursos que podem ser resolvidas utilizando a aritmética modular.

3.1
Definição

Dizemos que dois números inteiros a e b são congruentes módulo m, onde m é um número natural, se a e b deixam o mesmo resto na divisão euclidiana por m. Quando os inteiros a e b são congruentes módulo m utilizamos a seguinte notação:

$$a \equiv b \bmod m$$

Exemplo: $15 \equiv 7 \bmod 4$, pois:

- $15 = 4.3 + 3$
- $7 = 4.1 + 3$

Obviamente $m \neq 0$, pois não faz sentido falarmos em divisão euclidiana por zero. Também vamos considerar $m \neq 1$, pois como o resto da divisão de qualquer número inteiro por 1 é zero, então $a \equiv b \mod 1$, quaisquer que sejam os números inteiros a e b.

A congruência é uma relação de equivalência sobre Z já que, para $m > 1$ natural e a, b, c inteiros, tem-se que a congruência satisfaz as propriedades:

(i) $a \equiv a \bmod m$ (Reflexiva)

(ii) Se $a \equiv b \bmod m$ então $b \equiv a \bmod m$ (Simétrica)

(iii) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$ então $a \equiv c \bmod m$ (Transitiva)

Demonstração:

(i) Trivial.

(ii) Pela hipótese a e b deixam o mesmo resto na divisão por m, então, pela definição, $b \equiv a \bmod m$. ■

(iii) Seja r o resto da divisão euclidiana de a e b por m, como pela hipótese $b \equiv c \bmod m$, então, pela definição, c deixa também resto r na divisão por m, logo $a \equiv c \bmod m$ ■

3.2
Proposições

Para as proposições a seguir e suas demonstrações utilizaremos a notação m | a, com **m** e **a** números inteiros, quando **m** dividir **a**.

Proposição 1: Sejam **a** e **b** números inteiros e **m** um número natural, m > 1, $a \equiv b \bmod m$ se, e somente se, m | a – b.

Demonstração:

Da divisão euclidiana de a e b por m tem-se:

a = m.q + r, $0 \leq r < m$ e b = m.q`+ r`, $0 \leq r` < m$.

Então a – b = m.(q – q`) + (r – r`).

(=>) Se $a \equiv b \bmod m$, então m | a – b.

Pela hipótese a e b deixam o mesmo resto na divisão por m, então r = r`. Logo r – r`= 0. Portanto a – b = m.(q – q`), ou seja, m | a – b. ■

(<=) Se m | a – b, então $a \equiv b \bmod m$.

Sabe-se que a – b = m.(q – q`) + (r – r`).

Pela hipótese m | a – b, então r – r`= 0, ou seja, r = r`. Portanto se os restos das divisões de a e b por m são iguais, então $a \equiv b \bmod m$. ■

Um dos fatores que tornam a congruência uma poderosa ferramenta na matemática é o fato de ela ser uma relação de equivalência compatível com as operações de adição e multiplicação no conjunto dos números inteiros, conforme as propriedades a seguir.

Sejam a, b c, d, m números inteiros, com m > 1

Proposição 2: Se $a \equiv b \bmod m$, então $a + c \equiv b + c \bmod m$.

Demonstração:

Pela hipótese tem-se que $a \equiv b \bmod m$. Então, pela proposição 1,

m | a – b, ou seja, a – b = m.q (1).

Somando e subtraindo c no lado esquerdo de (1), tem-se:

(a + c) – (b + c) = m.q.

Então m | (a + c) – (b + c) e, portanto, pela proposição 1, $a + c \equiv b + c \bmod m$. ■

Proposição 3: Se $a \equiv b \bmod m$, então $ac \equiv bc \bmod m$.

Demonstração:

Assim como na demonstração anterior, sabe-se que m | a – b.

Então m | c.(a – b), mas c.(a – b) = ac – bc.

Portanto, pela proposição 1, $ac \equiv bc \bmod m$. ■

Proposição 4: Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

Demonstração:

Pela hipótese e pela proposição 1, tem-se que m | a – b e m | c – d.

Então m | (a – b) + (c – d), logo m | (a + c) – (b + d) e, portanto, pela proposição 1, $a + c \equiv b + d \bmod m$. ■

Proposição 5: Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.

Demonstração:

Como vimos na demonstração da proposição 4, m | (a – b) e m | (c – d).

Então m | c.(a – b) e m | b.(c – d) como consequência m | c.(a – b) + b.(c – d), mas c.(a – b) + b.(c – d) = ac – bd.

Portanto, pela proposição 1, se m | ac – bd , então $ac \equiv bd \bmod m$. ■

Proposição 6: Sejam **a** e **b** números inteiros e **n** um número natural, se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$

Demonstração:

A demonstração deste teorema se dá por indução finita em n.

(i) Caso base: n = 1

$a \equiv b \bmod m \Rightarrow a^1 \equiv b^1 \bmod m$

(ii) Se $a^n \equiv b^n \bmod m$, então $a^{n+1} \equiv b^{n+1} \bmod m$

Pela hipótese de indução, $a^n \equiv b^n \bmod m$, então, usando o caso base e a proposição 5, $a^n.a \equiv b^n.b \bmod m$, ou seja, $a^{n+1} \equiv b^{n+1} \bmod m$. ■

Antes das próximas proposições é importante deixar claro que será utilizada a notação (a,b) para o máximo divisor comum dos números inteiros **a** e **b**.

Proposição 7: Sejam **a**,**b**,**c**,**m** números inteiros, com m > 1. Temos que $ac \equiv bc \bmod m$ se, e somente se, $a \equiv b \bmod \frac{m}{(c,m)}$.

Demonstração:

Sabemos que $\frac{c}{(c,m)}$ e $\frac{m}{(c,m)}$ são coprimos, ou seja, $\left(\frac{c}{(c,m)}, \frac{m}{(c,m)}\right) = 1$.

Pela proposição 1, $ac \equiv bc \bmod m \Leftrightarrow m \mid ac - bc \Leftrightarrow m \mid c.(a - b) \Leftrightarrow$

$\Leftrightarrow \frac{m}{(c,m)} \mid \frac{c}{(c,m)}.(a - b) \Leftrightarrow \frac{m}{(c,m)} \mid (a - b) \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}$. ■

Sejam os inteiros **a** e **b**. Definimos o conjunto I(a,b) = {xa + yb}, onde **x** e **y** são números inteiros quaisquer, ou seja, o conjunto das combinações lineares de coeficientes inteiros de **a** e **b**.

Lema 1: Sejam os inteiros **a** e **b**, não ambos nulos. Se **d** é o menor número natural que pertence a I(a,b), então d = (a,b).

Demonstração:

Suponha que exista um número natural **c** que divida **a** e **b**, logo **c** divide xa + yb, quaisquer que sejam os inteiros **x** e **y**. Portanto c divide todos os elementos de I(a,b), então c | d.

Suponha por absurdo que **d** não divide **w**, onde $w \in$ I(a,b). Pela divisão euclidiana temos que w = d.q + r, onde 0 < r < d.

Como w = xa + yb e d = ma + nb, onde **x**, **y**, **m** e **n** são números inteiros, então: r = xa – mqa + yb – nqb, ou seja, r = (x – mq)a + (y – nq)b.

Concluímos que $r \in$ I(a,b), o que é um absurdo, pois r < d, mas d é o menor número natural que pertence a I(a,b). Portanto d divide todos os elementos de I(a,b). Em particular d | a e d | b.

Logo, se para todo divisor comum c de a e b temos que c | d, pela definição de mdc d = (a,b).■

Dados os inteiros **a**, **b** e **c**, definimos como uma equação diofantina linear toda equação do tipo ax + by = c.

Lema 2: Dois números **a** e **b** são coprimos se, e somente se, existem números inteiros **x** e **y** tais que xa + yb = 1.

Demonstração:

Seja d = (a,b).

(=>)

Pelo lema 1, podemos escrever **d** como combinação linear de **a** e **b**, ou seja, existem dois inteiros x e y, tais que xa + xb = d, mas pela hipótese (a,b)= d = 1.

Então existem x e y inteiros tais que xa + yb = 1. ■

(<=)

Temos que d divide xa + yb, mas pela hipótese xa + yb = 1. Então d | 1, portanto d = 1. ■

Proposição 8: Sejam **a** e **m** números inteiros, com m > 1. A congruência $aX \equiv 1 \bmod m$ possui solução se, e somente se, (a,m) = 1. Além disso, se x_0 é uma solução inteira, então **x** é uma solução da congruência se, e somente se, $x \equiv x_0 \bmod m$.

Demonstração:

(1ª parte)

Pela proposição 1, $aX \equiv 1 \bmod m$ tem uma solução x_0 se, e somente se, m | a. x_0 - 1, ou seja, a equação diofantina aX – mY = 1 possui solução inteira. Mas, pelo lema 2, isto ocorre se, e somente se, (a,m) = 1. ■

(2ª parte)

(=>)

Se x e x_0 são soluções da congruência $aX \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$ e (a,m) = 1, em virtude da proposição 7, $x \equiv x_0 \bmod m$.

(<=)

Veja que, se x_0 é solução da congruência $aX \equiv 1 \bmod m$ então $ax_0 \equiv 1 \bmod m$ e se $x \equiv x_0 \bmod m$ e (a,m)=1 então, pela proposição 7, $ax \equiv ax_0 \bmod m$, logo x também é solução da mesma congruência, pois $ax \equiv ax_0 \equiv 1 \bmod m$. ■

(Fonte: A. Hefez, *Aritmética*, Coleção PROFMAT, SBM, 2013).

3.2.1
Teorema de Euler

O teorema de Euler, além de ser uma ferramenta muito útil para a demonstração de teoremas importantíssimos como o pequeno teorema de Fermat, é de fundamental importância no estudo da criptografia, servindo com uma das principais argumentações no funcionamento do RSA.

Antes de enunciarmos o teorema devemos ter em mente algumas definições.

- Sistema completo de resíduos

Seja **m** um número inteiro tal que m > 1. O Sistema completo de resíduos módulo m é um conjunto de números que quando divididos por m deixam resto 0, 1, ..., m – 1, sem repetição e em qualquer ordem. Portanto, esse conjunto tem cardinalidade m.

Exemplo: {10,11,0,1,2,3} forma um sistema completo de resíduos módulo 6.

- 0 = 6.0 + 0
- 1 = 6.0 + 1
- 2 = 6.0 + 2
- 3 = 6.0 + 3
- 10 = 6.1 + 4
- 11 = 6.1 + 5

- Sistema reduzido de resíduos

Dado um número inteiro **m** tal que m > 1, chamamos de sistema reduzido de resíduos módulo m um conjunto de números inteiros $\{r_1, r_2, ..., r_s\}$ tais que $(r_i, m) = 1$, para todo i = 1, 2, ..., s e dados dois elementos quaisquer deste conjunto, eles não são congruentes módulo m.

Um sistema reduzido de resíduos módulo m pode ser obtido através do sistema completo de resíduos módulo m retirando, deste último, os elementos que não são primos relativos com m.

Exemplo: Como vimos {10, 11, 0, 1, 2, 3} forma um sistema completo de resíduos módulo 6, então {11, 1} forma um sistema reduzido de resíduos módulo 6, pois (11,6) = (1,6) = 1.

- Função fi de Euler

Denotaremos por φ(m) a quantidade de números naturais entre 0 e m – 1 que são coprimos com m, ou seja, a cardinalidade do sistema reduzido de resíduos módulo m, onde m é um inteiro tal que m > 1.

Exemplo: Como vimos {11,1} é um sistema reduzido de resíduos módulo 6, então φ(6) = 2.

Fazendo φ(1) = 1, podemos definir a função φ: N → N chamada função fi de Euler.

Pela definição, fica claro que φ(m) ≤ m – 1 para todo m ≥ 2 e, ainda mais, φ(m) = m – 1 se, se somente se, m é um número primo.

Demonstração:

Esta prova é direta, pois m é primo se, e somente se, 1, 2, ..., m – 1 forma um sistema reduzido de resíduos módulo m, ou seja, φ(m) = m – 1. ■

Lema 3: Sejam os inteiros **a**, **k**, **m** com m > 1 e (k,m) = 1. Se $\{a_1, a_2, ..., a_m\}$ forma um sistema completo de resíduos módulo m, então $\{a + ka_1, a + ka_2, ..., a + ka_m\}$ também é um sistema completo de resíduos módulo m.

Demonstração:

Para i, j = 1, 2, ..., m, pela proposição 2, $a + ka_i \equiv a + ka_j \bmod m$, então $(-a) + a + ka_i \equiv (-a) + a + ka_j \bmod m$, ou seja, $ka_i \equiv ka_j \bmod m$.

Mas, pela proposição 7, $ka_i \equiv ka_j \bmod m \Leftrightarrow a_i \equiv a_j \bmod m$. Como $\{a_1, a_2, ..., a_m\}$ é um sistema completo de resíduos módulo m, então $a_i \equiv a_j \bmod m \Leftrightarrow i = j$.

O resultado acima prova que dados dois elementos quaisquer do conjunto $\{a + ka_1, a + k a_2, ..., a + ka_m\}$, eles não são congruentes módulo m, ou seja, o conjunto forma um sistema completo de resíduos módulo m. ■

Proposição 9: Sejam o números naturais **m** e **m`** tais que (m,m`)=1. Então φ(m.m`) = φ(m).φ(m`).

Demonstração:

Para m = 1 ou m`= 1 o resultado é trivial. Então vamos supor que m > 1 e m`> 1.

Na tabela abaixo temos todos os números naturais de 1 a m.m`, ou seja, temos um sistema completo de resíduos módulo m.m`.

1	2	...	k	...	m`
m`+ 1	m`+ 2	...	m`+ k	...	2m`
⋮	⋮		⋮	...	⋮
(m – 1).m`+1	(m – 1).m`+ 2	...	(m – 1).m`+ k	...	m.m`

Sabemos que para todo inteiro t tem-se (t,m.m`) = 1 se, e somente se, (t,m) = (t,m`) = 1. Então devemos encontrar na tabela os números que são coprimos, simultaneamente, com m e m`.

Podemos observar, pelo lema 3, que em cada linha temos um sistema completo de resíduos módulo m` e que todos elementos de uma mesma coluna são congruentes módulo m`. Assim, se o primeiro elemento de uma coluna não for primo relativo com m`, então nenhum elemento desta coluna será. Desta forma fica claro que o número de colunas cujo primeiro elemento é coprimo com m` determina o número natural φ(m`).

Por outro lado, se 0, 1, ..., m – 1, forma um sistema completo de resíduos módulo m e (m,m`) = 1, então, em virtude do lema 3, a sequência k, m`+ k, ..., (m – 1)m`+ k também forma um sistema completo de resíduos módulo m e, portanto, o número de elementos em cada coluna que são coprimos com m é o natural φ(m).

Portanto temos φ(m`) colunas que representam os números que são coprimos com m` e em cada uma destas colunas temos φ(m) números que são coprimos com m, logo os números que são primos relativos com m e m` simultaneamente são em número φ(m).φ(m`), ou seja, φ(m.m`) = φ(m).φ(m`).■

Exemplo: Dados m = 5 e m`=4, vamos determinar φ(5.4).

Primeiramente montamos a tabela com os números de 1 a 20, formando assim um sistema completo de resíduos módulo 20.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20

Para determinar φ(20) devemos encontrar os números desta tabela que são primos relativos com 20. Como vimos na demonstração, devemos encontrar então os números que são coprimos com 5 e 4 simultaneamente.

Na primeira e na terceira coluna todos os números são coprimos com 4.

Cada coluna forma um sistema completo de resíduos módulo 5, portanto para calcular a quantidade de elementos que são coprimos com 5 em cada coluna basta calcular φ(5), como 5 é primo então φ(5) = 5 – 1 = 4.

Portanto são duas colunas onde os números são comprimos com 4, mas dentre os números de cada coluna apenas quatro são coprimos com 5, ou seja, ao todo são 8 números que são coprimos simultaneamente com 4 e 5. Logo φ(20) = 8 como era de se esperar, pois φ(4) = 2 e φ(5) = 4.

Lema 4: Seja $\{ r_1,...,r_{\varphi(m)} \}$ um sistema reduzido de resíduos módulo m e **a** um número inteiro tal que (a,m) = 1. Então $\{ ar_1,...,ar_{\varphi(m)} \}$ também é um sistema reduzido de resíduos.

Demonstração:

Pela hipótese $(r_i, m) = 1$, para todo i = 1,...,φ(m) e (a,m) = 1, então $(ar_i, m) = 1$, ou seja, $\{ ar_1,...,ar_{\varphi(m)} \}$ é um sistema reduzido de resíduos módulo m.■

Proposição 10(Teorema de Euler): Sejam **a** e **m** dois números inteiros com m > 1 e (a,m) = 1. Então $a^{\varphi(m)} \equiv 1 \bmod m$.

Demonstração:

Seja $\{ r_1,...,r_{\varphi(m)} \}$ um sistema reduzido de resíduos módulo m, pelo lema 4, temos que $\{ ar_1,...,ar_{\varphi(m)} \}$ também é um sistema reduzido de resíduos módulo m, pois (a,m) = 1. Portanto, pela proposição 5:

$$a^{\varphi(m)} r_1.r_2.....r_{\varphi(m)} = ar_1.ar_2.....ar_{\varphi(m)} \equiv r_1.r_2.....r_{\varphi(m)} \bmod m.$$

Como $(r_1.r_2.....r_{\varphi(m)}, m) = 1$, então, pela proposição 7, $a^{\varphi(m)} \equiv 1 \bmod m$. ■

Proposição 11(Pequeno teorema de Fermat): Sejam **a** um número inteiro e **p** um número primo tais que (a,p) = 1. Tem-se que $a^{p-1} \equiv 1 \bmod p$.

Demonstração:

Na hipótese observamos que (a,p) = 1, então, do teorema de Euler, concluímos que $a^{\varphi(p)} \equiv 1 \bmod p$, mas como p é um número primo, então $\varphi(p) = p - 1$, ou seja, $a^{p-1} \equiv 1 \bmod p$. ■

Lema 5: Se **p** é um número primo, então para todo inteiro **a** e todo natural **k** tem-se que $a^{k(p-1)+1} \equiv a \bmod p$.

Demonstração:

Pelo pequeno teorema de Fermat $a^{p-1} \equiv 1 \bmod p$, então, pela proposição 6, $(a^{(p-1)})^k \equiv 1^k \bmod p$, ou seja, $a^{k(p-1)} \equiv 1 \bmod p$.

Como (a,p) = 1, então, pela proposição 7, $a^{k(p-1)}.a \equiv 1.a \bmod p$, ou seja, $a^{k(p-1)+1} \equiv a \bmod p$. ■

Para os próximo enunciados e suas demonstrações utilizaremos a notação [a,b] para o mínimo múltiplo comum dos números inteiros a e b.

Lema 6: Sejam **a** e **b** números inteiros e $\mathbf{m, n, m_1,...,m_r}$ números inteiros maiores que 1. Temos que:

(i) se $a \equiv b \bmod m$ e $n \mid m$, então $a \equiv b \bmod n$.

(ii) $a \equiv b \bmod m_i$, para todo i = 1,...,r se, e somente se, $a \equiv b \bmod [m_1,..., m_r]$.

Demonstração:

(i) Como $a \equiv b \bmod m$, então, pela proposição 1, $m \mid a - b$. Pela hipótese $n \mid m$, então $n \mid a - b$, logo, pela proposição 1, $a \equiv b \bmod n$. ■

(ii)

(=>)

$a \equiv b \bmod m_i$, então, pela proposição 1, $m_i \mid a - b$, para todo i = 1,...,r, ou seja, a – b é um múltiplo comum a todos os m_i`s.

Pela definição de mínimo múltiplo comum, temos que $[m_1,...,m_r] | a - b$, ou seja, pela proposição 1, $a \equiv b \bmod [m_1,...,m_r]$.■

(<=)

Se $[m_1,...,m_r]$ é o mmc de todos os m_i`s, i = 1,...,r, então temos que $m_i | [m_1,...,m_r]$ para todo i.

Se $a \equiv b \bmod [m_1,...,m_r]$ e $m_i | [m_1,...,m_r]$ para todo i = 1,...,r, então pelo lema 6 (i), $a \equiv b \bmod m_i$.■

Proposição 12: Seja **m** um número cuja fatoração é $p_1.p_2.....p_r$, onde $\mathbf{p_1,...p_r}$ são números primos distintos, então para todo número inteiro **a** e todo número natural **k** tem-se que $a^{k\varphi(m)+1} \equiv a \bmod m$.

Demonstração:

Como $m = p_1.p_2.....p_r$, sendo $p_1,...p_r$ números primos distintos, então temos que $\varphi(m) = (p_1 - 1).(p_2 - 1).....(p_r - 1)$.

Seja $k_i = k.(p_1 - 1).(p_2 - 1).....(p_{i-1} - 1).(p_{i+1} - 1).....(p_r - 1)$, tem-se que $k\varphi(m) = k_i(p_i - 1)$, então, para todo número inteiro **a**, todo número natural **k** e todo i = 1,...,r, $a^{k\varphi(m)+1} = a^{k_i(p_i-1)+1} \equiv a \bmod p_i$, pelo lema 5.

Do fato que $[p_1,...,p_r] = p_1.p_2.....p_r = m$ e pelo lema 6 (ii), temos que $a^{k\varphi(m)+1} \equiv a \bmod m$.■

3.3
Questões de concursos

Em alguns concursos com nível de ensino fundamental exigido, questões envolvendo aritmética modular aparecem. Alguns exemplos estão resolvidos a seguir.

Exemplo 1: (Colégio Militar de Fortaleza – 2011) Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:

(a) 1 (b) 2 (c) 3 (d) 4 (e) 5

Solução:

Sejam x e y o primeiro e o segundo números inteiros tratados no problema.

Segundo o enunciado temos: $x \equiv 6 \bmod 7$ e $y \equiv 5 \bmod 7$.

Pela proposição 4, $(x + y) \equiv (6 + 5) \bmod 7 \Rightarrow (x + y) \equiv 11 \bmod 7$, mas $11 \equiv 4 \bmod 7$, então $(x + y) \equiv 4 \bmod 7$, ou seja, o resto da divisão de x + y por 7 é 4.

Resposta: letra (d)

Exemplo 2: (Colégio Naval – 2011) É correto afirmar que o número $5^{2011} + 2.11^{2011}$ é múltiplo de:

(a) 13 (b) 11 (c) 7 (d) 5 (e) 3

Solução:

Analisando as alternativas observamos que utilizando a letra **(e)** temos:

$5 \equiv 2 \bmod 3$ e $11 \equiv 2 \bmod 3$, ou seja, ambos deixam o mesmo resto na divisão por 3. Pela proposição 6, temos $5^{2011} \equiv 2^{2011} \bmod 3 \text{ e } 11^{2011} \equiv 2^{2011} \bmod 3$ e, pela proposição 7, $2.11^{2011} \equiv 2.2^{2011} \bmod 3$, então:

$5^{2011} + 2.11^{2011} \equiv 2^{2011} + 2.2^{2011} \bmod 3$, mas $2^{2011} + 2.2^{2011} = 3.2^{2011}$ que é um múltiplo de 3.

Resposta: letra (e)

Exemplo 3: (Colégio Naval – 2007) Qual será o dia da semana na data 17 de setembro de 2009?

(a) segunda-feira (b) terça-feira (c) quarta-feira

(d) quinta-feira (e) sexta-feira

Solução:

O concurso do colégio naval de 2007 ocorreu no dia 29 de julho que era um domingo, logo esta data servia como referência para os candidatos.

Primeiramente devemos contar quantos dias se passaram de 29/07/2007(exclusive) até 17/09/2009(inclusive). Vejamos:

● **Considerando o ano de 2007.**

Julho → 2 Dias Outubro → 31 Dias Total → 155 Dias

Agosto → 31 Dias Novembro → 30 Dias

Setembro → 30 Dias Dezembro → 31 Dias

● **Considerando o ano de 2008, que é um ano bissexto.**

366 Dias

● **Considerando o ano de 2009.**

Janeiro → 31 Dias Junho → 30 Dias

Fevereiro → 28 Dias Julho → 31 Dias

Março → 31 Dias Agosto → 31 Dias

Abril → 30 Dias Setembro 17 Dias

Maio → 31 Dias Total → 260 Dias

● **Total de dias.**

155 + 366 + 260 = 781 Dias

Como 29 de julho de 2007 foi um domingo, então se o total de dias passados for um múltiplo de 7, a data será um domingo, se o resto da divisão for 1, então a data será uma segunda, pois será um múltiplo de 7 mais um dia e assim por diante. Então podemos montar a tabela que relaciona o resto da divisão com o dia da semana:

RESTO	0	1	2	3	4	5	6
DIA	DOM	SEG	TER	QUA	QUI	SEX	SAB

Como o total de dias foi 781 e $781 \equiv 4 \bmod 7$, ou seja, o resto da divisão de 781 por 7 é 4, então dia 17 de setembro de 2009 foi uma quinta-feira.

Resposta: letra (d)

Exemplo 4: (Colégio Naval – 2003) O resto da divisão de $5^{131}+7^{131}+9^{131}+15^{131}$ por 12 é igual a:

a) 0 b) 2 c) 7 d) 9 e) 11

Solução:

Pelas proposições 1 e 7 temos:

$$5 \equiv (-7) \bmod 12 \Rightarrow 5^{131} \equiv (-7)^{131} \bmod 12$$

$$9 \equiv (-3) \bmod 12 \Rightarrow 9^{131} \equiv (-3)^{131} \bmod 12$$

$$15 \equiv 3 \bmod 12 \Rightarrow 15^{131} \equiv 3^{131} \bmod 12$$

Pela proposição 4 temos:

$5^{131}+7^{131}+9^{131}+15^{131}\equiv(-7)^{131}+7^{131}+(-3)^{131}+3^{131} \bmod 12$, como 131 é ímpar, então $(-7)^{131}+7^{131}=(-3)^{131}+3^{131}=0$, logo o resto da divisão que o enunciado trata é zero.

Resposta: letra (a)

Exemplo 5: (Colégio Naval – 2002) Se **a** e **b** são números naturais e 2a + b é divisível por 13, então um número múltiplo de 13 é:

(a) 91a + b (b) 92a + b (c) 93a + b (d) 94a + b

(e) 95a + b

Solução:

Se 2a + b é divisível por 13, então (2a + b) ≡ 0 mod 13.

Pela proposição 2 temos (91a + 2a + b) ≡ 91a mod 13.

Mas 91a ≡ 0 mod 13, pois 91 = 7.13, então (93a + b) ≡ 0 mod 13, ou seja, 93a + b é um múltiplo de 13.

Resposta: letra (c)

4
A matemática que envolve o DHM e o RSA

Neste capítulo vamos mostrar o funcionamento dos dois sistemas de codificação e os argumentos matemáticos que fazem com que eles funcionem. Existem diversos recursos computacionais capazes de realizar os cálculos que serão feitos neste capítulo sem nenhuma dificuldade, dois exemplos destes recursos que foram utilizados são: o aplicativo Wolfram alpha e o software Maple.

4.1
O funcionamento do DHM

Como já foi citado anteriormente a matemática que envolve o DHM é espantosamente simples e o mais incrível é imaginar que o problema chegou a ser considerado sem solução. A função de mão única que o trio Diffie, Hellman e Merkle tanto procuraram é a função do tipo $Y^x \equiv \alpha \bmod P$, onde $\alpha < P$, ou seja, α é o resto da divisão de Y^x por P, fato que o torna único para cada valor natural de x. Na aritmética modular se você souber o valor do α, não é uma tarefa simples descobrir o valor do x.

Para facilitar essa apresentação, vamos fazer uso de dois personagens fictícios: Gabriela e Matheus. Suponha que Gabriela e Matheus desejam trocar mensagens, mas estão com medo de que elas sejam interceptadas. Para isso eles devem trocar uma chave, mas os meios de comunicação não são seguros.

Primeiramente Gabriela e Matheus escolhem os números naturais Y e P em comum acordo sem se preocuparem com o risco deles se tornarem públicos. No próximo passo, a Gabriela escolhe um número natural α_G, este deve ser mantido em segredo, e calcula $\beta_G < P$ tal que $Y^{\alpha_G} \equiv \beta_G \bmod P$, que será enviado ao Matheus. Por sua vez o Matheus escolhe um α_M, que também não deve ser revelado, e calcula $\beta_M < P$ tal que $Y^{\alpha_M} \equiv \beta_M \bmod P$, que será enviado à Gabriela.

Em seguida Gabriela calcula $\alpha < P$, onde α é o resto da divisão de ${\beta_M}^{\alpha_G}$ por P, como $\beta_M \equiv Y^{\alpha_M} \bmod P$, então: ${\beta_M}^{\alpha_G} \equiv (Y^{\alpha_M})^{\alpha_G} \equiv Y^{\alpha_M \alpha_G} \equiv \alpha \bmod P.$

Matheus chegará ao mesmo valor de α, calculando o resto da divisão de $\beta_G{}^{\alpha_M}$ por P, pois de forma análoga $\beta_G \equiv Y^{\alpha_G} \bmod P$, logo:

$$\beta_G{}^{\alpha_M} \equiv (Y^{\alpha_G})^{\alpha_M} \equiv Y^{\alpha_G \alpha_M} \equiv \alpha \bmod P.$$

Está calculada a chave α. Observe que o sistema é útil quando se trata da comunicação de duas pessoas por vez, o que não é sempre satisfatório, e que o cálculo da chave depende do envio de β_G, calculado pela Gabriela e de β_M, calculado pelo Matheus, tornando possivelmente, esse processo demorado.

Exemplo: Suponha que a Gabriela e o Matheus escolham Y = 53 e P = 170 de comum acordo. A Gabriela escolhe α_G = 7 e Matheus α_M = 5, mantendo estes números em sigilo. Vamos determinar a chave que eles irão compartilhar.

Gabriela calcula β_G e o envia para Matheus:

$53^7 \equiv 77 \bmod 170$, ou seja, β_G = 77.

Matheus Calcula β_M e o envia para Gabriela:

$53^5 \equiv 83 \bmod 170$, ou seja, β_M = 83.

Para calcular a chave, Gabriela faz o seguinte cálculo:

$83^7 \equiv 127 \bmod 170$.

Analogamente Matheus calcula a chave:

$77^5 \equiv 127 \bmod 170$.

Como era de se esperar, ambos encontram o mesmo resultado, logo a chave é α = 127.

4.2
Sistema de numeração binário

O sistema de numeração que utilizamos no nosso cotidiano é o sistema decimal, que utiliza sequências com os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 para formar seus números. Porém existem outros sistemas não menos importantes que o decimal. Nesta seção daremos ênfase ao sistema de numeração de base 2, também chamado de sistema de numeração binário. Neste sistema os números são formados por sequências de 0`s e 1`s.

Dado o número binário $a_n a_{n-1}...a_1 a_0$, onde $a_i \in \{0,1\}$ para todo i = 0,...n, a sua representação decimal é dada por $x = a_0.2^0 + a_1.2^1 + ... + a_{n-1}.2^{n-1} + a_n.2^n$.

Exemplo: A representação decimal do número binário 100111 é:

$x = 1.2^0 + 1.2^1 + 1.2^2 + 0.2^3 + 0.2^4 + 1.2^5 = 1 + 2 + 4 + 32 = 39$

Mas também podemos transformar um número cuja representação decimal é x em um número binário utilizando sucessivamente a divisão euclidiana:

$x = 2.q_0 + r_0,\ r_0 < 2$

$q_0 = 2.q_1 + r_1,\ r_1 < 2$

Como $x > q_0 > q_1 ...$, num determinado momento teremos $q_{n-1} < 2$, portanto na última divisão temos: $q_{n-1} = 2.0 + q_{n-1}$, ou seja, $q_n = 0$ e $r_n = q_{n-1}$. Assim x escrito na forma binária é a sequência $q_{n-1} r_{n-1} r_{n-2} ... r_1 r_0$.

Exemplo: Determinar o número binário cuja representação decimal é 37:

Efetuando as divisões:

37 = 2.18 + 1

18 = 2.9 + 0

9 = 2.4 + 1

4 = 2.2 + 0

2 = 2.1 + 0

1 = 2.0 + 1

Assim o número binário que tem representação decimal x = 37 é 100101.

4.3
A tabela ASCII

Como os computadores lidam apenas com dígitos binários ou simplesmente *bits* (abreviação de binary digits), então a partir de 1960 passou a ser desenvolvido o American Standard Code for International Interchange, cuja abreviação é ASCII e em português significa código padrão americano para o intercâmbio de informação. O ASCII trata de uma tabela que associa a cada número binário de 7 dígitos uma letra do alfabeto, ou símbolos, que são utilizados com frequência. Há 2^7 = 128 maneiras de formar sequências deste tipo, ou seja, a tabela pode associar 128 tipos de caracteres a cada número binário, onde os 32

primeiros e o último são chamados de sinais de controle (não imprimíveis). A Figura 9 ilustra a representação das letras maiúsculas do nosso alfabeto, o que já é suficiente para o objetivo do trabalho.

LETRA	NÚMERO BINÁRIO	NÚMERO DECIMAL	LETRA	NÚMERO BINÁRIO	NÚMERO DECIMAL
A	1000001	65	**N**	1001110	78
B	1000010	66	**O**	1001111	79
C	1000011	67	**P**	1010000	80
D	1000100	68	**Q**	1010001	81
E	1000101	69	**R**	1010010	82
F	1000110	70	**S**	1010011	83
G	1000111	71	**T**	1010100	84
H	1001000	72	**U**	1010101	85
I	1001001	73	**V**	1010110	86
J	1001010	74	**W**	1010111	87
K	1001011	75	**X**	1011000	88
L	1001100	76	**Y**	1011001	89
M	1001101	77	**Z**	1011010	90

Figura 9 – Letras maiúsculas do nosso alfabeto na tabela ASCII.

(Fonte: Elaborada pelo autor).

4.4
Os detalhes matemáticos do RSA

A segurança do RSA se encontra na dificuldade técnica de fatorar números que possuem fatores primos muito grandes. Segundo COUTINHO (2015), o RSA Laboratory, que pertence à empresa detentora dos direitos do sistema, durante algum tempo propôs desafios que consistiam em fatorar possíveis chaves públicas. A última fatoração, anunciada em 2005, corresponde a um número de 193 algarismos e foi feita no Escritório Federal de Segurança de Informação da Alemanha, mas os cálculos utilizaram 80 computadores de 2.2GHz cada um e, ainda assim foram necessários 5 meses para que as contas fossem finalizadas.

4.4.1
Como e por que funciona?

Para facilitar a apresentação e a compreensão deste tópico vamos trabalhar com a situação hipotética de uma loja virtual que utiliza o sistema RSA para dar mais segurança aos dados que seus clientes enviam durante uma compra. Primeiramente a loja deve escolher dois números primos suficientemente grandes p e q e multiplicá-los obtendo N = p.q, onde o valor de N será amplamente divulgado, mas os valores de p e q deverão ficar em sigilo.

Em seguida a loja escolhe um número α, código de cifragem, tal que $(\alpha,\varphi(N)) = 1$, onde $\varphi(N) = (p - 1).(q - 1)$. O valor de α também será amplamente divulgado e será utilizado para calcular sua chave de decifragem β, chave que a loja utilizará para decifrar as mensagens enviadas por seus clientes. O valor de β é uma solução congruência $\alpha.\beta \equiv 1 \bmod \varphi(N)$ que, pela proposição 8, possui solução se, e somente se, $(\alpha,\varphi(N)) = 1$. Os valores de p e q são fundamentais para o cálculo da chave de decifragem, mas após este cálculo eles não são mais necessários, podendo ser esquecidos. Voltemos aos nossos personagens Gabriela e Matheus.

A Gabriela está efetuando uma compra nesta loja e deverá enviar informações pessoais, mas não pode correr o risco de ter suas informações interceptadas. Os dados da Gabriela são convertidos em números binários de acordo com a tabela ASCII, utilizando a sequência 0100000 para representar o espaço entre cada palavra. A codificação dos dados da Gabriela é feita como descreveremos a seguir.

Corta-se a mensagem em **r** sequências de tamanhos arbitrários, onde $x_1, x_2, ..., x_r$ são suas representações decimais, de modo que cada sequência não inicie com zero, com o propósito de descobrir tal sequência a partir do número que ela representa e $x_i < N$, i = 1,...r, a segunda restrição será explicada mais adiante.

Gabriela calcula e envia para a loja $C(x_i) < N$ de modo que $(x_i)^{\alpha} \equiv C(x_i) \bmod N$, ou seja, $C(x_i)$ é o resto da divisão de $(x_i)^{\alpha}$ por N, logo $C(x_i)$ é único.

Ao receber $C(x_1)$, $C(x_2)$,...,$C(x_r)$, a loja utiliza sua chave de decifragem para calcular $D(C(x_i)) < N$ tal que $[C(x_i)]^{\beta} \equiv D(C(x_i)) \bmod N$. Como no cálculo de $C(x_i)$, $D(C(x_i))$ é o resto da divisão de $C(x_i)^{\beta}$ por N, que também o torna único.

Sabe-se que $D(C(x_i)) \equiv [C(x_i)]^{\beta} \bmod N$ e $C(x_i) \equiv (x_i)^{\alpha} \bmod N$, então $D(C(x_i)) \equiv [(x_i)^{\alpha}]^{\beta} = (x_i)^{\alpha\beta} \bmod N$, mas sabemos que $\alpha.\beta \equiv 1 \bmod \varphi(N)$, ou seja, pela proposição 1, $\varphi(N) \mid \alpha.\beta - 1$. Logo existe um número inteiro k tal que $\alpha.\beta = 1 + k.\varphi(N)$. Então $D(C(x_i)) \equiv (x_i)^{k\varphi(N)+1} \bmod N$, portanto, pela proposição 12, $D(C(x_i)) \equiv x_i \bmod N$, onde $D(C(x_i))$ e x_i são menores que N.

A restrição $x_i < N$ se deve ao fato de torná-lo único, caso não houvesse tal restrição o x_i poderia assumir uma infinidade de valores bastando satisfazer a condição $D(C(x_i)) \equiv x_i \bmod N$, o que tornaria a decifragem praticamente impossível.

Assim a loja obtém $D(C(x_1)) = x_1$, $D(C(x_2)) = x_2$,..., $D(C(x_r)) = x_r$. Revertendo cada x_i para a forma binária e os enfileirando, basta separar as sequências de 0`s e 1`s em grupos de 7 dígitos e comparar com a tabela ASCII, a mensagem original surge.

Exemplo: Suponha que o Matheus deseja enviar um simples **OI** para a Gabriela utilizando o sistema RSA. Sabendo que a Gabriela escolheu os números primos p = 13 e q = 11 e o código de cifragem $\alpha = 7$, atendendo as restrições necessárias, então Matheus procura a chave pública da Gabriela em uma lista e encontra N = 143 e o código de cifragem.

Primeiramente Matheus escreve a mensagem em números binários, conforme a tabela ASCII (Figura 9), obtendo :

$$\underbrace{1001111}_{O}\underbrace{1001001}_{I}$$

Agora ele separa esta sequência em blocos (no caso 3), mas nenhum deles iniciando com zero:

Bloco 1 → 10011, cuja representação decimal é $x_1 = 19$.

Bloco 2 → 11100, cuja representação decimal é $x_2 = 28$.

Bloco 3 → 1001, cuja representação decimal é $x_3 = 9$.

Em posse dos valores de N e do código de cifragem Matheus calcula $C(x_1)$, $C(x_2)$ e $C(x_3)$, e os envia para a Gabriela:

- $(x_1)^{\alpha} \equiv C(x_1) \bmod N \Rightarrow 19^7 \equiv 46 \bmod 143$, ou seja, $C(x_1) = 46$.
- $(x_2)^{\alpha} \equiv C(x_2) \bmod N \Rightarrow 28^7 \equiv 63 \bmod 143$, ou seja, $C(x_2) = 63$.
- $(x_3)^{\alpha} \equiv C(x_3) \bmod N \Rightarrow 9^7 \equiv 48 \bmod 143$, ou seja, $C(x_3) = 48$.

Para decifrar a mensagem a Gabriela calcula a chave de decifragem β resolvendo a equação $\alpha.\beta \equiv 1 \bmod \varphi(N)$, onde α = 7 e φ(N) = (13 – 1).(11 – 1) = 120, ou seja, ela deve determinar algum β tal que $7\beta \equiv 1 \bmod 120$, obtendo como uma das soluções β = 103.

Com o valor β se inicia o processo de decifragem da mensagem:

- $[C(x_1)]^{\beta} \equiv D(C(x_1)) \bmod N \Rightarrow 46^{103} \equiv 19 \bmod 143$, ou seja, $D(C(x_1)) = 19$.
- $[C(x_2)]^{\beta} \equiv D(C(x_2)) \bmod N \Rightarrow 63^{103} \equiv 28 \bmod 143$, ou seja, $D(C(x_2)) = 28$.
- $[C(x_3)]^{\beta} \equiv D(C(x_3)) \bmod N \Rightarrow 48^{103} \equiv 9 \bmod 143$, ou seja, $D(C(x_3)) = 9$.

Gabriela então escreve estes números na forma binária. Como vimos no início do exemplo:

19 → 10011

28 → 11100

9 → 1001

Enfileirando estas sequências e separando em grupos de 7 dígitos ela obtém 1001111 1001001. Consultando a tabela ASCII encontra a mensagem original: **OI**.

5
Uma pequena aplicação e seus resultados na educação básica

Um dos desafios para nós, professores de matemática da educação básica, é fazer com que nossos alunos não apenas compreendam os conteúdos lecionados, mas também se interessem pela disciplina. A matemática muitas vezes é vista como um vilão para alguns alunos, fato que, por si só, já gera um bloqueio na mente dos discentes. Outro fator importante que pode acentuar o desinteresse pela matemática, é a questão de alguns conteúdos serem apresentados apenas como regras a serem decoradas e aplicadas sem o contexto histórico que as justifique e sem o conhecimento de algumas de suas aplicações. É claro que estas aplicações nem sempre serão algo de fácil compreensão pelo alunado, mas podem apenas ser comentadas ou abordadas de forma superficial.

Como sabemos a aritmética modular é uma ferramenta de grande utilidade para que algumas destas questões sejam minimizadas e, além do mais, serve como um meio para que a criptografia, tema que costuma despertar a curiosidade e interesse dos alunos, seja introduzida na educação básica.

Foi feita uma aplicação de parte deste trabalho com alguns alunos da educação básica na forma de uma oficina que contou com a presença de 12 alunos do 8º e 9º anos da Escola Municipal Joaquim da Silva Gomes[6] organizada em 5 encontros.

A oficina foi dividida em três momentos: no primeiro momento foi apresentado a aritmética modular com suas definições básicas, algumas de suas proposições, exercícios de fixação e questões de concursos de nível fundamental, conforme o ANEXO I. Foi também mostrado como essa teoria pode justificar alguns critérios de divisibilidade que já tinham sido estudados por eles.

No segundo momento o tema gerou em torno da criptografia. Sua importância e contexto histórico foram debatidos e alguns exercícios com diferentes métodos de cifragens propostos conforme o ANEXO II.

[6] Escola da rede municipal de ensino do Rio de Janeiro localizada no bairro de Santa Cruz.

No último momento foi apresentada uma aplicação de aritmética modular na criptografia com um exemplo do funcionamento do RSA conforme o ANEXO III. Nesta parte foi utilizado o recurso do aplicativo Wolfram Alpha para efetuar as contas e mostrar que a fatoração de números suficientemente grandes não é uma tarefa simples nem mesmo para as máquinas e ainda foi apresentada de forma superficial a tabela ASCII, fatos que despertaram a curiosidade dos discentes.

Ao final da oficina os alunos responderam a um questionário, como mostra o ANEXO IV sobre suas conclusões acerca dos temas trabalhados.

Com base nas respostas e nos comentários dos alunos no questionário ficou claro que a grande maioria dos alunos nunca tinha ouvido falar de criptografia e, os poucos que já tinham ouvido falar, não sabiam do que se tratava e não imaginavam que havia relação com a matemática. Veja o comentário de uma aluna do 9º ano:

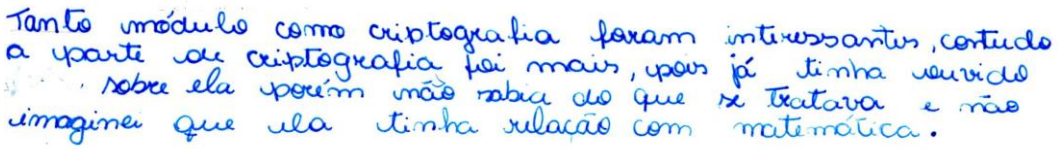


Figura 10 – Resposta do aluno A à pergunta 3 do questionário.

Além do interesse pela criptografia, outro fator que os deixou bastante animados foi o fato de estarem compreendendo com facilidade um conteúdo que não faz parte do currículo escolar e que geralmente é lecionado nas graduações. Como podemos ver em algumas respostas selecionadas:

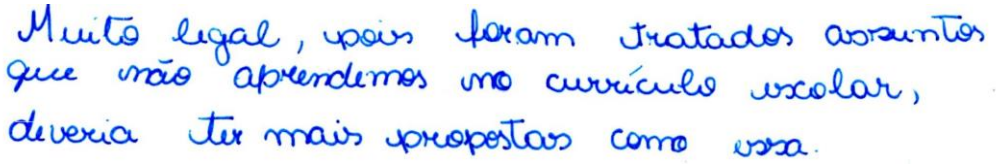


Figura 11 – Resposta do aluno A à pergunta 1 do questionário.

Perguntada sobre o que achou mais interessante na oficina uma aluna respondeu:

Figura 12 – Resposta do aluno B à pergunta 3 do questionário.

No campo dos comentários outra aluna escreveu:

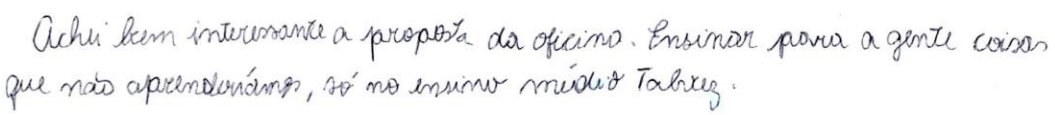


Figura 13 – Comentário do aluno C sobre a oficina

O fato de a criptografia estar diretamente relacionada com a computação despertou o interesse de alguns alunos que pensam em seguir carreira na área da informática. Os próximos relatos, por não estarem legíveis, serão transcritos:

[...] Achei uma proposta bem interessante, pude aprender um pouco de como a matemática está inserida na informática (que é uma possível carreira que eu posso seguir).

[...] A parte que achei mais interessante foi a criptografia, pois eu amo a área de informática.

Quanto à questão de inserir estes conteúdos no ensino fundamental, a maioria dos alunos achou que seria uma boa ideia, mas dois alunos entenderam que inserir no currículo não seria conveniente, seus argumentos estão baseados no que foi citado no início do capítulo sobre a má fama que a matemática tem em parte da sociedade e o desinteresse crescente pela matemática. A seguir, alguns comentários de alunos que entendem que seria adequado inserir estes conteúdos no currículo da educação básica:

Figura 14 – Parte da resposta do aluno A à pergunta 4 do questionário.

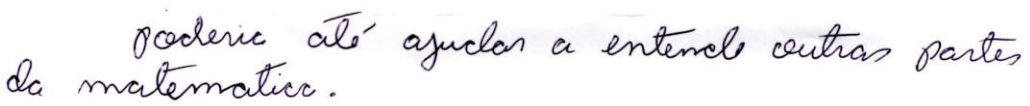


Figura 15 – Parte da resposta do aluno B à pergunta 4 do questionário.

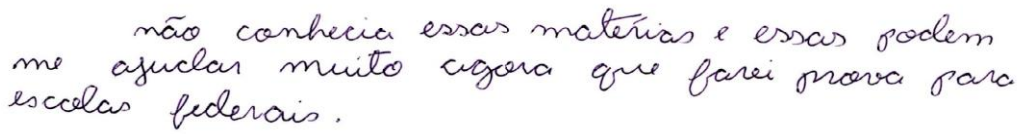


Figura 16 – Parte da resposta do aluno B à pergunta 2 do questionário

Os relatos dos alunos que entendem não ser adequada a inclusão destes conteúdos na educação básica estão transcritos abaixo.

[...] essa matemática (aritmética modular) pode ser entendida por pessoas que tem uma certa facilidade, porém duvido muito que toda uma sala de aula consiga acompanhar esses conteúdos. Afinal, matemática não é a matéria dos sonhos.

[...] no nível atual dos estudantes, acho que muitos nem ligariam, seria melhor que fosse opcional, como um projeto mesmo.

Na maioria dos questionários os alunos citam que deveriam ter mais propostas como esta, o que mostra que a oficina foi proveitosa. De forma geral a oficina mostrou que quando a aplicação de determinado conteúdo é mostrada ao aluno, seu interesse pela matéria aumenta uma vez que torna a aprendizagem mais significativa. Os conteúdos ministrados, neste caso, foram apropriados pelo alunado de forma mais lúdica, prazerosa e com resultados bem satisfatórios.

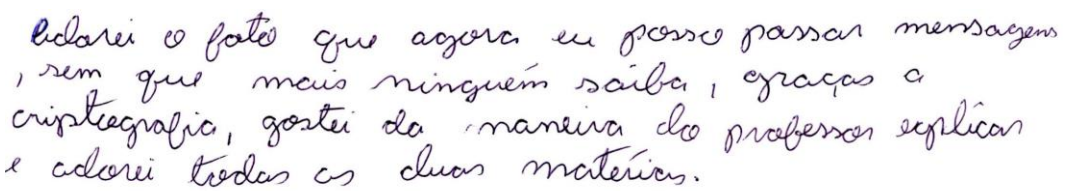


Figura 17 – Comentário do aluno B sobre a oficina.

6
Conclusão

O objetivo principal deste trabalho foi apresentar o funcionamento do código RSA, mas priorizando também a evolução da criptografia ao longo da história. Como vimos, um pré-requisito para entender o RSA é a aritmética modular, um conteúdo que, além da aplicação vista neste trabalho, possui diversas outras e auxilia na aprendizagem de conteúdos que constam no currículo da educação básica ensinados muitas vezes de forma pouco atrativa.

Embora a criptografia seja bastante utilizada no nosso cotidiano e um tema que envolve muitos estudos e publicações atuais, ela ainda é desconhecida pela maior parte dos alunos da educação básica. Percebemos que a simples introdução desse assunto possibilitou um grande envolvimento do alunado tanto na evolução quanto na operação do tema. Com os relatos dos alunos que participaram da oficina e o retorno durante as aulas ficou claro que apresentar a evolução histórica da criptografia até o surgimento do RSA foi um aliado para construção de importantes conceitos matemáticos. O aluno aprendeu de uma forma mais lúdica, vendo aplicações diretas e situadas num contexto histórico.

Concluímos que cada vez mais devemos procurar construir nossas aulas partindo de temas que possibilitem um engajamento do alunado que muitas vezes pode ser alcançado a partir de uma contextualização histórica ou de comentários sobre a significância do tema. Dessa forma acreditamos que o aluno se interesse mais pelo aprendizado dos conteúdos propostos além de proporcioná-los ganhos culturais e acadêmicos que servirão de subsídios para que exercitem a construção de argumentações mais eficientes e lógicas auxiliando na construção de um cidadão cada vez mais autônomo e consciente.

7
Bibliografia

[1] COUTINHO, SEVERINO. Criptografia. Rio de Janeiro. IMPA, 2015.

[2] GROENWALD, C.L.O; OLGIN, C.A. Códigos e senhas: Sequência didática com o tema criptografia no ensino fundamental. Anais do X Encontro Nacional de Educação Matemática, 2010.

[3] HEFEZ, A. Aritmética. Coleção PROFMAT. Rio de Janeiro. Editora SBM, 2013.

[4] SÁ, I.P. Aritmética modular e algumas de suas aplicações. Disponível em:<http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf >. Acesso em: 28 de fevereiro de 2016.

[5] SANT`ANNA, I.K. DE. A aritmética modular como ferramenta para as séries finais do ensino fundamental. Dissertação de mestrado. Orientador: Prof. Dr. Roberto Imbuzeiro Oliveira. IMPA, 2013.

[6] SINGH, S. O livro dos códigos. Rio de Janeiro. São Paulo. Editora Record, 2007.

Anexo I

E M JOAQUIM DA SILVA GOMES
OFICINA DE MATEMÁTICA

ALUNO(A):_____
PROFESSOR: IGOR NASCIMENTO

Aritmética modular

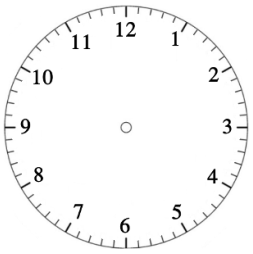
A aritmética modular é uma ferramenta muito importante no estudo da teoria dos números. Uma aplicação importante do conceito de congruência é a criptografia que é uma teoria fundamental para garantir a segurança na troca de informações.

Definição: Dois números inteiros a e b são congruentes módulo m (m é um inteiro não nulo) quando as divisões de a por m e de b por m têm o mesmo resto. Por exemplo, o número 10 é congruente ao número 3, módulo 7, pois ambos deixam resto 3, ao serem divididos por 7. Representamos essa congruência do exemplo por $10 \equiv 3 \bmod 7$.

Veja outros exemplos:

a) $13 \equiv 3 \bmod 10$ b) $20 \equiv 4 \bmod 8$ c) $15 \equiv 6 \bmod 9$

● **Aritmética do relógio**



Um exemplo clássico de congruência no nosso cotidiano é o relógio analógico. Observe que 13 horas corresponde a 1 hora, pois ambos deixam resto 1 quando divididos por 12, ou seja, $1 \equiv 13 \equiv 25 \equiv \ldots$. mod 12 da mesma forma que 4 horas corresponde a 16 horas, pois $4 \equiv 16 \equiv 28 \equiv \ldots$ mod 12.

● **Calendário**

Utilizando o conceito da aritmética modular podemos calcular em que dia da semana "cai" qualquer data. Observe o exemplo a seguir:

Sabe-se que o dia 29/09/2015 “caiu” numa terça-feira. Vamos calcular em que dia da semana será 28/05/2016.

- Primeiramente vamos contar quantos dias existem entre o dia 29/09/15 (exclusive) e o dia 28/05/2016 (inclusive)

- Considerando o ano de 2015, temos:

SETEMBRO → 1 DIA OUTUBRO → 31 DIAS NOVEMBRO → 30 DIAS DEZEMBRO → 31 DIAS

- Considerando agora o ano de 2016 (ano bissexto), temos:

JANEIRO → 31 DIAS FEVEREIRO → 29 DIAS MARÇO → 31 DIAS ABRIL → 30 DIAS MAIO → 28 DIAS

- **TOTAL:** 242 DIAS

Sabemos que a data considerada (29/09/2015) aconteceu numa terça-feira. Então, a cada 7 dias, temos uma nova terça-feira, ou seja, se o total de dias passados for um múltiplo de 7, então o dia 28/05/2016 será numa terça-feira, caso a divisão dê resto 1, então será um múltiplo de 7 mais 1 dia, ou seja, quarta-feira e assim por diante. Podemos então montar a tabela que relaciona o resto da divisão do total de dias por 7 com o dia que cairá a data que desejarmos. Veja:

RESTO	0	1	2	3	4	5	6
DIA	TER	QUA	QUI	SEX	SÁB	DOM	SEG

Como 242 = 34 .7 + 4, ou seja, 242 deixa resto 4 na divisão por 7 podemos concluir que o dia 28/05/2016 será um sábado. Observe que escrever que 242 deixa resto 4 na divisão por 7 é o mesmo que escrever que 242 ≡ 4 (mod 7).

Algumas proposições importantes:

1) Se a ≡ b mod m, então m| (a – b).

Exemplos:

a) 12 ≡ 3 mod 9, então 9| (12 – 3). De fato 12 – 3 = 9 e $\frac{9}{9} = 1$

b) 37 ≡ 5 mod 4, então 4| (37 – 5). De fato 37 – 5 = 32 e $\frac{32}{4} = 8$

c) 25 ≡ -1 mod 13, então 13|[25 – (-1)]. De fato 25 – (-1)=26 e $\frac{26}{13} = 2$

2) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

Exemplos:

a) $3 \equiv 3 \bmod 7$ e $9 \equiv 2 \bmod 7$, logo $3 + 9 \equiv 3 + 2 \bmod 7 \Rightarrow 12 \equiv 5 \bmod 7$.

b) $8 \equiv 2 \bmod 6$ e $13 \equiv 1 \bmod 6$, logo $8 + 13 \equiv 2 + 1 \bmod 6 \Rightarrow 21 \equiv 3 \bmod 6$.

3) Se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$.

Exemplos:

a) $3 \equiv 1 \bmod 2$, então $3^{52} \equiv 1^{52} \bmod 2 \Rightarrow 3^{52} \equiv 1 \bmod 2$.

b) $19 \equiv -1 \bmod 5$, então $19^{2000} \equiv (-1)^{2000} \bmod 5 \Rightarrow 19^{2000} \equiv 1 \bmod 5$

Exercícios

1) Resolva as congruências:

a) $12 \equiv$___ mod 4 b) $32 \equiv$___ mod 3 c) $71 \equiv$____ mod 8

d) $38 \equiv$ ___ mod 13 e) $48 \equiv$___ mod 6 f) $27 \equiv$ ___ mod 11

2) Determine o resto da divisão de:

a) 227^4 por 5. d) $6^{225} + 16^{225} + 11^{225} + 12^{225}$ por 9.

b) 25^{2015} por 6. e) $(2006^{2006} + 2004^{2004})^{2005}$ por 5.

c) 41^{65} por 7. f) 12^{12} por 5.

Desafios:

1. **(Colégio Militar de Fortaleza – 2011)** Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:

a) 1 b) 2 c) 3 d) 4 e) 5

2. **(Colégio Naval – 2007)** Qual será o dia da semana na data 17 de setembro de 2009?

a) segunda-feira b) terça-feira c) quarta-feira d) quinta-feira e) sexta-feira

3. **(Colégio Naval – 2011)** É correto afirmar que o número $5^{2011} + 2 \times 11^{2011}$ é múltiplo de:

a) 13 b) 11 c) 7 d) 5 e) 3

4. **(Colégio Naval – 2003)** O resto da divisão de $5^{131}+7^{131}+9^{131}+15^{131}$ por 12 é igual a:

a) 0 b) 2 c) 7 d) 9 e) 11

Anexo II

E M JOAQUIM DA SILVA GOMES
OFICINA DE MATEMÁTICA

ALUNO(A):_____

PROFESSOR: IGOR NASCIMENTO

Criptografia

● Cifragem por substituição simples

Consiste em trocar cada letra do texto original por outra letra, seguindo um padrão pré definido. No caso da cifra de Cesar, o alfabeto utilizado para a cifragem corresponde ao alfabeto original descolado de três posições, ou seja, a letra A corresponde à letra D, a letra B corresponde à letra E e assim por diante.

1) Utilizando a cifra de Cesar, cifrem a mensagem "JOAQUIM DA SILVA GOMES"

2) Ainda utilizando a cifra de Cesar:

a) Envie uma mensagem para sua dupla.

MENSAGEM ORIGINAL:_____

MENSAGEM CIFRADA:_____

b) Ela decifrou corretamente?

□ **SIM** □ **NÃO**

3)Crie, junto com sua dupla, uma tabela que identifique a substituição que será feita pelas letras do alfabeto.

4) Utilizando a tabela anterior:

a) Cifrem a mensagem "EU AMO MATEMÁTICA".

b) Compare com a cifragem da sua dupla. Ficou igual?

□ **SIM** □ **NÃO**

c) Agora escolha uma mensagem para mandar para sua dupla decifrar.

MENSAGEM ORIGINAL:_____

MENSAGEM CIFRADA:_____

d) Ela decifrou corretamente?

□ **SIM** □ **NÃO**

● Sistema de Vigenère

Os interessados na mensagem devem compartilhar uma chave, que pode ser uma letra, uma palavra ou até mesmo uma frase. O processo de cifragem da mensagem é descrito assim: escreve-se o texto original e acima escreve-se a chave, sincronizando letra por letra, repetindo-a quantas vezes sejam necessárias. Utilizando a tábula recta, a primeira linha será a referência para as letras da chave e a primeira coluna será a referência para as letras da mensagem. Assim, se sobre uma letra do texto encontra-se uma determinada letra da chave, ela será substituída pela correspondente na sua linha e coluna da letra da chave. Para decifrar a mensagem basta fazer o caminho inverso. Veja:

CHAVE	O	L	A		O	L	A	O	L
MENSAGEM ORIGINAL	B	O	A		N	O	I	T	E
MENSAGEM CIFRADA	P	Z	A		B	Z	I	H	P

5) Compartilhe com sua dupla a chave que será utilizada para cifrar e decifrar as mensagens.

CHAVE:_____

6) Conhecendo a chave:

a) Cifrem a mensagem “ALUNO NOTA DEZ”.

b) Compare a mensagem cifrada com sua dupla. Ficou igual?

□ **SIM** □ **NÃO**

c) Envie uma mensagem para sua dupla decifrar.

MENSAGEM ORIGINAL:_____

MENSAGEM CIFRADA:_____

d) Ela decifrou corretamente?

□ **SIM** □ **NÃO**

Anexo III

E M JOAQUIM DA SILVA GOMES
OFICINA DE MATEMÁTICA

ALUNO(A):_____
PROFESSOR: IGOR NASCIMENTO

Aplicação de aritmética modular na criptografia

Durante muito tempo o problema da distribuição das chaves foi uma barreira para os criptoanalistas, mas a busca incessante da solução deste problema desencadeou a descoberta do sistema de codificação mais seguro há quase quatro décadas, o RSA. A aritmética modular foi uma ferramenta de suma importância para que este sistema fosse descoberto e é a base do seu funcionamento. Vejamos um exemplo prático.

Para facilitar o nosso exemplo vamos considerar os personagens fictícios Gabriela e Matheus. Suponha que a Gabriela deseja mandar para o Matheus um simples **N** como uma resposta negativa de uma pergunta anterior do Matheus.

● Matheus escolhe dois números primos **p** e **q** suficientemente grandes, mas para facilitar o nosso exemplo vamos considerar p =17 e q = 11. Estes números devem ser mantidos em sigilo. A princípio parece óbvio descobrir os valores de **p** e **q** conhecendo o valor de **N**, mas a fatoração de números cujos fatores são números primos suficientemente grandes não é uma tarefa fácil nem mesmo para os computadores.

● Matheus então multiplica p e q obtendo N = 187. E em seguida o Matheus escolhe um número α (código de cifragem), neste caso ele escolhe α = 7. Os valores de N e α podem ser amplamente divulgados e juntos são chamados de chave pública.

OBS: α e (p – 1).(q – 1) devem der primos relativos.

● Para enviar uma mensagem primeiramente ela deve ser convertida em números binários conforme a tabela ASCII. Para os nossos cálculos vamos utilizar a representação decimal, neste caso consultando a tabela ASCII a letra N é o número binário 1001110 cuja representação decimal é o número M = 78.

● Para cifrar a mensagem a Gabriela consulta a chave pública do Matheus e envia a mensagem cifrada como um número C que é obtido através da congruência $M^{\alpha} \equiv C \bmod N$, onde $C < N$ sendo assim:

$78^{7} \equiv C \bmod 187$, efetuando os cálculos com o auxílio do aplicativo Wolfram Alpha obtemos $C = 56$.

● O Matheus então recebe a mensagem $C = 56$, mas para decifrar a mensagem ele necessita calcular sua chave de decifragem β. O valor de β é calculado através da congruência $\alpha.\beta \equiv 1 \bmod (p - 1).(q - 1)$, ou seja, $7.\beta \equiv 1 \bmod 160$. Efetuando os cálculos com o recurso do aplicativo Wolfram Alpha obtém-se que $\beta = 23$ satisfaz a condição. Observe que para o cálculo da chave de decifragem é necessário conhecer os valores de p e q.

● Calculada sua chave de decifragem o Matheus então decifra a mensagem da seguinte forma:

$C^{\beta} \equiv M \bmod N$, onde $M < N$. Neste caso então $56^{23} \equiv M \bmod 187$, mais uma vez recorrendo ao aplicativo Wolfram Alpha obtemos $M = 78$, ele então consulta a tabela ASCII e verifica que a mensagem da Gabriela é **N**.

Anexo IV

E M JOAQUIM DA SILVA GOMES
OFICINA DE MATEMÁTICA

ALUNO(A):_____
PROFESSOR: IGOR NASCIMENTO

QUESTIONÁRIO

1) O que você achou da proposta da oficina?

2) Aprendeu algo novo?

3) O que achou mais interessante?

4) Você acha que estes conteúdos poderiam ser estudados no ensino fundamental?

5) Comentários: