PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo845

Criptografia RSA na Educação Básica: uma necessidade no mundo atual

Danilo de Araújo Moura

Resumo

Este artigo abordará a história da Criptografia e uma aplicação da Criptografia RSA, sigla correspondente às iniciais de seus autores, utilizando congruência, na educação básica, corroborando para difusão de conteúdos aplicados de tecnologia através de conceitos matemáticos, bem como favorecendo o debate sobre a segurança da informação, temáticas fundamentais no mundo atual.

Palavras-chave: Segurança da Informação, Contexto e Problemas da Educação Brasileira; Surgimento da Criptografia; Implantação dos Computadores; O sistema RSA; Metodologia para Desenvolvimento em Sala do Sistema RSA; Aplicação do Sistema RSA.

Abstract

Information Security, Context and Problems of Brazilian Education; Emergence of Cryptography; Computer Deployment; The RSA Method; RSA System Development Methodology; Application of the RSA System.

Keywords: Information Security, Context and Problems of Brazilian Education; Emergence of Cryptography; Computer Deployment; The RSA Method; RSA System Development Methodology; Application of the RSA System.

1. Introdução

Como forma de contextualizar os conceitos de criptografia e segurança da informação, irei, primeiramente, abordar o estado da arte, juntamente com os problemas enfrentados pela educação brasileira.

Atualmente, na era digital, há uma grande preocupação com a garantia da segurança das informações. No Brasil, por exemplo, a certificação digital iniciou-se com o surgimento da infraestrutura de Chaves Públicas, segundo a medida provisória 2.200-2/2001. O certificado digital é um arquivo em meio eletrônico, em que são encontradas informações do usuário (pessoa física ou jurídica) de um estipulado local, garantindo a respectiva identidade e assegurando, por conseguinte, os princípios de segurança da informação (confidencialidade, autenticidade, autoria e não repúdio), tendo como pressuposto as transações eletrônicas assinadas, bem como o intercâmbio de informações, preservando, assim, a integridade, o sigilo e a segurança. Logo, o arcabouço, para esse processo, deve-se ao usufruto da criptografia e padrões específicos.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

No entanto, as medidas para salvaguardar os verdadeiros destinatários da informação não se restringem ao ambiente nacional. A comunidade internacional vive, constantemente, preocupada com a segurança de seus dados, e aqui podemos citar o episódio envolvendo o ex-administrador da CIA (Central Intelligence Agency) e ex-contratado da NSA (National Security Agency), Edward Joseph Snowden, que abalou o mundo, colocando em xeque os meios de segurança das diversas nações. Além disso, existiram escândalos sobre divulgações de informações particulares dos usuários da maior rede social do mundo, o Facebook, gerenciada por Mark Elliot Zuckerberg, deixando-nos os seguintes questionamentos: Até que ponto nossas informações estão protegidas? Podemos confiar nos meios cibernéticos? Será que devemos abandoná-los em definitivo? Existe um meio de melhorar a segurança cibernética?

Por outro lado, o acesso à internet banda larga de qualidade e irrestrito é uma oportunidade valiosa para uma nação, pois favorecerá o desenvolvimento tecnológico, o crescimento econômico, a diminuição das fronteiras, o ensino inovador e a escalada da produção, a título de exemplo. Além disso, a revista *Exame* de 4 de março de 2020, cuja capa é DEVS (Desenvolvedores de *software*) ratifica a importância do aprimoramento da tecnologia da informação, ressaltando o crescimento exponencial das Startups nas potências mundiais e no Brasil, além das projeções futuras, deixando evidente a importância da ciência de dados para o progresso das nações. O lado indigesto, essencialmente para o nosso país, deve-se à falta de profissionais qualificados nas áreas de tecnologia, ciência, engenharia e matemática. Brasileiros preparados nessas áreas, que desenvolvem *softwares*, são assediados por várias multinacionais e escolhem onde querem exercer suas atribuições bem como a remuneração que acham justas receber, conforme a reportagem. Tudo isso diante de um cenário de crescimento econômico pífio e, ainda, elevados índices de desempregos na República, ou seja, panorama oposto às estatísticas tristes vivenciadas pelo povo brasileiro.

Na perspectiva da singularidade – expressão utilizada no campo da Física para representar eventos extremos desprovidos de equações associadas, ou seja, trata-se de um campo além do previsível – trago a visão do engenheiro e futurista Ray Kwrzweil que considera que a singularidade ocorrerá nos próximos 30 anos. Na matéria publicada no *site* da UOL vestibulares, na parte de atualidade, intitulado: *Você sabe o que é Inteligência Artificial e Singularidade?*, Carolina Cunha retrata muito bem as projeções de Ray, sendo uma delas representada no seguinte trecho:

,

> *"... se imaginarmos o crescimento exponencial no século 21 como uma curva exponencial, ele será equivalente a 20 anos de progresso na velocidade atual"* (Ray Kwrzweil).

Em outro fragmento do artigo, é enaltecido o desenvolvimento tecnológico, como segue:

,

> *"...um computador de mil dólares tem hoje a mesma inteligência de um inseto. No futuro, ele se igualará à capacidade de um rato, de um homem e, finalmente, de toda a humanidade"* (Ray Kwrzweil).

Logo, certos autores, como Ray, vislumbram, em um futuro próximo, a inteligência artificial, em que as próprias máquinas desenvolverão outras mais funcionais sem influência humana.

Diante do retrato mundial, atual e futuro, assim como o exposto anteriormente, percebe-se a necessidade de um aprimoramento constante dos meios de segurança da informação, pois a tecnologia das coisas, da ciência de dados e a transparência digital são fundamentais no mundo competitivo e avançado, e negligenciá-los é naufragar no retrocesso, na desigualdade e no descaso com o futuro de toda uma sociedade. O Brasil, observando o cenário internacional e os relatos acadêmicos, implementou, como objetivo estratégico, o E-Digital – estratégia brasileira para a transformação digital, tendo como um dos temas a confiança no ambiente digital, consoante a imagem abaixo.

Figura 1: *Temas para Transformação Digital Brasileira* (E-Digital, 2018, p.9)

É relevante considerar, também, que um dos grandes problemas enfrentados pela educação nacional é a má formação e a baixa qualidade no ensino de disciplinas atreladas à tecnologia, tais quais ciência, engenharia e matemática, conforme p.19 e p.26 da revista *Exame*, edição 1204, de 4 de Março de 2020. O fato contribui para enormes dificuldades econômicas enfrentadas pelo Brasil ao longo dos anos, gerando grandes *deficits* de profissionais no crescente setor de tecnologia da informação. Ademais, a mesma reportagem da revista *Exame*, edição 1204, de 4 de Março de 2020, página 26, traz o resultado do Pisa e do Enade de 2019, como segue:

,

> *Em 2019, os resultados do Programa Internacional de Avaliação de Estudante (Pisa, na sigla em inglês) mostraram que dois terços dos alunos brasileiros de 15 anos sabiam menos do que o essencial em Matemática. Considerando também as áreas de*

> *leitura e ciência, apenas 2,5% dos estudantes atingiram notas de "alto desempenho" na prova. A média da Organização para Cooperação e Desenvolvimento Econômico (OCDE) é de 15,7%. Essa defasagem continua no ensino superior. Em 2018, apenas 1,7% dos cursos universitários conseguiu nota máxima no Exame Nacional dos Estudantes* (Revista *Exame*, 2020, p.26).

Portanto, observa-se a falta de políticas públicas de incentivo à educação básica, e os reflexos estão nos dados apresentados acima.

Em mais algumas investigações, podemos verificar que há uma lacuna de profissionais trabalhando nas áreas tecnológicas, segundo destaca a mesma reportagem, agora na página 19, no relato abaixo.

,

> *No país há, atualmente, apenas 2 milhões de trabalhadores graduados nas áreas de ciência, tecnologia, engenharia e matemática, o correspondente a 1,9% da força de trabalho, segundo dados da Organização para Cooperação e Desenvolvimento Econômico. De 2019 a 2024, de acordo com Cálculo do Brasscom, a demanda média deve ser de 70.000 profissionais por ano. No entanto, em 2017, de 46.000 profissionais formados, apenas 26.000 entraram no mercado de trabalho, evidenciando uma defasagem no currículo das instituições. Nesse ritmo, ao final do período de seis anos, o* deficit *chegaria a 264.000* (Revista *Exame*, 2020, p.19).

Figura 2: *Gráficos* (*Exame*, 2020, p.19)

Agora, após essa explanação do cenário vigente, temos, iniciando, de fato, o conteúdo, que a criptografia moderna edificou-se em torno dos anos 70 do século XX. Até aquele momento, a Teoria dos Números, da qual a Aritmética é o componente mais primário, era apontada como um dos ramos mais genuínos e abstratos da Matemática, desconectada de qualquer tipo de aplicação concreta. Essa visão modificou-se com o desenvolvimento da Teoria da Informação, que inclui a criptografia, dentre outros tópicos, entusiasmada pelo progresso e disseminação dos computadores e a capacidade de conexão com as grandes redes mundiais. Rotineiramente, a criptografia estava vinculada ao sigilo militar, no entanto foi o manuseio exorbitante dos computadores, pelo público, para assuntos variados, que mais atraiu a expansão da criptografia moderna.

A proposta de resguardar os meios de comunicação gerados por certa população advém do início da civilização, e o pensamento de tutelar os instrumentos de comunicação, bem como o conteúdo da mensagem, pelo método da cifração é, também, rudimentar.

,

> *A criptografia é o estudo de métodos para enviar e receber mensagens secretas. Em geral, há um emissor que tenta enviar uma mensagem para um receptor. Existe também um adversário que deseja interceptar a mensagem. O método utilizado será considerado bem-sucedido se o remetente for capaz de transmitir uma mensagem para o receptor sem que o adversário descubra em que ela consiste* (Stein, 2013, p. 49).

Em Roma, Júlio César utilizou uma criptografia singela para realizar a interlocução com o seu exército. Em sua cifra, na transmissão do conteúdo original, cada letra era lançada três posições à direita e o alfabeto restringia-se a ele mesmo. Ao longo dos tempos, a codificação das frases tornou-se uma atividade cada vez mais elaborada, e o surgimento dos computadores potencializou a comunicação entre as pessoas, bem como diminuiu as distâncias, porém, o meio cibernético não é tão seguro e, nesse contexto, a criptografia expande em importância para assegurar a cifração das informações.

,

> *Não ser decifrado por um adversário é um objetivo difícil. Nenhum código é completamente indecifrável. Se houver um livro de códigos impresso, o adversário poderá roubá-lo. Nem toda a sofisticação matemática pode impedir essa possibilidade já que um adversário pode ter grande poder de computação e recursos humanos dedicados a tentar decifrar um código* (Stein, 2013, p.49).

Um método criptográfico relevante chamado RSA, sigla correspondente às iniciais de seus autores, e bastante difundido no cenário atual, usufrui de conteúdos da Teoria dos Números, em especial congruência e números primos, para desenvolver todo um encadeamento lógico, com auxílio de chaves assimétricas, para proceder a uma significativa segurança na atividade de decifração.

Em razão do exposto, o artigo científico mostrará um pouco da história da criptografia e a utilização da congruência para o desenvolvimento da criptografia RSA, tendo em vista a aplicação de conceitos de Teoria dos Números na educação básica, estimulando, assim, os discentes na inserção do debate da segurança da informação. Ressalto, também, que os conceitos elementares de congruência são pré-requisitos para o bom entendimento do artigo, pois eles devem estar inseridos no currículo dos discentes da educação básica;e enalteço, por fim, a importância da matemática nessa perspectiva toda, sem deixar de influenciar a formação de novos profissionais de outras áreas atreladas às Ciências Exatas e à Tecnologia.

2. Surgimento da Criptografia

A origem da palavra criptografia vem do grego, em que *kriptos* significa oculto, e, assim, criptografia representa "escrita oculta". Há relato de que persas, gregos e chineses desfrutavam de inúmeras práticas para ocultar mensagens. O desenvolvimento criptográfico foi no intuito de não mais esconder fisicamente as mensagens, entretanto desfrutar de artimanhas para encobrir sua interpretação ao público que não correspondessem aos verdadeiros destinatários delas, de maneira que pudessem ser disponibilizadas por meio de um instrumento público de comunicação. É interessante observar que um método utilizado com frequência em Roma, por Júlio César, conhecido como cifra de César, foi fundamentado em ideias criptográficas.

,

> *A criptografia tradicional é conhecida como criptografia de chaves secretas. O remetente e o destinatário concordam com antecedência sobre um código secreto e, em seguida, enviam mensagens usando-o. Por exemplo, um dos mais antigos códigos é uma cifra de César* (Stein, 2013, p.50).

Tal sistema traduz-se em substituir cada letra do alfabeto, na mensagem primária, por outra letra do alfabeto, conforme uma regra bem estipulada. Esse dispositivo criptográfico é nomeado de cifra de substituição simples, no qual as letras de um alfabeto são trocadas por outras. A cifra de César detém ao menos 25 variantes. Um dos pontos vulneráveis nos sistemas criptográficos por substituição simples é o fato de, em um conteúdo (em relação a determinada língua), as letras do alfabeto aparecerem em períodos diversos, além de haver certas disposições rígidas de contato entre elas – conforme o idioma português, que apresenta, com muita intensidade, letras que se seguem após a utilização de outras, como a letra q seguida de u, fornecendo rastros úteis aos que se dedicam ao exercício da quebra dos códigos de outrem: os criptoanalistas. Um método para alterar a análise de frequência é relacionar a cada letra, com periodicidade alta, diversos símbolos diferentes, que estão associados só a essa letra. Ainda assim, o diagnóstico do contato entre letras e a estrutura linguística dá indícios sobre como desvendar um desses códigos. Por outro lado, existe outra linha de sistema criptográfico consubstanciada na transposição, isto é, na geração de anagramas da mensagem original. Por exemplo, um conteúdo com 15 letras origina 15! permutações dissemelhantes das letras, e para mensagem com um número elevado delas, a alta quantidade de permutações torna bastante complicada a tarefa de decifrar, na hipótese de não deter a chave para tal. A grande problemática do molde citado é que a mudança de chaves, entre os clientes do sistema, fica árdua na conjuntura de existirem muitos deles longe uns dos outros, pois demanda uma chave diferente para cada par de usuários. Percebeu-se, então, que a junção dos métodos de substituição de letras e transposição dava origem a sistemas criptográficos mais satisfatórios. O arquiteto italiano Leone Battista Alberti, considerado o pai da criptografia ocidental, sugeriu uma nuance bem mais elaborada da cifra de César, com a utilização da relação de substituição polialfabética. Referia-se ao usufruto de uma aparelhagem designada disco de Alberti, composta de dois discos de mesmo centro com diâmetros distintos, presos por um pino central, o menor sobre o maior, podendo o disco menor girar. Os discos eram fragmentados em 24 grupos similares em que, na borda do disco maior, estavam inscritos, no sentido horário, as seguintes 20 letras: A, B , C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, e Z. Além dos números 1, 2, 3 e 4, um em cada setor. Já na extremidade do disco menor, estavam inscritos, em ordem arbitrária, as letras minúsculas do alfabeto, à exceção das letras j ,u e w, além da palavra do latim *et.*

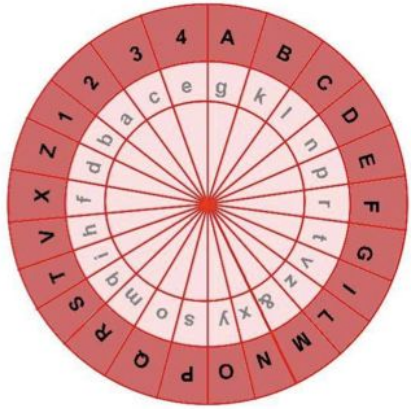


Figura 3: *Disco de Alberti*

,

> *A grande inovação de Alberti foi o uso de cifras polialfabeticas, como segue: a cada grupo de algumas palavras (quatro ou cinco), o pequeno disco é girado aleatoriamente e a nova letra do disco menor correspondente à letra A no disco maior é inserida na mensagem original, indicando que a partir daquele momento é essa a nova posição do disco rotativo (o menor), com relação ao disco fixo (o maior)* (Hefez, 2016, p. 268).

Johannes Trithemius contribuiu significativamente para o avanço da criptografia com a obra nomeada *Poligrafia*, publicado em 1518. No livro, ele descreve um novo método utilizando a *tabula recta*, dispondo de uma tabela, nomeada de *tabula recta*, com a igualdade de linha e colunas, observando que na primeira linha ficará o alfabeto em ordem convencional e, a partir das demais linhas, haverá uma permutação circular da linha anterior. Ele descreve o passa a passo no seguinte trecho:

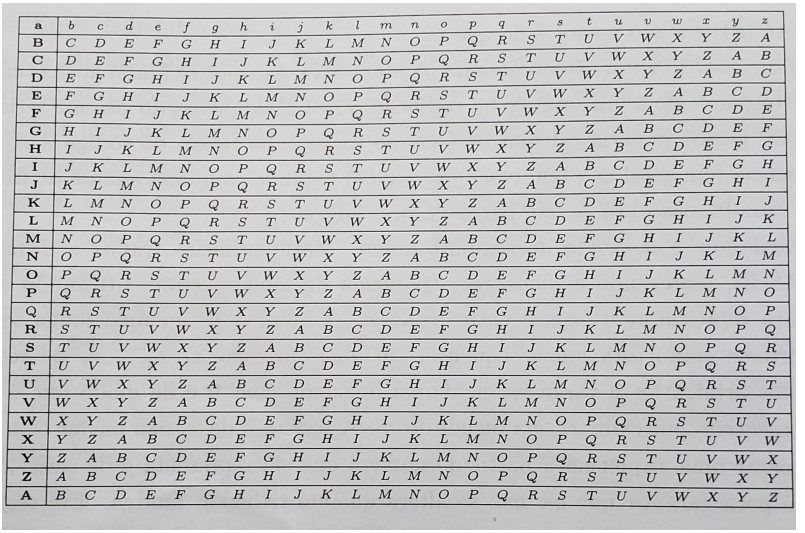
,

> *A cifragem procederia da seguinte forma: a primeira letra da mensagem a ser cifrada é transformada na letra correspondente da segunda linha, a segunda letra é transformada na letra correspondente da terceira linha e assim sucessivamente até esgotar todas as linhas quando se volta para a segunda linha novamente.* (Hefez, 2016, p.268 e p.269)

A tabela posterior, foi retirada do livro *Aritmética- Coleção Profmat- p.276* e retrata a *Tabula recta.*

Analisando a figura acima e seguindo os passos sugeridos na última citação temos, por exemplo, para a palavra:

CRIPTOGRAFIA,



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 4: *Tabula recta*

a seguinte cifra:

DTLTYUNZJPTM.

Em 1553, com o trabalho do italiano Giovanni Battista Bellaso, divulgado no curto livro *La cifra del seig Giovan Batista Belaso*, foi adotado o pensamento de chave para cifrar e decifrar uma mensagem. O dispositivo faz uso da *tabula recta*, além de compartilhar uma chave, que pode ser uma palavra, um conjunto de letras ou uma frase. Tendo a chave, registra-se em uma linha o conteúdo a ser cifrado e, na linha acima, as letras da chave sobre as letras do texto, repetidas o quanto for necessário.

,

> *A cifragem de Giovanni Battista Belloso ocorre da seguinte forma: caso sobre uma dada letra do texto encontra uma determinada letra da palavra-chave, então substitui essa por aquela que lhe corresponde na sua coluna e na linha que começa com a letra da palavra-chave.* (Hefez, 2016, p.269)

Imagine, a título de exemplo, que a chave seja "Aritmética" e a mensagem enviada, através desse sistema, seja Teoria dos Números. Desta maneira, a cifragem aconteceria do seguinte modo:

aritme tic aaritme

teoria dos numeros

TVWKUE WWU NUDMKAW

Observe que, para cifrar e decifrar, de acordo com o método, recorre-se à mesma chave. O dispositivo foi considerado penoso de ser quebrado, porque era resistente à análise de frequência, visto que uma mesma letra pode ser exibida por diversas outras e existe um número enorme de chaves possíveis. Com a publicação do livro *Traicté des Chiffres*, em 1586, Blaise de Vigenère implementa um sistema baseado em Bellaso, que propõe o conceito de autochave, isto é, a utilização do texto em si como chave. A proposta institui-se de forma que os correspondentes compartilhavam uma chave comum, que era uma letra, e a utilizavam como chave no método de Bellaso para codificar a primeira letra do conteúdo. Posteriormente, essa letra inicial era constituída como chave para cifrar a segunda letra do conteúdo e assim sucessivamente.

Os métodos de cifragem não foram bastante praticados por serem muito desgastantes em suas construções e pelo fato de, observado um erro no processo, gerar uma mensagem praticamente perdida. Por isso, foram empregados, em seus lugares, os livros de códigos intitulados *nomenclators*, em que palavras eram cifradas em espécies de dicionários produzidos com esse efeito. A cifra de Bellaso foi quebrada por volta do século XIX, depois de um longo tempo dada como infalível.

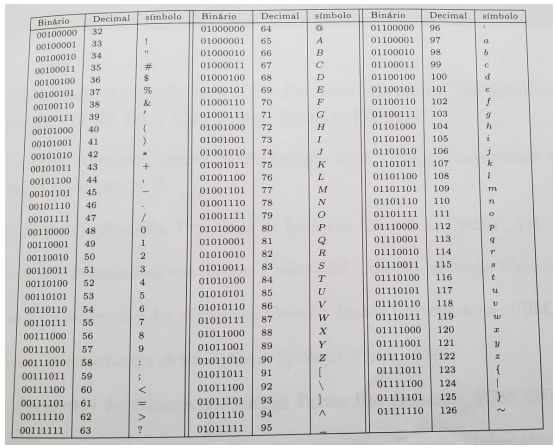
Uma característica relevante é que qualquer dispositivo criptográfico precisa de uma troca de chaves para que as partes possam decifrar as frases que lhes são enviadas e, além disso, deve fazer chegar ao destinatário, de forma segura, a chave da cifra.

Portanto, os métodos criptográficos comentados até aqui fazem uso da mesma chave para cifrar e decifrar um dado conteúdo, ou seja, operam-se com fundamentos nas chaves simétricas.

3. Implementação dos Computadores

Com a chegada dos computadores (PCs), ocorreria uma reviravolta na Teoria da Informação. A popularização dos PCs obrigou uma procura por padronização nos processos. Pelo fato de eles fazerem uso de códigos binários, toda estrutura deveria ser moldada nesse formato. Daí, surgiu o *American Standard Code for Information Inter Change* (ASCII) que significa código padrão americano para o intercâmbio de informação. Tal codificação, construída desde 1960, não representa um sistema de cifragem e sim a tradução para a linguagem binária dos símbolos mais representados. Assim, incorporou-se o código ASCII. Com isso, necessitava-se, agora, uniformizá-lo para o uso de sistemas criptográficos. Foi então que, em 1973, o National Bureau of Standards escolheu o sistema criptográfico Data Encryption Standard (DES), construído pela IBM, com o intuito de ser o sistema oficial americano. O DES era muito complexo e utilizava chaves simétricas, o que ensejava uma grande problemática logística de distribuição de chaves, levando ao surgimento de outros métodos.

A figura abaixo, anexa do livro de *Aritmética-Coleção Profmat-p.277*, mostra a Tabela de código ASCII.



Binário	Decimal	símbolo	Binário	Decimal	símbolo	Binário	Decimal	símbolo
00100000	32		01000000	64	@	01100000	96	`
00100001	33	!	01000001	65	A	01100001	97	a
00100010	34	"	01000010	66	B	01100010	98	b
00100011	35	#	01000011	67	C	01100011	99	c
00100100	36	$	01000100	68	D	01100100	100	d
00100101	37	%	01000101	69	E	01100101	101	e
00100110	38	&	01000110	70	F	01100110	102	f
00100111	39	'	01000111	71	G	01100111	103	g
00101000	40	(	01001000	72	H	01101000	104	h
00101001	41	)	01001001	73	I	01101001	105	i
00101010	42	*	01001010	74	J	01101010	106	j
00101011	43	+	01001011	75	K	01101011	107	k
00101100	44	,	01001100	76	L	01101100	108	l
00101101	45	−	01001101	77	M	01101101	109	m
00101110	46	.	01001110	78	N	01101110	110	n
00101111	47	/	01001111	79	O	01101111	111	o
00110000	48	0	01010000	80	P	01110000	112	p
00110001	49	1	01010001	81	Q	01110001	113	q
00110010	50	2	01010010	82	R	01110010	114	r
00110011	51	3	01010011	83	S	01110011	115	s
00110100	52	4	01010100	84	T	01110100	116	t
00110101	53	5	01010101	85	U	01110101	117	u
00110110	54	6	01010110	86	V	01110110	118	v
00110111	55	7	01010111	87	W	01110111	119	w
00111000	56	8	01011000	88	X	01111000	120	x
00111001	57	9	01011001	89	Y	01111001	121	y
00111010	58	:	01011010	90	Z	01111010	122	z
00111011	59	;	01011011	91	[	01111011	123	{
00111100	60	<	01011100	92	\	01111100	124	|
00111101	61	=	01011101	93	]	01111101	125	}
00111110	62	>	01011110	94	^	01111110	126	~
00111111	63	?	01011111	95	_			

Figura 5: *Tabela de Código ASCII*

Observação: A tabela de código ASCII é apenas uma exemplificação, usada somente para ilustrar. Ela não foi utilizada ao longo do artigo para fazer codificações, portanto, os símbolos e números constantes no artigo não estão associados a ela.

Retomando, temos que o desafio, portanto, voltava-se a desvendar um modo lógico de troca de chaves entre correspondentes e combater o paradigma da impossibilidade da troca de senhas sem a intermediação de um portador. Whitfield Driffie, Martin Hellman e Ralph Merkle utilizaram uma ideia brilhante, baseada na Teoria dos Números, para desmistificar o paradigma. Eles fizeram uso de conceitos de congruência para tentar solucionar o imbróglio da distribuição de chaves. O pensamento dos americanos dá-se da seguinte forma: Pedro e Camila querem trocar entre si uma chave secreta através de uma comunicação não segura. Eles chegam ao consenso sobre um par de números s e t e os tornam públicos. Pedro escolhe um novo número natural c e o mantém em segredo. Com ele, calcula o único número $z < t$ tal que $s^c \equiv z \bmod t$, e o envia para Camila. Por sua vez, Camila indica um número natural h, mantendo-o secreto, e, com ele, calcula o único número $f < t$ tal que $s^h \equiv f \bmod t$; e posteriormente o envia para Pedro.

Daí, Pedro calcula f^c, obtendo:

$$f^c \equiv (s^h)^c \equiv s^{hc} \equiv k \bmod t \text{ , com } k < t.$$

Depois, Maria calcula z^h, extraindo:

$$z^h \equiv (s^c)^h \equiv s^{ch} \equiv k \bmod t \text{ , com } k < t.$$

Concluído! Está trocada a chave secreta k entre Pedro e Camila. Então, são públicas as informações s, t, z, f e são secretas as informações c, que só Pedro conhece, h, que somente Camila sabe, e k, que apenas Pedro e Camila têm.

Vamos mostrar uma aplicação, ou seja, um exemplo para tornar mais didática a ideia em sala de aula. Suponha que Pedro e Camila tenham escolhido de comum acordo $s = 14$ e $t = 151$. Por sua vez, Pedro elege $c = 3$ como sua chave secreta, enquanto Camila escolhe $h = 5$. Fazendo a análise para saber qual a chave k que eles compartilham, obtêm-se:

1. 1 - Pedro elabora a seguinte conta para determinar z e enviá-lo à Camila:

$$s^c \equiv z \bmod t \Rightarrow 14^3 = 14^2 \cdot 14 = 196 \cdot 14 \equiv 45 \cdot 14 = 630 \equiv 26 \bmod 151.$$

Então, z = 26.

Agora, Camila faz o seguinte cálculo para encontrar f e encaminhá-lo a Pedro:

$s^h \equiv f \bmod t \Rightarrow 14^5 = 14^2 \cdot 14^2 \cdot 14 = 196 \cdot 196 \cdot 14 \equiv 45 \cdot 45 \cdot 14 = 630 \cdot 45 \equiv 26 \cdot 45 = 1170 \equiv 113 \bmod 151$.

Para determinar a chave k, Pedro tem que reduzir $f^c = 113^3$ módulo 151.

Daí, $113^2 \cdot 113 = 12769 \cdot 113 \equiv 85 \cdot 113 = 9605 \equiv 92 \bmod 151$. Pedro encontra, por conseguinte, k = 92.

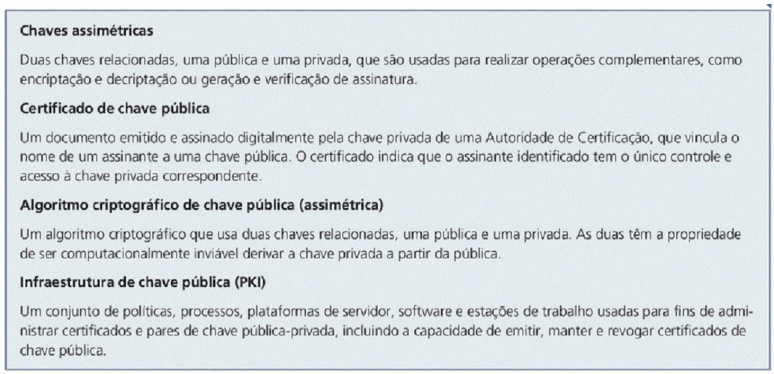
2. 2- Para Maria, tem-se:

$z^h = 26^5$ módulo 151. Porém, $26^5 = 26^2 \cdot 26^2 \cdot 26 = 676 \cdot 676 \cdot 26 \equiv 72 \cdot 72 \cdot 26 = 5184 \cdot 26 \equiv 50 \cdot 26 = 1300 \equiv 92 \bmod 151$. Logo, k = 92, como queríamos mostrar.

O êxito desse método consiste na dificuldade de desvendar qualquer dos três números c, h e k, sabendo somente os dados públicos s, t, z e f. Naturalmente, dado $x \in N$, é de certa forma trivial calcular o resto da divisão de s^x por t, no entanto não é fácil o caminho oposto, ou seja, dado $y \in N$, é trabalhoso achar $x \in N$ de tal forma que y é o resto da divisão de s^x por t. Os restos da divisão de s^x por t, ao variar x, estabelecem-se de maneira caótica. Essa ferramenta tem o defeito de trocar chaves entre dois indivíduos por vez, e, portanto, não é satisfatória no mundo global.

Driffie teve o pensamento de utilizar chaves assimétricas, isto é, cada pessoa teria duas chaves: uma pública, para codificar a mensagem e, outra privada, para decodificá-la. O sistema deveria ser fácil para cifrar e praticamente impossível, sem o uso da chave secreta, para decodificar. Ele somente publicou a teoria e não fez nada na prática.

O quadro abaixo foi extraído do livro *Criptografia e Segurança de Redes: Princípios e Práticas, p.200,* e faz alusão aos aspectos da criptografia assimétrica.



Chaves assimétricas

Duas chaves relacionadas, uma pública e uma privada, que são usadas para realizar operações complementares, como encriptação e decriptação ou geração e verificação de assinatura.

Certificado de chave pública

Um documento emitido e assinado digitalmente pela chave privada de uma Autoridade de Certificação, que vincula o nome de um assinante a uma chave pública. O certificado indica que o assinante identificado tem o único controle e acesso à chave privada correspondente.

Algoritmo criptográfico de chave pública (assimétrica)

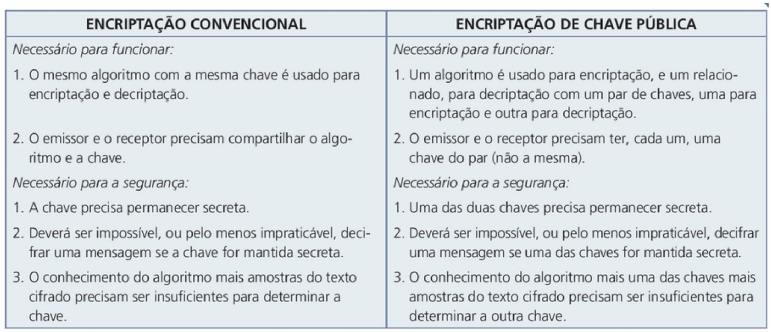
Um algoritmo criptográfico que usa duas chaves relacionadas, uma pública e uma privada. As duas têm a propriedade de ser computacionalmente inviável derivar a chave privada a partir da pública.

Infraestrutura de chave pública (PKI)

Um conjunto de políticas, processos, plataformas de servidor, software e estações de trabalho usadas para fins de administrar certificados e pares de chave pública-privada, incluindo a capacidade de emitir, manter e revogar certificados de chave pública.

Figura 6: *Terminologia relacionada à criptografia assimétrica*

Já o resumo seguinte, por fim, elucida as principais divergências entre a encriptação simétrica (convencional) e a de chaves públicas. A imagem foi tirada, também, do livro *Criptografia e Segurança de Redes: Princípios e Práticas, p.203.*



ENCRIPTAÇÃO CONVENCIONAL	ENCRIPTAÇÃO DE CHAVE PÚBLICA
Necessário para funcionar:	*Necessário para funcionar:*
1. O mesmo algoritmo com a mesma chave é usado para encriptação e decriptação.	1. Um algoritmo é usado para encriptação, e um relacionado, para decriptação com um par de chaves, uma para encriptação e outra para decriptação.
2. O emissor e o receptor precisam compartilhar o algoritmo e a chave.	2. O emissor e o receptor precisam ter, cada um, uma chave do par (não a mesma).
Necessário para a segurança:	*Necessário para a segurança:*
1. A chave precisa permanecer secreta.	1. Uma das duas chaves precisa permanecer secreta.
2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se a chave for mantida secreta.	2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se uma das chaves for mantida secreta.
3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Figura 7: *Encriptação convencional e de chave pública*

4. O Sistema RSA

Ronald Rivest, Adi Shamir e Leonard Adlman deram, em 1978, um importante progresso no sistema criptográfico idealizado por Driffie. O propósito foi fundamentado na aparente facilidade de encontrar números primos grandes e, simultaneamente, na extrema dificuldade concreta em fatorar o produto de dois desses números, além do uso de fundamentos elementares da Teoria dos Números, conforme a variante do Teorema de Euler ilustrado no Corolário 1.

,

> *Diffie e Hellman apresentaram publicamente os conceitos da criptografia de chaves públicas em 1976. Hellman dá créditos a Merkle com a descoberta independente e simultânea do conceito, embora Merkle não o tenha publicado antes de 1978 [6]. De fato, o primeiro documento não confidencial descrevendo a distribuição de chaves públicas e a criptografia foi uma proposta de projeto de 1974 por Merkle http://merkle.com/1974. Esse, porém, não foi o verdadeiro início. O almirante Bobby Inman, como diretor da National Security Agency (NSA), reivindicou que a criptografia de chave pública tinha sido descoberta na NSA em meados da década de 1960 [8] . A primeira apresentação documentada desses conceitos veio em 1970, do Communucations-Electrons Security Group, o equivalente britânico da NSA, em um relatório confidencial de James Ellis [3]. Ellis referia-se à técnica como criptografia não secreta, e descreve a descoberta em [2]* (Stalling, 2015, p.201).

,

> *O artigo pioneiro de Diffie e Hellaman [1] introduziu uma nova técnica para criptografia e, com efeito, desafiou os criptologistas a encontrarem um algoritmo criptográfico que atendesse os requisitos para os sistemas de chave pública. Diversos algoritmos foram propostos. Alguns deles, embora inicialmente promissores, provaram ser falhos* (Stalling, 2015, p.207).

,

> *Uma das primeiras respostas ao desafio foi desenvolvido em 1977 por Ron Rivest, Adi Shamir e Len Adleman, no MIT, e publicado em 1978 [7]. O esquema Rivest-Shamir-Adleman (RSA), desde essa época, tem reinado soberano como a técnica de uso geral mais aceita e implementada para a encriptação de chaves públicas* (Stalling, 2015, p.207).

Com isso, procurava-se um sistema criptográfico com duas chaves, uma pública e uma privada, para que qualquer pessoa pudesse codificar um conteúdo previamente cifrado em ASCII e somente o seu autêntico destinatário pudesse decifrá-lo.

A proposta, nesse caso, foi construída assumindo, por exemplo, que Pedro quer criar um sistema criptográfico em que uma pessoa encaminhe para ele uma frase cifrada, com uma chave pública, e que ele, e só ele, possa decodificá-la com sua chave secreta.

Então, Pedro escolhe dois números primos p e q muito grandes e, posteriormente, efetua o seu produto, ou seja, $n = p \cdot q$.

Observação: Perceba que é tranquilo encontrar o algarismo n, mas é muito difícil, e computacionalmente duradouro fatorá-lo. Essa é a razão positiva da técnica, ou seja, um processo fácil de realizar, todavia árduo de desfazer.

Continuando o processo, Pedro escolhe uma dupla de números λ e d de modo que:

$$\lambda \cdot d \equiv 1 \bmod \phi(n),$$

onde $\phi(n) = p^{\alpha_1 - 1} \cdot q^{\alpha_2 - 1} \cdot (p-1) \cdot (q-1)$ é um caso particular da função ϕ de Euler. Além disso, como α_1 e α_2 são iguais a 1, pois $n = p \cdot q$, temos que $\phi(n) = (p-1) \cdot (q-1)$.

Observação: É fundamental que λ e $\phi(n)$ e d e $\phi(n)$ sejam coprimos. Para isso, podemos tomar λ tal que $(\lambda, \phi(n)) = 1$ e em seguida determinar a congruência $\lambda \cdot X \equiv 1 \bmod \phi(n)$.

Com isso, Pedro, enfim, disponibiliza os números n e d, ou seja, as chaves públicas, e guarda, consigo, as chaves secretas que são os primos p, q e os números $\phi(n) = (p-1) \cdot (q-1)$ e λ.

Assim, fornecendo-se um valor $b < n$, tal que ele possa ser a representação decimal[1] de um símbolo ASCII, visto conforme um número na base 2, a codificação feita por uma pessoa qualquer, que tenha a chave pública de Pedro (n, d), pode cifrar b, como segue, por exemplo, segundo os passos realizados por Camila.

Ela acha o único $A(b) < n$ tal que:

$$b^d \equiv A(b) \bmod n.$$

Com isso, ela manda A(b) para Pedro.

Pedro, ao receber A(b), utiliza sua chave privada λ para achar $E(A(b)) < n$ de tal forma que:

$$A(b)^\lambda \equiv E(A(b)) \bmod n.$$

Observe que só Pedro pode achar E(A(b)), porque ele é o único que tem a chave λ. No entanto, $E(A(b)) = b$, devido à existência de $r \in N$ tal que $\lambda.d = 1 + r.\phi(n)$. Agora analisando o corolário 1 abaixo, temos:

Corolário 1. *Seja* n *um número inteiro livre de quadrados, então para todo* $b \in Z$ *e todo* $r \in N$, *tem-se que:*

$$b^{r\phi(n)+1} \equiv b \ mod \ n$$

Demonstração. Tomando $n = p_1 \cdot p_2 \cdots p_k$, em que $p_1, p_2, \cdots, p_k$ são números primos diferentes, segue que a função ϕ de Euler, será da forma:

$$\phi(n) = \phi(p_1) \cdots \phi(p_k).$$

Com isso, fazendo $r_i = r \cdot (p_1 - 1) \cdots (p_{i-1} - 1) \cdot (p_{i+1} - 1) \cdots (p_k - 1)$ e sabendo que $8b \in Z$, $8r \in N$ e $8i = 1, \cdots, k$, segue que:

[1] Na realidade, para construção dos cálculos computacionais, não é preciso desfrutar da base 10, tudo pode ser realizado no sistema de numeração convencional da máquina

$$b^{r\cdot\phi(n)+1} = b^{r_i\cdot(p_i-1)+1} \equiv b \bmod p_i.$$

Daí, como $a \equiv b \bmod n_i, \forall i = 1, \cdots, k \Leftrightarrow a \equiv b \bmod [n_1, \cdots, n_k]$, com $a, b \in Z$ e $n, n_1, \cdots, n_k$ inteiros maiores do que 1, além de $[p_1 \cdots p_k] = p_1 \cdots p_k = n$, então obtemos o que queríamos mostrar.

□

Assim, pelo corolário anterior, segue que:

$$E(A(b)) \equiv A(b)^{\lambda} \equiv (b^{d})^{\lambda} = b^{d\lambda} = b^{r\phi(n)+1} \equiv b \bmod n,$$

onde $E(A(b))$ e b são menores do que n.

Podemos questionar que, caso Camila só cifrasse cada algarismo relacionado a um símbolo na codificação ASCII, a quebra do sistema seria rápida, pois qualquer cidadão calcularia os $A(b)$ ao variar b na tabela de códigos ASCII, e com a correlação (nem sempre biunívoca) $b \longrightarrow A(b)$ poderia, com um estudo de frequência na frase cifrada, desvendar os b através de suas imagens $A(b)$. Essa fraqueza, entretanto, é solucionada como segue:

De início, Camila traduz o conteúdo para o código ASCII, relatando a mensagem traduzida de maneira corrida, associando a sequência 0100000 para esboçar o espaço entre palavras. Logra-se, portanto, uma grande sequência de 0 e 1. Divide-se essa imensa sequência em uma sucessão $b_1, b_2, ..., b_k$ de sequências de comprimento arbitrário e diferentes, sem começar com 0 e de forma que os algarismos na base 2, associados por cada b_i seja menor que n.

,

> *A restrição de* b_i *não iniciar com zero é para poder recuperar uma sequência a partir do número que ela representa; e de cada* b_i *ser menor do que* n *é para garantir que ele não se altere quando reduzido mod* n. (Hefez, 2016, p.275)

No próximo passo, Camila acha os valores de $A(b_1), A(b_2), A(b_3), \cdots, A(b_k)$ e os encaminha para Pedro. Logo, Pedro determina $E(A(b_1)) = b_1, E(A(b_2)) = b_2, \cdots, E(A(b_k)) = b_k$ e os dispõe de modo corrido. Posteriormente, fraciona o texto em conjuntos de sete dígitos e os transmuta de ASCII para siglas comuns, e surgirá o texto que Camila propunha para Pedro.

5. Metodologia para Desenvolvimento em Sala do Sistema RSA

Sabendo da importância do desenvolvimento metodológico no intuito de qualificar o ensino no ambiente escolar, trago, resumidamente, uma estrutura distribuída em 5 etapas, para o desenvolvimento do método RSA. Tal instrumento foi baseado no portal do saber, ou seja, na perspectiva do professor Teixeira de Souza. Portanto, devemos seguir as seguintes etapas:

1. Escolha dois números primos p e q;
2. Ache a chave de codificação $n = p \cdot q$;
3. Utilize para codificar a regra $b^{\lambda} \equiv a \bmod n$, tais que $(b, n) = (a, n) = 1$ e que b e a sejam menores que n;

4. Faça a seguinte operação $\lambda \cdot d \equiv 1 \cdot \mod (p-1)\cdot(q-1)$ para encontrar d;

5. Utilize, por fim, para decodificar a regra $a^d \equiv b \bmod n$.

Observação(*): Nos variados exercícios, podemos desfrutar sempre de $\lambda = 3$, recorrendo aos primos p e q da forma:

$$p \equiv 5 \bmod 6$$

$$q \equiv 5 \bmod 6$$

Demonstração. Escolha p e q de forma que:

$$p \equiv 5 \bmod 6 \text{ e } q \equiv 5 \bmod 6,$$

podemos reescrevê-los de tal modo:

$$p \equiv 5 \bmod 6 \equiv p - 1 \equiv 4 \bmod 6$$

$$q \equiv 5 \bmod 6 \equiv q - 1 \equiv 4 \bmod 6.$$

Agora, fazendo o produto $p \cdot q$, que é o relevante, tem-se:

$(p-1)\cdot(q-1) \equiv 16 \equiv 4 \bmod 6$ e, pela divisão euclidiana, sabemos que existe um $w \in Z$, tal que:

$$(p-1)\cdot(q-1) = 6\cdot w + 4 = 6\cdot w + 3 + 1 = 3\cdot(2\cdot w + 1) + 1.$$

Daí, surge uma nova congruência com o formato:

$$3\cdot(2\cdot w + 1) \equiv -1 \cdot \bmod (p-1)\cdot(q-1) \Leftrightarrow 3\cdot(2\cdot w + 1) \equiv -1 \cdot \bmod (6\cdot w + 4).$$

Em seguida, multiplique ambos os lados da congruência por –1, encontrando:

$$3\cdot(-2w - 1) \equiv 1 \bmod (6\cdot w + 4).$$

Somando $6\cdot w + 4$ a ambos os lados da última equivalência, obtemos:

$$3(4w + 3) \equiv 1 \bmod (6w + 4).$$

Enfim, o resultado assegura que o inverso existe e, além disso, fornece um algoritmo para os cálculos; para tanto, basta tomar $\lambda = 3$, $d = 4w + 3$, $(p-1)\cdot(q-1) = 6w + 4$, $p \equiv 5 \bmod 6$ e $q \equiv 5 \bmod 6$.

□

6. Aplicação do Sistema RSA

Assumindo todo o arcabouço teórico evidenciado na seção anterior, vamos elencar um exemplo da aplicação do sistema RSA com o intuito de motivar a introdução do conteúdo, já na educação básica, contribuindo para o enriquecimento formal do discente bem como a sua inserção nas discussões de temas envolvendo segurança da informação, mostrando que a matemática está presente nessa abordagem que é fundamental para a sociedade moderna. Assim, iremos codificar a sigla **"UFG"**, fazendo uso de números primos pequenos para diminuir as contas, pensando na abordagem apresentada em sala de aula. Com isso, faremos uso dos seguintes números primos: p = 5 e q = 17. Além disso, utilizaremos a tabela de conversão abaixo.

A	B	C	D	E	F	G	H	I	J
11	12	18	19	14	21	23	24	26	27
K	L	M	N	O	P	Q	R	S	T
28	29	16	31	32	47	49	36	37	38
U	V	W	X	Y	Z				
39	51	41	42	43	44				

Tabela 1: Tabela de Conversão

Primeiramente, para solução do exercício, perceba que:

p = 5 deixa resto 5 na divisão por 6 e q = 17, também, deixa resto 5 na divisão por 6. Ou seja, $p \equiv 5 \bmod 6$ e $q \equiv 5 \bmod 6$, conforme a observação (*). Então vamos utilizar $\lambda = 3$.

Com isso, para codificar a mensagem, transforme suas letras em números, de acordo com a tabela de conversão acima. Daí, U = 39, F = 21 e G = 23. Ou seja:

39- 21- 23.

Em seguida, calculando a chave de codificação n, temos:

$$n = p \cdot q = 5 \cdot 17 = 85.$$

Aplique, agora, a relação $b^{\lambda} \equiv a \bmod n$. Assim, obtemos:

Para a 1ª letra, ou seja, $U = b_1 = 39$, $\lambda = 3$ e $n = 85$, segue que:

$39^3 = 39^2 \cdot 39 = 1521 \cdot 39 \equiv 76 \cdot 39 = 2964 \equiv 74 \bmod 85$.

Logo, $a_1 = 74$.

Para a 2ª letra, ou seja, $F = b_2 = 21$, $\lambda = 3$ e $n = 85$, segue que:

$21^3 = 21^2 \cdot 21 = 441 \cdot 21 \equiv 16 \cdot 21 = 336 \equiv 81 \bmod 85$.

Logo, $a_2 = 81$.

E, por fim, para a 3ª letra, isto é, $G = b_3 = 23$, $\lambda = 3$ e $n = 85$, segue que:

$23^3 = 23^2 \cdot 23 = 529 \cdot 23 \equiv 19 \cdot 23 = 437 \equiv 12 \bmod 85$.

Logo, $a_3 = 12$.

Encontramos, por conseguinte, o bloco codificado. Isto é:

74- 81 - 12

Para decodificá-lo, primeiramente, ache o valor de d através da congruência:

$$\lambda \cdot d \equiv 1 \bmod (p-1)\cdot(q-1).$$

Procedendo, temos:

$$3 \cdot d \equiv 1 \bmod (5-1)\cdot(17-1)$$

$$3 \cdot d \equiv 1 \bmod 4 \cdot 16$$

$$3 \cdot d \equiv 1 \bmod 64$$

Logo, d = 43.

Com d em mãos, recorra à relação:

$$a^d \equiv b \bmod n,$$

e substitua em "a" os valores 74, 81 e 12 para encontrar os b respectivos e, com isso, volte na tabela de conversão para verificar a sigla original.

Operando, encontramos:

Para $a_1 = 74$, verifica-se que:

$$\begin{aligned} 74^{43} &\equiv [(-11)^6]^7 \cdot (-11) \equiv [1771561]^7 \cdot (-11) \equiv [76]^7 \cdot (-11) \equiv \\ &\equiv [(-9)^2]^3 \cdot (-11) \cdot (-9) = [81]^3 \cdot (-11) \cdot (-9) \equiv [-4]^3 \cdot (-11) \cdot (-9) \equiv \\ &\equiv (21) \cdot (-11) \cdot (-9) = (-231) \cdot (-9) \equiv 24 \cdot (-9) = -216 \equiv 39 \bmod 85. \end{aligned}$$

Então, $b_1 = 39$, que corresponde à letra U, conforme a tabela de conversão.

Prosseguindo, para $a_2 = 81$, verifica-se que:

$$\begin{aligned} 81^{43} &\equiv [(-4)^6]^7 \cdot (-4) = (4096)^7 \cdot (-4) \equiv (16)^7 \cdot (-4) = \\ &= [(16)^2]^3 \cdot (16) \cdot (-4) = (256)^3 \cdot (16).(-4) \equiv \\ &\equiv (1)^3 \cdot (16) \cdot (-4) = -64 \equiv 21 \bmod 85. \end{aligned}$$

Logo, $b_2 = 21$, que corresponde à letra F na tabela de conversão.

E, por fim, para $a_3 = 12$, temos:

$$\begin{aligned} 12^{43} &= [(12)^6]^7 \cdot (12) = [(12)^4]^7 \cdot [(12)^2]^7 \cdot (12) = \\ &= (20736)^7 \cdot (144)^7 \cdot (12) \equiv (81)^7 \cdot [(59)^2]^3 \cdot (59) \cdot (12) \equiv \\ &\equiv (-4)^7 \cdot (3481)^3 \cdot (59) \cdot (12) \equiv (-16384) \cdot (81)^3 \cdot (708) \equiv \\ &\equiv (-64) \cdot (-4)^3 \cdot (28) = (-64) \cdot (-64) \cdot (28) = (4096) \cdot (28) \equiv \\ &\equiv (16) \cdot (28) = 448 \equiv 23 \bmod 85. \end{aligned}$$

Portanto, $b_3 = 23$, que corresponde à letra G na tabela.

Por essa razão, o bloco decodificado fica com o formato:

39 - 21 - 23,

que se refere à mensagem original:

U F G,

como queríamos encontrar.

7. Resultados Principais

O dispositivo RSA é muito inteligente, contudo há a necessidade do usufruto do computador para realizar as operações mais elaboradas. Precisa, também, de números primos bastante grandes e dispor de uma escolha cuidadosa das chaves do sistema. Por isso, o ensino de conteúdos de Teoria dos Números é fundamental, não só na graduação, mas também na educação básica, pois o ingresso na academia ainda é restrito em nosso país e são poucos os calouros que, de fato, terão acesso a tal conhecimento, visto que grande parte deles não cursarão ciências exatas e suas tecnologias. Além do mais, o estudo de criptografia corroborará a introdução de conceitos de segurança da informação, pois, sem dúvida, eles terão amplo acesso aos diversos meios digitais, tais como: *e-mail*, redes sociais, aplicativos e bancos digitais. Por fim, os resultados enaltecem a relevância da Teoria dos Números e a percepção de quão fundamental é a segurança da informação para a economia em larga escala, para a qualidade de vida e, principalmente, no cenário atual, para a grande demanda de ambientes voltados à realização de *home office* com fidúcia, devido, em especial, à pandemia do Coronavírus (Covid-19) e outras doenças que podem surgir ao longo da história da humanidade, prejudicando os trabalhos ⌈in loco.

8. Conclusão

O que se observa é que a cifragem surgiu da necessidade em fornecer dados apenas para cidadãos específicos. Na guerra, por exemplo, uma mensagem sigilosa resgatada pode gerar consequências terríveis e, portanto, os povos embarcaram no exercício de criar ferramentas para codificar suas comunicações. Uma das primeiras foi a de César, que desfrutou do próprio alfabeto para codificar conteúdos, no entanto o dispositivo não logrou êxito, pois os criptoanalistas identificaram, com certa facilidade, desfrutando da análise de frequências, as propostas encaminhadas. Posteriormente, foram produzidos sistemas baseados na tabela recta, em números e em chaves simétricas, disposta, somente, aos que se entretinham no eixo de comunicação. Esse sistema também não funcionou, porque a quebra continuava acontecendo. A incorporação dos computadores deu origem ao Sistema de Informação e veio com ele a necessidade de gerar métodos mais eficazes para garantir a confidencialidade das informações. Essa necessidade partiu do fato de que se percebeu que a internet não é um meio seguro, e criptografar era essencial no processo de salvaguardar as informações. Através das ideias de Driffie, os estudiosos Rivest, Shamir e Adlman propuseram o sistema criptográfico RSA. Foi, então, que observaram a relevância da Teoria dos Números, algo, até aquele momento, abstrato e desprovido de aplicação concreta. Conceberam, agora, um sistema robusto que faz uso de números primos enormes, chaves assimétricas e congruência. O mais engenhoso é que se trata de uma operação simples de se realizar, todavia quase impossível de desfazer. Assim, o artigo elucida o sistema criptográfico RSA, que se embasa na Aritmética Modular, ramo da Teoria dos Números de relevância ímpar, tendo em vista a difusão de conteúdos aplicados de tecnologia e o debate da segurança da informação no ambiente escolar pelo docente.

Referências

[1] Diffie, W. e Hellman,M. *Multiuser Cryptographic Techniques*, IEEE Transaction on Information Theory, 1976.

[2] Ellis, J. *The History of Non-secret Encryption* , Cryptologia, 1999.

[3] Ellis, J. *The Possibility of Secure Non-Secret Digital Encryption* , CESG Repart, 1970.

[4] Hefez, A. *Aritmética*, Sociedade Brasileira de Matemática, 2016.

[5] Quaresma, P. *Criptografia*, Artigo, Disponível em: <https://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf>. Acesso em: 17 de março de 2020.

[6] Merkle, R. *Secure Communucation Over an Insecure Channel* , Communications of the ACM, 1978.

[7] Rivest, R.; Shamir,A. e Adleman,L. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM, 1978.

[8] Simmons, G. *Cryptology* , Encyclopaedia Britannica, Fifteenth Edition, 1993.

[9] Sousa, F.H.Teixeira de, *Programa de Iniciação Científica da Obmep*, Aritmética, Aula 68, Observações prática, Disponível em: <https://www.youtube.com/watch?v=v1BTf1UlJHw>, Acesso em: 17 de fevereiro de 2020.

[10] Stalling, William *Criptografia e Segurança de Redes: Princípios e Práticas*, Pearson Education do Brasil, 2015.

[11] Stein,Clifford; L.Drysdale,Robert; Bogart,Kenneth *Matemática Discreta para Ciência da Computação*, Pearson Education, 2013.

Danilo de Araújo Moura
Secretaria de Estado de Justiça e Cidadania
Distrito Federal
<daniloaraujo543@gmail.com>

Recebido: 23/04/2020
Publicado: 23/12/2020