Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Criptografia de Chave Pública, Criptografia RSA

Antonio Nilson Laurindo Sousa

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática Universitária como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Eliris Cristina Rizziolli

Rio Claro, 2013

TERMO DE APROVAÇÃO

Antonio Nilson Laurindo Sousa
Criptografia de Chave Pública, Criptografia RSA

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Eliris Cristina Rizziolli
Orientadora

Prof. Dr. Aldicio José Miranda
Instituto de Ciências Exatas - UNIFAL-MG/Alfenas - MG

Prof. Dr. Henrique Lazari
Instituto de Geociências e Ciências Exatas - UNESP/Rio Claro - SP

Rio Claro, 16 de Agosto de 2013

À minha família, fonte de energia e inspiração que irradia a minha vida, em especial a Lucimar, minha mãe, e Raimundo Nonato, meu pai. Os quais sempre acreditaram na superação e sempre nos fizeram acreditar que podíamos ir além, apesar de toda a adversidade. A minha esposa Patrícia, irmã Nilvan, irmãos Silas, Paulo e Eliezer parceiros de todos os momentos, ao meu filho João Antonio e aos meus sobrinhos Breno, Vinícius e Rafaela minhas esperança no futuro.

Agradecimentos

Agradeço primeiramente a Deus que foi minha fortaleza e meu equilíbrio e permitiu as condições físicas para que eu pudesse chegar até aqui.

À professora Elíris Cristina Rizziolli que aceitou a orientação deste trabalho e que foi além de um porto seguro, onde encontrei segurança, foi a amiga imprescindível, a orientadora precisa e indispensável na realização desta etapa.

Aos professores Henrique Lazari verdadeiro mestre e amigo, Wladimir Seixas generoso, Thiago disponível, Marta exemplo de atenção e de carinho, Suzi acolhimento e sinceridade, Renata e Selene justas. Aos demais professores do programa de pós-graduação em matemática minha gratidão pelo belo trabalho de saber ensinar.

Aos membros da Banca Examinadora de qualificação deste trabalho, minha gratidão pela dedicação e seriedade na leitura deste, os quais contribuiram para a melhoria do mesmo. Meus sinceros agradecimentos ainda, ao Professor Aldício José Miranda (UNIFAL-MG).

Às secretárias do Departamento de Matemática Ana, Eliza e Inajara secretária da Pós-Graduação em Matemática, por todo o suporte que me foi dado, obrigado.

Aos meus amigos Olívio, Leandro pela parceria, generosidade, honestidade e grande ajuda obrigado, Renato, Paulo, Carlos, Edgard, Caritá, Glauco, Vinícius, Jean pelas grandes contribuições e ajuda, Mariana, Luciana, Gislene, Polyana, Tatiana e Mauro, Michel e Evelize, os amigos-irmãos das lojas Amor e Justiça N^{o}52 e Amizade Fraternal N^{o}275, que estiveram presente no decorrer desta caminhada e aos demais colegas que direta ou indiretamente contribuiram para a realização deste trabalho.

Aos amigos de Balsas-Ma, Jerson e Ariadna, Alaécio e Josélia, Celso Henrique e Mariana, Clésio e Elizandra, Valdelúcio, Devani e Rozali, José Ataíde e Tatiana, Costinha e Carine, Raimunda Nonata (Didi), Eduardo e Gessi pelo apoio e a torcida por mim.

Agradeço ainda, de forma especial, a Maria Aparecida, João Carmo, Jesus Almeida e toda minha família de Balsas que deram o apoio necessário para esta jornada, bem como a Viane, Flávia e Silvania pessoas que torceram e vibram com meu crescimento.

Obrigado a todos, os quais me mostraram que a vitória é uma caminhada que não se faz sozinho e que se faz necessário o apoio de pessoas especiais e amigas que ajudam materialmente, espiritualmente e intelectualmente, todos vocês deram um brilho especial e particular a esta caminhada.

A álgebra é generosa: frequentemente ela dá mais do que se lhe pediu.

Jean Le Rond d'Alembert

Resumo

Este trabalho apresenta a criptografia, que é estudada desde a antiguidade e suas técnicas hoje consistem basicamente em conceitos matemáticos. Os números inteiros prestam um papel importante na criptografia de chave pública RSA, onde são apresentados alguns conceitos importantes, propriedades e resultados desse conjunto, destacando as relações com os números primos, a função de Euler e a operação módulo, conhecida como problema do logaritmo discreto. Apresentam-se os fundamentos da Criptografia de Chave Pública RSA, em que a base é a cifra assimétrica, mostrando a garantia da privacidade e assinatura das mensagens. Finaliza-se com a ideia do protocolo de criptografia RSA, a construção de um sistema de correios eletrônico, cuja essência é o método para estabelecer uma criptografia de chave pública RSA, baseada no conceito apresentado por Diffie e Hellman [1].

Palavras-chave: Criptografia, Matemática, Chave Publica RSA, Diffie-Hellman.

Abstract

This dissertation presents Cryptography, which is studied since the ancient times and whose techniques consist basically of mathematical concepts. The integers play an important role on the Public Key Cryptography RSA, for which are presented some important results and properties of this set, emphasizing its relations with prime numbers, Euler's totient function and the modulo operation, also known as the problem of discrete logarithm. We present the foundations of the Public Key Cryptography RSA, whose basis is the asymmetric cipher, showing the privacy security of the messages. It ends with the idea of the RSA cryptography protocol, a construction of an electronic mail system, whose gist lies in the method used to establish a Public Key Criptography system RSA, based on the concept presented by Diffie and Hellman.

Keywords: Encryption, Mathematics, RSA Public key, Diffie-Hellman.

Lista de Tabelas

Sumário

1 Introdução

A criptografia é a ciência incumbida em estudar os métodos para codificar uma mensagem de forma que só o destinatário legítimo consiga interpretá-la. "É a arte dos códigos secretos". Esta arte se apresenta já na infância quando se brinca de substituir uma letra por outra, transladando o alfabeto uma casa para diante. A criptografia é estudada desde a antiguidade, sendo que durante os séculos seguintes foram desenvolvidos diversos sistemas criptográficos mais ou menos engenhosos. Porém, em geral com a segurança dependente da dificuldade de se decifrar os esquemas sem o auxílio de dispositivos que acelerassem os cálculos. Com a disponibilidade de computadores as técnicas de decifração se tornaram mais eficientes e acessíveis, fazendo com que a maioria dos métodos conhecidos de cifração resultassem obsoletos, tornando necessário o desenvolvimento de novas técnicas que permitam garantir a segurança de trânsito de dados entre dispositivos digitais, bem como a certificação de mensagens. Dentro do cenário descrito acima, a pesquisa em criptografia se orientou em mostrar técnicas de cifração que tornassem difícil a decifração de mensagens, mesmo com o recurso de computadores eficientes, isto levou a se buscar métodos que envolvessem uma maior sofisticação matemática. Desta forma justifica uma introdução adequada ao presente assunto, ao lado de um estudo de criptografia de chaves públicas e privadas e os aspectos algébricos e geométricos mais relevantes dos métodos criptográficos atuais. Este trabalho tem como objetivo geral apresentar os fundamentos da criptografia de chaves públicas: RSA, tendo como fio condutor a referência [7]. O objetivo específico é descrever o protocolo de cifração e de certificação RSA. Tendo como resultado final um texto que representará o trabalho executado, que também poderá ser usado como um texto para um curso, para programas de estudo individual ou orientado em criptografia.

Com o intuito de situar historicamente este assunto, apresentamos a seguir o surgimento, evolução e presença da criptografia ao longo dos tempos até o momento atual.

Há milhares de anos, Líderes Militares, representantes de várias dinastias, buscavam formas eficientes de comunicação, de comandar seus exércitos e de governar seus reinos. A importância de não revelar segredos e estratégias às forças inimigas, motivou o desenvolvimento de códigos e cifras, como técnicas para mascarar uma mensagem, permitindo que apenas o destinatário lesse o conteúdo. Os países passaram a criar departamentos para elaborar códigos, consequentemente, surgiram os decifradores de

códigos, criando uma corrida armamentista intelectual. As diversas formas e utilidades dadas aos códigos, ao longo do tempo, mostram a presença fundamental da matemática na evolução de tal teoria. Desta forma, a evolução é um termo bem apropriado, já que todo código sempre está sob o ataque dos decifradores, que ao revelar a fraqueza de um código, o mesmo deixa de ser útil, resultando no desenvolvimento de um novo código. Sendo que a criação deste, prosperará até que decifradores identifiquem suas fraquezas e assim por diante. Ao longo da história, os códigos foram decisivos no resultado de batalhas. À medida que a informação se torna cada vez mais valiosa, o processo de codificação de mensagens tem um papel cada vez maior na sociedade.

> *Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. .(SINGH, 2007, p.13).*

É comum encontrar relatos na história, de episódios envolvendo os códigos em operações durante guerras, onde criptoanalistas desvendaram o código dos criptógrafos "inimigos", mas mantiveram tal informação em sigilo, a fim de impedir que novos códigos fossem criados para substituir o decifrado. Assim podiam obter informações extremamente importantes para táticas de defesa e ataque.

Tais informações eram repassadas em uma comunicação secreta, constituída da ocultação da mensagem, conhecida como esteganografia, do grego, steganos, que significa coberto, e graphein, que significa escrever. Um exemplo interessante de esteganografia é encontrado em "As histórias", onde Heródoto narrou os conflitos entre Grécia e Pérsia, ocorridos no século V a.C.. Uma das histórias é a de Histaeu que queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para transmitir suas instruções em segurança, Histaeu raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo crescesse. O mensageiro, que aparentemente não levava nada que o comprometesse, viajou sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça, possibilitando assim a leitura da mensagem pelo destinatário. É evidente que a época tolerava tamanha lentidão.

O grande período em que a esteganografia perdurou, demonstra que ela certamente ofereceu certa segurança, embora sofresse de uma fraqueza fundamental: Se o mensageiro fosse revistado e a mensagem descoberta, então o conteúdo da comunicação secreta seria imediatamente revelado. A interceptação da mensagem compromete toda

a segurança. Juntamente com a evolução da esteganografia, houve a evolução da criptografia, do grego kryptos, que significa oculto, que ao contrário da esteganografia, a criptografia tem como objetivo ocultar o significado da mensagem e não a mensagem propriamente dita. Um dos mais simples destes códigos consiste em substituir uma letra pela seguinte: isto é, transladar o alfabeto uma casa para diante. Um código semelhante foi usado por Júlio César para comunicar-se com as legiões em combate pela Europa. Este parece ter sido o primeiro exemplo de um código secreto que se tem notícia. Também por volta do século X, os administradores árabes usavam a criptografia para codificar os segredos de Estado e proteger o registro de impostos. Utilizavam geralmente, um alfabeto cifrado apenas rearranjando o alfabeto original, mas também empregavam alfabetos que continham outros símbolos, essa cifra se dá o nome de **Cifra de substituição monoalfabética**, onde cada letra do alfabeto original é substituída por outra letra ou por um símbolo. Esta cifra permaneceu invulnerável por séculos. Era comum deslocar as letras do alfabeto, por exemplo, como na tabela 1.1, o alfabeto utilizado para cifrar uma mensagem tem início na letra H.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
H	I	J	K	L	M	N	O	P	Q	R	S	T
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
U	V	W	X	Y	Z	A	B	C	D	E	F	G

Tabela 1.1: Alfabeto cifrado

A grande vantagem da criptografia sobre a esteganografia é que, se o inimigo interceptar a mensagem codificada, ela está a princípio, ilegível e seu conteúdo não poderá ser descoberto de imediato. Foram os estudiosos árabes que, obtiveram o sucesso de descobrir um método para quebrar a cifra de substituição monoalfabética. Nasce então, nesse momento, a criptoanálise, irmã gêmea da criptografia na arte de decifrar códigos secretos, que é a ciência que permite decifrar uma mensagem sem conhecer a chave. Os códigos que consistem em transladar o alfabeto uma casa para diante como o de Júlio César, padeciam de um grande mal, a facilidade de decifrar. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer, sofre do mesmo problema. Isso se deve ao fato de que a frequência média com que cada letra é usada em uma língua é mais ou menos constante.

No século IX, Al-Kindi, um cientista conhecido como “o filósofo dos árabes”, inspirado em técnicas utilizadas por teólogos para examinarem as revelações contidas no Corão, descreveu a técnica de estudar a frequência das letras para quebrar códigos. O sistema consistia basicamente em conhecendo seu idioma, encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página. E a partir disso passa a contar a frequência com que cada letra aparece. Em seguida examinar o

criptograma que se deseja decifrar e também classificar seus símbolos, com relação à frequência com que aparecem na mensagem. É coerente portanto fazer uma correspondência entre as letras e os símbolos mais frequentes. Analisando, por exemplo, uma mensagem codificada na língua portuguesa, pode-se dizer que o símbolo mais frequente na mensagem corresponde é letra A. Analogamente, o segundo símbolo mais frequente corresponde à letra E, e assim por diante. Vale observar que há letras que aparecem com a mesma frequência, mas substituindo os símbolos mais frequentes torna-se mais fácil decifrar o restante, justamente por conhecer o idioma da mensagem e, consequentemente, suas palavras. O método de *contagem de frequência* de caracteres também pôde ser usado para decifrar inscrições antigas. O exemplo mais famoso é o da decifração dos hieróglifos egípcios por J-F. Champollion em 1822. A chave da decifração foi a *pedra de roseta*, um bloco de basalto negro que está atualmene no Museu Britânico, em Londres. A pedra contém uma mesma inscrição escrita em hieróglifos, demótico e grego. Na época de Champollion muito se discutia que tipo de escrita seriam os hierógrafos: se ideográficas, silábica ou alfabética. Em uma escrita ideográfica os símbolos representam ideias; como acontecem no chinês. Nas escritas silábicas, cada símbolo vale uma sílaba. As inscrições gregas mais antigas foram escritas em um silabário conhecido como *Linear* ***B***, decifrado em 1954. Assim em uma escrita ideográfica cada palavra corresponde essencialmente a um símbolo. Imagine que um texto escrito em grego (que é alfabético) foi traduzido para uma escrita edeográfica. Esperamos, então, que o número de símbolos usados na tradução corresponda aproximadamente ao número de palavras no texto grego. Por isso, Champollion começou seu processo de decifração contando caracteres nas incrições da pedra de Roseta. Ele descobriu que havia 486 palavras no texto grego e 1419 caracteres no texto em hieróglifos. Portanto a escrita dos antigos egípcioso não podia ser ideográfica. Hoje sabemos que os hieróglifos formam um sistema misto. Há caracteres ideográficos, caracteres silábicos e os chamados determinativos. Estes últimos servem para distinguir homônimos, indicando a que classe pertecem. Por exemplo, se escrevêssemos em português usando hieróglifos, poderíamos distinguir a fruta manga da manga da camisa usando determinativo de fruta aposto à primeira.

Portanto, os criptoanalistas estavam vencendo a guerra contra os criptógrafos. Então Cabia aos criptógrafos criar uma nova cifra, mais forte, algo que pudesse vencer os criptoanalistas. Por volta de 1460, o italiano Leon Battista Alberti (1404 - 1472), escreveu um ensaio sobre o que ele acreditava ser uma nova forma de cifra: Naquela época todas as cifras de substituição exigiam um único alfabeto cifrado para codificar cada mensagem. Alberti propôs o uso de pelo menos dois alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial. A grande vantagem do sistema de Alberti é que a mesma letra do texto original não aparece necessariamente como uma única letra no texto cifrado. Embora houvesse descoberto o avanço mais relevante das cifras num período de um milênio, Alberti não conseguiu desenvolver sua

ideia: de transformá-la num sistema completo de cifragem. Esta tarefa coube a um grupo de intelectuais que aperfeiçoaram a ideia original, o alemão Johannes Trithemius (1462 - 1516), depois o italiano Giovanni Porta (1541 - 1615), e por fim o francês Blaise de Vigenére (1523 - 1596). Este último tomou conhecimento dos trabalhos e examinou em detalhes as ideias de Alberti, Trithemius e Porta, mesclando-as para formar uma nova cifra, coerente e poderosa. A cifra ficou conhecida como cifra de Vigenére em homenagem ao homem que a desenvolveu em sua forma final. A cifra de Vigenére consiste em até 26 alfabetos distintos (tabela 2) para criar a mensagem cifrada. O primeiro passo é montar o chamado quadrado de Vigenére, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. Em resumo, o remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante.

	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**
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Tabela 1.2: Quadrado de Vigenére

Assim, para decifrar a mensagem, o destinatário precisa saber que linha do quadrado Vigenére foi usada para a cifragem de cada letra, por isso deve existir um sistema previamente combinado para a mudança entre linhas. Conseguia-se isso por intermedio do uso de uma palavra-chave. O comunicado "**Caros, informo a todos que outra vez os criptógrafos estão na frente na corrida dos código**", pode ser codificado como "**Eaick, knwcjoo r hgfoj emg olhjc vvn gu ciwhvoxfshoj skvaf bs hrvblg nr qgtrzrs foj qgfixck**", sendo que a palavra-chave é a primeira palavra, ou seja, toda a mensagem foi codificada usando cinco dos vinte e seis alfabetos de Vigenére. Mais especificamente, a primeira letra da mensagem foi codificada com o alfabeto que tem início em C, a segunda com o alfabeto que tem início na letra A, a terceira com o alfabeto que inicia em R, a quarta com o que inicia em O, a quinta com o que

inicia em S, a sexta volta a ser codificada com o alfabeto que inicia em C e, assim por diante. A grande vantagem da cifra de Vigenére é que ela é imune à análise de frequência. Além disso, a cifra tem um número enorme de chaves. Um criptoanalista não conseguiria decifrar a mensagem procurando todas as chaves possíveis, porque o número de opções é simplesmente grande demais: 26^{26}. A cifra polialfabética de Vigenére era considerada indecifrável e tornou-se conhecida pela expressão francesa Le chiffre indéchiffable. Finalmente os criptógrafos estavam em vantagem sobre os criptoanalistas. É claro que decifrar uma mesagem por contagem de frequência é ainda mais simples se temos um computador. Supondo que a língua é conhecida, a maior parte do processo pode ser automatizado. Isto torna essencialmente inviável todos os códigos que envolvem substituição de letras. Na verdade alguns dos computadores foram montados exatamente para auxiliar na decifração dos códigos secretos usados pelos alemães durante a $2^{\underline{a}}$ guerra mundial. Um dos cientistas responsáveis por este projeto foi **Alan Turing**, o idealizador do conceito teórico da ***máquina de Turing*** que deu origem aos computadores e devido a este fato, ele foi considerado o pioneiro da inteligência artificial.

Nos dias atuais a possibilidade de comunicação entre computadores via internet trouxe novos desafios para a criptografia. Por ser relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis, como transações bancárias, comerciais, ou até mesmo uma compra feita com cartão de crédito. Imagine que uma empresa envia a um banco uma autorização para uma transação de milhões de reais. Dois problemas imediatamente surgem. Primeiro que é preciso proteger a mensagem para que não possa ser lida, mesmo que seja interceptada por uma concorrente, ou por um ladrão de bancos. Por outro lado, o banco precisa ter certeza de que a mensagem foi enviada por um usuário da empresa, ou seja, como se a mensagem estivesse assinada. Desta forma, tornou-se necessário inventar novos códigos, que mesmo com a ajuda de um computador, fossem difíceis de decifrar. Estes códigos não foram criados para a comunicação entre espiões e sim, para o uso em aplicações comerciais. Na década de 70, surgiu na Califórnia, com Whitfield Diffie, Martin Hellman da Universidade de Stanford e Ralph Merkle da Universidade da Califórnia, a ideia da cifra assimétrica, onde diferentemente dos códigos criados anteriormente, saber codificar não implica em saber decodificar. A fim de desenvolver esta forma de criptografia, a ideia era encontrar uma função de mão única que, como o nome sugere, fosse irreversível. É como quebrar um ovo e fazê-lo voltar a sua condição inicial, o que se torna impossível. Começou assim um frenético estudo para encontrar uma função matemática apropriada.

Diffie publicou um resumo de sua ideia em 1975, a partir daí, outros cientistas se uniram em busca de uma função de mão única que preenchesse os requisitos de uma cifra assimétrica. Inicialmente havia um grande otimismo, mas os meses se passavam e, parecia cada vez mais provável que as funções de mão única não existissem. A

ideia do trio funcionaria na teoria, mas não na prática, já que apesar do esforço, não descobriram uma função apropriada e, consequentemente, a cifra assimétrica não se tornava realidade.

Em 1977, na costa Leste dos Estados Unidos, Ronald Rivest, Adi Shamir e Leonard Adleman, encontraram uma função capaz de colocar em prática a ideia do trio californiano. Surge assim, no Massachusetts Institute of Technology, a criptografia RSA, em homenagem a Rivest, Shamir e Adleman. Até hoje, o RSA é o mais conhecido dos métodos de criptografia de chave pública, nome dado ao sistema de criptografia assimétrica, onde são usadas duas chaves distintas e uma delas é disponibilizada publicamente, uma vez que a chave utilizada para cifrar uma mensagem não é capaz de decifrar a mesma.

2 Números Inteiros

Os números inteiros desempenham um papel fundamental na criptografia. Neste capítulo, apresenta-se as principais propriedades dos números inteiros e descreve-se os algoritmos fundamentais. Detalhes sobre essas propriedades encontra-se em [5].

Definição 2.1. Indica-se por $\mathbb{Z}$ o conjunto dos números inteiros, como segue

$$\mathbb{Z} = \{0 \pm 1, \pm 2, \pm 3, \ldots\}.$$

Este conjunto munido das operações usuais adição e multiplicação satisfaz as propriedades:

- Propriedades da adição.

(a) $a + (b + c) = (a + b) + c$, $\forall a$, b, c, $\in \mathbb{Z}$ (*associativa*);

(b) $a + b = b + a$, $\forall a$, $b \in \mathbb{Z}$ (*comutativa*);

(c) $a + 0 = a$, $\forall a \in \mathbb{Z}$ (0 *é o elemento neutro da adição*).

(d) Para todo $a \in \mathbb{Z}$, existe $(-a) \in \mathbb{Z}$ tal que $a + (-a) = (-a) + a = 0$ (*Elemento oposto*)

- Propriedades da multiplicação.

(a) $a(bc) = (ab)c$, $\forall a$, b, c, $\in \mathbb{Z}$ (*associativa*);

(b) $ab = ba$, $\forall a$, b, $\in \mathbb{Z}$ (*comutativa*);

(c) $a1 = a$, $\forall a$, $\in \mathbb{Z}$ 1 (*é o elemento neutro da multiplicação*);

(d) $ab = 0 \Rightarrow a = 0$, ou $b = 0$ (*lei do anulamento do produto*);

(e) $ab = 1 \Rightarrow a = \pm 1 = b = \pm 1$;

(f) $a(b + c) = ab + ac$, $\forall a$, b, c, $\in \mathbb{Z}$.

Ainda, pode-se estabelecer uma relação de ordem total a $\mathbb{Z}$, a saber:

$$a \leq b \Leftrightarrow \exists p \in \mathbb{N} = \{0, 1, 2, \ldots\} \text{ tal que } b = a + p.$$

Ou seja, $(\mathbb{Z}, \leq)$ é tal que:

(a) $a \leq a$, $\forall a \in \mathbb{Z}$ (*reflexiva*);

(b) $a \leq b$ e $b \leq a \Rightarrow a = b$ (*anti-simétrica*);

(c) $a \leq b$ e $b \leq c \Rightarrow a \leq c$ (*transitiva*);

(d) Dados a e b em $\mathbb{Z}$, então $a \leq b$ ou $b \leq a$ (*totalidade*).

Além disso, esta relação é compatível com as operações adição e multiplicação, uma vez que são válidas as seguintes propriedades:

(e) $a \leq b \Rightarrow a + c \leq b + c$, $\forall c \in \mathbb{Z}$ (*compatibilidade com a adição*);

(f) $0 \leq a$ e $0 \leq b \Rightarrow 0 \leq ab$ (*compatibilidade com a multiplicação*).

E ainda temos

(g) $a \leq 0$ e $0 \leq b \Rightarrow ab \leq 0$;

(h) $0 \leq a$ e $b \leq 0 \Rightarrow ab \leq 0$;

(i) $a \leq 0$ e $b \leq 0 \Rightarrow 0 \leq ab$.

A seguir tem-se um dos principais resultados quando trata-se do conjunto dos números inteiros, a saber, o Princípio do Menor Inteiro; para tanto vale relembrar que um subconjunto não vazio $L \subset \mathbb{Z}$ é limitado inferiormente se existe um elemento $a \in \mathbb{Z}$ de maneira que: $a \leq x, \forall x \in \mathbb{Z}$.

Teorema 2.1. *Se L é um conjunto não vazio de $\mathbb{Z}$ e L é limitado inferiormente, então existe um único $l_0 \in L$, denominado elemento mínimo de L, tal que*

$$l_0 \leq x, \forall x \in L.$$

Por exemplo o conjunto $L = \{-2, 0, 2, 4, \ldots\}$ é limitado inferiormente. Os limites inferiores de L são $-2, -3, -4, \ldots,$ e o mínimo de L é -2. Enquanto que um subconjunto $S \subset \mathbb{Z}$ não limitado inferiormente não possui mínimo, por exemplo considerando

$S = \{\ldots, -6, -4, -2, 0\}$ este não é limitado inferiormente, não existe portanto o mínimo de S.

Os primeiro e segundo Princípios de Indução Finita relativos ao conjunto dos números naturais podem ser adaptados ao conjunto dos números inteiros como segue.

Proposição 2.1 (Primeiro Princípio da Indução para $\mathbb{Z}$)**.** *Dados $a \in \mathbb{Z}$ e $n \in \mathbb{Z}$ com $n \geq a$, suponha associada uma propriedade $P(n)$.*

Então, $P(n)$ é válida, para todo $n \geq a$, desde que

(i) $P(a)$ é válida;

(ii) Se $P(r)$ é válida para $r \geq a$, então $P(r+1)$ também é válida.

Demonstração.

Seja $L = \{x \in \mathbb{Z} | x \geq a$ e $P(x)$ é falsa$\}$. Se mostrar que $L = \emptyset$, o princípio estará justificado. Suponha $L \neq \emptyset$. Então, uma vez que L é limitado inferiormente (a é um limite inferior), e do teorema 2.1, segue que existe $l_0 =$ mín (L). Como $P(a)$ é verdadeira, por hipótese (i), $a \notin L$, logo $l_0 > a$ e, então, $l_0 - 1 \geq a$. Por outro lado, $P(l_0 - 1)$ é verdadeira, já que $l_0 - 1 \in L$, mas $l_0 =$ mín. de (L). Então da hipótese (ii), $P((l_0 - 1) + 1)$ é verdadeira, o que é absurdo pois l_0 está em L.

□

Exemplo 2.1.

Este último resultado é aplicado para demonstrar que $1 + n \leq 2^n, \quad \forall n \geq 0$.

Com efeito:

(i) $n = 0:$ $\quad 1 + 0 \leq 2^0$ é obviamente verdadeira.

(ii) Supõe-se $1 + r \leq 2^r$, com $r \geq 0$.

Então $1 + r \leq 2^r$ que multiplicado por (2) em ambos os lados da inequação, tem-se:

$$2 + 2r \leq 2^{r+1} \Rightarrow 2(1 + r) \leq 2^{r+1}$$

Como $r \geq 0$ então,
$2 + 2r - r \leq 2(1 + r) \leq 2^{r+1} \Rightarrow 2 + r \leq 2(1 + r) \leq 2^{r+1}$ e pela transitividade, tem-se:
$2 + r \leq 2^{r+1}$.
Daí, $1 + (1 + r) \leq 2^{r+1}$.

Portanto pela proposição 2.1 segue que $1 + n \leq 2^n, \ \forall n \geq 0$.

Observe que neste exemplo a propriedade $P(n)$ é dada por $P(n) = \{n \in \mathbb{Z}_+ \ : \ 1 + n \leq 2^n\}$.

Proposição 2.2 (Segundo Princípio de Indução para $\mathbb{Z}$)**.** *Dados $a \in \mathbb{Z}$, e $n \in \mathbb{Z}$ com $n \geq a$ suponha associada propriedade $P(n)$.*

Então $P(n)$ será válida, para todo $n \geq a$, desde que

(i) $P(a)$ é válida;

(ii) Dado $r > a$, se $P(k)$ é válida para todo k tal que $a \leq k < r$, então $P(r)$ é válida.

Demonstração. Seja $L = \{x \in \mathbb{Z} | x \geq a$ e $P(x)$ é falsa$\}$. Deve-se provar que $L = \emptyset$. Suponha que $L \neq \emptyset$ então pelo teorema 2.1, segue que $l_0 =$ mín (L). Como $P(a)$ é verdadeira, devido à hipótese (i), temos $l_0 > a$. Logo, para todo $k \in \mathbb{Z}$, $a \leq k < l_0$, $P(k)$ é verdadeiro (pois l_0 é o mínimo dos $x \geq a$ para os quais $P(x)$ é falsa). Consequentemente, pela hipótese (ii), $P(l_0)$ também é verdadeira, o que é um absurdo. Portanto, $L = \emptyset$ e $P(x)$ é verdadeira para todo $x \geq a$.

□

Exemplo 2.2.

Aplica-se o Segundo Princípio de Indução para demonstrar que $n^2 \geq 2n$, para todo inteiro $n \geq 2$. De fato,

Para $n = 2$, temos:

$2^2 = 2 \cdot 2 \Rightarrow 4 = 4$, portanto verdadeiro.

Seja $r > 2$ e suponha que se tenha $k^2 \geq 2k$, para todo inteiro k tal que $2 \leq k < r$.

Faz-se $r - k = t$, do que segue $r = k + t$, em que $t > 0$.

Daí: $r^2 = (k + t)^2 = k^2 + 2kt + t^2 \geq 2k + 2kt + t^2 > 2k + 2kt$.

Mas, como $k \geq 2$ e $t > 0$, então $2k > 2$ e, portanto, $2kt > 2t$.

De onde:

$r^2 > 2k + 2t = 2(k + t) = 2r$. Portanto, $r^2 > 2r$.

2.1 Múltiplos e Algoritmo da Divisão

Definição 2.2. Seja $a \in \mathbb{Z}$, qualquer. Os múltiplos de a são os números da forma ka, em que k é elemento de $\mathbb{Z}$.

Se ka e ha são múltiplos de a, então sua soma e seu produto também são múltiplos de a, já que:

$$ha + ka = (h + k)a \text{ e } h(a)(ka) = (hak)a.$$

Quando $a, b, c \in \mathbb{Z}$ são tais que $c = ab$ diz-se que a é um *divisor* de c ou que a *divide* c ou ainda que c é *divisível* por a.

Notação: $a|c$, leia-se a divide c.

Teorema 2.2. *Dados a, $b \in \mathbb{Z}$, com b estritamente positivo, existem únicos q, $r \in \mathbb{Z}$, de maneira que $a = bq + r$ e $0 \leq r < b$.*
Denomina-se q e r de quociente e resto da divisão de a por b respectivamente.

Demonstração.

Seja b um número inteiro estritamente positivo.

Dado $a \in \mathbb{Z}$, então ou a é um

múltiplo de b ou está situado entre dois múltiplo consecutivos qb e $(q+1)b$ de b, ou seja,

$$qb < a < (q+1)b.$$

Mas isto equivale a

$$0 < a - qb < b.$$

Somando $-(qb)$ às desigualdades anteriores. Fazendo $r = a - qb$ obtém-se

$$a = bq + r, \text{ em que } 0 < r < b.$$

Sintetizando os dois casos pode-se dizer que $a = bq + r$, $0 < r < b$.

Obviamente $r = 0$ quando a é múltiplo de b.

Agora estuda-se a unicidade de q e r, para tanto supõe-se $a = bq + r = a = bq_1 + r_1$, em que $0 \leq r$, $r_1 < b$.

Admite-se $r \neq r_1$, por exemplo $r > r_1$.

Como $b(q_1 - q) = r - r_1$ tem-se então $q_1 > q$. Assim

$$r = r_1 + b(q_1 - q).$$

Ora, sendo $r_1 \geq 0$ e $q_1 - q \geq 1$, conclui-se desta última igualdade que $r \geq b$ o que é um absurdo.

Então $r = r_1$ e, consequentemente, $q_1 = q$. □

Exemplo 2.3.

(a) $a = 60$ e $b = 7$. Neste caso $60 = 7 \cdot 8 + 4$, onde $q = 8$ e $r = 4$.

(b) $a = -60$ e $b = 7$. Aqui, $-60 = 7 \cdot (-9) + 3$, $q = -9$ e $r = 3$.

Proposição 2.3.

(i) $a|a$, $\forall a \in \mathbb{Z}$;

(ii) Se a, $b \in \mathbb{Z}_+$ são tais que $a|b$ e $b|a$ então, $a = \pm b$.

(iii) Se a, b, $c \in \mathbb{Z}$ são tais que $a|b$ e $b|c$ então, $a|c$.

(iv) Se $a|b$ e $a|c$ então, $a|(bx+cy)$, $\forall x,\ y \in \mathbb{Z}$.

Demonstração.

(i) $a|a$, já que $a = a1, \forall a \in \mathbb{Z}$;

(ii) Suponha $b = ac_1$ e $a = bc_2$ com $c_1,\ c_2 \in \mathbb{Z}_+$.

Se $a = 0$ ou $(b = 0)$, então $b = 0$ ou $(a = 0)$.

Caso contrário,

tem-se $c_1 > 0$ e $c_2 > 0$.

Como $a = a(c_1c_2)$, então $c_1 = c_2 = \pm 1$.

Donde $c_1 = c_2 = 1$ já que são números inteiros positivos.

Consequentemente $a = b$.

(iii) Da hipótese segue $b = ad_1$ e $c = bd_2$, $d_1,\ d_2 \in \mathbb{Z}$.

Daí $c = a(d_1d_2)$. Ou seja, $a|c$, como queríamos demonstrar.

(iv) Suponha $b = ad_1$ e $c = ad_2$, com $d_1,\ d_2 \in \mathbb{Z}$.

Logo,

$bx = a(xd_1)$ e $cy = a(yd_2)$.

Portanto,

$bx + cy = a(xd_1 + yd_2)$,

ou seja, a divide $bx + cy$.

□

2.2 Máximo Divisor Comum e Número Primo

Definição 2.3. Dados $a,\ b \in \mathbb{Z}$, diz-se que $d \in \mathbb{Z}_+$ é máximo divisor comum entre a e b se:

(i) $d|a$ e $d|b$ e

(ii) se d' é um número inteiro tal que $d'|a$ e $d'|b$, então $d'|d$.

Notação: mdc (a, b).

Observação 2.1.

(a) Se d e d_1 são máximos divisores comuns entre a e b, então $d = d_1$.

De fato, como $d|d_1$ e $d_1|d$ e, ainda, são ambos positivos, de 2.3 (ii). Conclui-se que $d = d_1$;

(b) Se $a = b = 0$, então $d = 0$;

(c) Se $a = 0$ e $b \neq 0$, então $d = |b|$;

(d) Se d é máximo divisor comum entre a e b então d também é máximo divisor comum entre a e $-b$, $-a$ e b e, ainda, entre $-a$ e $-b$.

Proposição 2.4. *Quaisquer que sejam a, $b \in \mathbb{Z}$, existe $d \in \mathbb{Z}$ que é o máximo divisor comum de a e b.*

Demonstração. Considerando a observação acima pode-se limitar ao caso em que $a > 0$ e $b > 0$.

Seja $L = \{ax + by \mid x,\ y \in \mathbb{Z}\}$.

Evidentemente existem elementos estritamente positivos em L, faça-se, por exemplo, $x = y = 1$.

Seja d o menor desses elementos, o que existe pelo princípio do menor inteiro.

Note que $d \geq 0$, d é o máximo divisor comum entre a e b.

Com efeito:

(i) Como $d \in L$, então existem x_0, $y_0 \in \mathbb{Z}$ de maneira que $d = ax_0 + by_0$.

Aplicando o algorítmo da divisão aos elementos a e d, segue que:

$a = dq + r \quad (0 \leq r < d)$.

Ou, ainda $r = a(1 - qx_0) + b(-y_0)q$, ou seja, $r \in L$.

Sendo r positivo e levando em conta a escolha do elemento d a conclusão é que $r = 0$. Daí tem-se $a = dq$ o que mostra que $d|a$.

Analogamente se prova que $d|b$;

(ii) Se $d'|a$ e $d'|b$, como $d = ax_0 + by_0$, então tem-se

$d = ax_0 + by_0 = (k_1 d')x_0 + (k_2 d')y_0 = (k_1 x_0 + k_2 y_0)d'$.

Ou seja, $d'|d$.

□

Observação 2.2. Se $d = \text{mdc}\ (a, b)$, então se verificou, na demonstração acima, que $d = ax_0 + by_0$, onde x_0, $y_0 \in \mathbb{Z}$. Os elementos x_0 e y_0 que satisfazem tal identidade não são necessariamente únicos. Uma tal identidade recebe o nome de *identidade de Bezout* para os elementos a e b.

Definição 2.4. Um número $p \in \mathbb{Z}$ é chamado de número primo se

(i) $p \neq 0$;

(ii) $p \neq \pm 1$ e

(iii) os únicos divisores de p são 1, -1, p e $-p$.

Observação 2.3. Os divisores a, $-a$, 1 e -1 de $a \in \mathbb{Z}$ são chamados de *divisores triviais* de a. Dizer que a *não* é *primo* significa, quando $a \neq 0$ e $a \neq \pm 1$, que existem outros divisores de a além dos triviais. Um número $a \in \mathbb{Z}$ tal que $a \neq 0$, $a \neq \pm 1$, e não é primo será chamado de número inteiro *composto*.

Exemplo 2.4. O número 6 é composto pois, além dos divisores 1, -1, 6 e -6 triviais, admite também os divisores 2, -2, 3 e -3.

Proposição 2.5. *Se p é primo e $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Supõe-se que p não seja divisor de a.
Então os divisores comuns de p e a são apenas 1 e -1.
Daí o mdc $(a, p) = 1$.
Logo, existem x_0, $y_0 \in \mathbb{Z}$ de maneira que

$$1 = ax_0 + py_0.$$

Portanto

$$b = (ab)x_0 + p(by_0).$$

Como $p|(ab)$ e $p|p$, então $b = (kp)x_0 + p(by_0) = p(kx_0 + by_0)$. Logo, $p|b$.

□

Aplicando o Princípio de Indução, tem-se uma generalização da proposição 2.5.

Corolário 2.1. *Se $p|a_1a_2 \ldots a_n$, então p divide um dos a_i, para algum $i \in \{1, \ldots, n\}$.*

Proposição 2.6. *Se a é um número inteiro não nulo e diferente de ± 1, então o mínimo do conjunto $S = \{x \in \mathbb{Z} \mid x > 1 \text{ e } x|a\}$ é um número primo.*

Demonstração. Como a e $-a$ são divisores de a é óbvio que $S \neq \emptyset$.

Seja p o menor dos elementos de S. Se p não fosse primo, então existiria um divisor não trivial q de p.

Mas $(-q)$ também é um divisor de p, pode-se dizer que existe um divisor q_1 de $p(q_1 = q$ ou $q_1 = -q)$ tal que $1 < q_1 < p$.

Assim de $p|a$ e $q_1|p$ decorre que $q_1|a$ implicando que $q_1 \in S$. Absurdo pois p é o mínimo de S. □

Teorema 2.3 (Teorema Fundamental da Aritmética)**.** *Dado um número inteiro $a > 1$, exitem r números inteiros primos estritamente positivos $p_1, \ldots, p_r$ de maneira que $a = p_1 p_2 \ldots . p_r$ $(r \geq 1)$. Além disso, se também $a = q_1 q_2 \ldots . q_s$, onde os q_j são primos estritamente positivos, então $r = s$ e cada p_i é igual a um dos q_j.*

Demonstração.

(i) Usa-se o Segundo Princípio de Indução.

Se $a = 2$, então a afirmação do enunciado é válida pois o número 2 é primo.

Supõem-se que o teorema é válido para todo $b \in \mathbb{Z}$ tal que $2 \leq b < a$. A proposição 2.6 garante que existe um número primo $p_1 > 0$ que divide a, ou seja $a = p_1 a_1$.

Se $a_1 = 1$ ou a_1 é primo, a conclusão é imediata.

Caso contrário, como $2 \leq a_1 < a$, a hipótese de indução nos garante que $a_1 = p_2 \ldots . p_r$ $(r - 1 \geq 1)$, onde os p_i são estritamente positivos e primos.

Logo

$$a = p_1 \; p_2 \ldots \; p_r \; .$$

(ii) Se $p_1 \ldots \; p_r = q_1 \ldots \; q_s \Rightarrow p_1 | q_1 q_2, \ldots, q_s \Rightarrow p_1 | q_j$ $(1 \leq j \leq s)$ devido a

proposição 2.5.

Supõem-se que $j = 1$ então $p_1 | q_1$ e daí $p_1 = q_1$ uma vez que q_1 é primo e $p_1 > 1$.

Cancelando p_1 e q_1 na igualdade inicial e prosseguindo com o raciocínio desenvolvido até aqui, chega-se à unicidade da decomposição.

□

Corolário 2.2. *Seja a um número inteiro não nulo e diferente de ± 1. Então existem (e são únicos) os números primos estritamente positivos $p_1, \ldots, \; p_r$ $(r \geq 1)$, de maneira que $a = \pm p_1 \ldots p_r$.*

2.3 Congruências

Definição 2.5. Seja $m > 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, diz-se que a é côngruo a b, módulo m, se, e somente se, $m|(a-b)$.

Notação: $a \equiv b(mod\ m)$.

Exemplo 2.5.

(a) $21 \equiv 1(mod\ 5)$ pois $21 - 1 = 20$ é divisível por 5.

(b) $100 \equiv 1(mod\ 9)$ pois $100 - 1 = 99$ é múltiplo de 9.

Proposição 2.7.

(i) $a \equiv a(mod\ m)$, $\forall a \in \mathbb{Z}$.

(ii) $a \equiv b(mod\ m) \Rightarrow b \equiv a(mod\ m)$.

(iii) $a \equiv b(mod\ m)$ *e* $b \equiv c(mod\ m) \quad \Rightarrow \quad a \equiv c(mod\ m)$.

(iv) $a \equiv b(mod\ m)$ *e* $c \equiv d(mod\ m) \quad \Rightarrow \quad a + c = b + d(mod\ m)$.

(v) $a \equiv b(mod\ m) \quad \Rightarrow \quad ac \equiv bc(mod\ m), \ \ \forall c \in \mathbb{Z}$.

(vi) $a \equiv b(mod\ m) \quad \Rightarrow \quad a^r \equiv b^r(mod\ m), \ \forall r \geq 1$.

Demonstração.

(i) Pois $a - a = 0$ é divisível por m.

(ii) De fato, se $m|(a-b)$, então $m|(b-a)$, pois $b - a = -(a-b)$.

(iii) Como $m|(a-b)$ e $m|(b-c)$, então $m|[(a-b)+(b-c)]$, seja, $m|(a-c)$. Isto equivale à tese.

(iv) Se $a \equiv b(mod\ m)$, então $m|(a-b) \Rightarrow (a-b) = k_1 \cdot m$, $k_1 \in \mathbb{Z}$. Se $c \equiv d(mod\ m)$, então $m|(c-d) \Rightarrow (c-d) = k_2 \cdot m$, $k_2 \in \mathbb{Z}$. Somando membro a membro as duas equações, tem-se: $(a-b)+(c-d) = k_1m+k_2m \Rightarrow (a+c)-(b+d) = m(k_1+k_2) \Rightarrow$ $\Rightarrow (a+c)-(b+d) = km$, $k \in \mathbb{Z}$. Então: $m|[(a+c)-(b+d)] \quad \Rightarrow \quad (a+c) \equiv (b+d)\ (mod\ m)$.

(v) Se $a \equiv b(mod\ m)$, então: $m|(a-b) \Rightarrow (a-b) = k_1$, $k_1 \in \mathbb{Z}$. Multiplicando por c, ambos os membros, tem-se: $c(a-b) = ck_1m \Rightarrow (ac-bc) = ck_1m \Rightarrow (ac-bc) = km$ $\Rightarrow m|(ac-bc) \Rightarrow ac \equiv bc(mod\ m)$.

(vi) Para $r = 1$ a implicação é evidente. Supõem-se que $a^r \equiv b^r (mod\ m)$. Então $a^{r+1} \equiv ab^r (mod\ m)$. Por outro lado, de $a \equiv b (mod\ m)$, segue que $ab^r \equiv b^{r+1} (mod\ m)$. Juntando as duas conclusões tiramos $a^{r+1} \equiv b^{r+1} (mod\ m)$.

□

Exemplo 2.6.

Critério de divisibilidade por 3.

A relação definida acima no conjunto $\mathbb{Z}$, pode ser usada para explorar o critério de divisibilidade por 3, a saber:

Um número natural $a \geq 1$ sempre admite a decomposição

$$a = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$

quando se usa a base 10 para o sistema de numeração.

Nessa representação (que é única), a_0 é o algarismo das unidades, a_1 o das dezenas, e assim por diante. Então:

$$a_0 \equiv a_0 (mod\ 3)$$

bem como,

$$10a_1 \equiv a_1 (mod\ 3),\ \text{pois } 10 \equiv 1 (mod\ 3)$$

$$10^2 a_2 \equiv a_2 (mod\ 3),\ \text{pois } 10^2 \equiv 1 (mod\ 3)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$10^r a_k \equiv a_k (mod\ 3),\ \text{pois } 10^r \equiv 1 (mod\ 3).$$

Somando as congruências acima de acordo com a propriedade (iv) da proposição tem-se

$$a \equiv a_0 + a_1 + \ldots + a_r (mod\ 3).$$

Disto se tira a seguinte conclusão: se $a_1 + \ldots + a_r$ for divisível por 3, isto é, côngruo a zero módulo 3, o número a também é divisível por 3, e vice versa.

Por exemplo:
$\underbrace{84.366}_{a} = \underbrace{6}_{a_0} + \underbrace{6}_{a_1} \cdot 10^1 + \underbrace{3}_{a_2} \cdot 10^2 + \underbrace{4}_{a_3} \cdot 10^3 + \underbrace{8}_{a_4} \cdot 10^4$
$6 \equiv 6(mod\ 3)$ pois, $3|(6-6) \Rightarrow 3|0 = 0$
$10 \cdot 6 \equiv 6(mod\ 3)$ pois, $3|(10-1) \Rightarrow 3|9 = 3$
$10^2 \cdot 3 \equiv 3(mod\ 3)$ pois, $3|(100-1) \Rightarrow 3|99 = 33$
$10^3 \cdot 4 \equiv 4(mod\ 3)$ pois, $3|(1000-1) \Rightarrow 3|999 = 333$
$10^4 \cdot 8 \equiv 8(mod\ 3)$ pois, $3|(10000-1) \Rightarrow 3|9999 = 3333$. Assim, segue que:
$84.366 \equiv 6+6+3+4+8(mod\ 3)$
$84.366 \equiv 27(mod\ 3) \Rightarrow 3|(84.366-27) = 3|(84.339) = 28.113$.
Consequentemente 84.339 é múltiplo de 3.

Definição 2.6. Uma relação R sobre um conjunto E não vazio é chamada *relação de equivalência sobre* E se, e somente se, R é *reflexiva*, *simétrica* e *transitiva*, isto é, se são verdadeiras as sentenças:

(i) $(\forall x)\ (x \in E \ \rightarrow\ xRx)$;

(ii) $(\forall x, \forall y)\ (xRy \ \rightarrow\ yRx)$;

(iii) $(\forall x, \forall y, \forall z)\ (xRy \text{ e } yRz \ \rightarrow\ xRz)$.

Quando R é uma relação de equivalência sobre E, para exprimir que $(a, b) \in R$ usa-se a notação $a \equiv b\ (R)$, que se lê: "a é equivalente a b módulo R".

Definição 2.7. Seja R uma relação de equivalência sobre E. Dado $a \in E$, chama-se *classe de equivalência determinada por* a*, módulo* R, o subconjunto $\overline{a}$ de E constituído pelos elementos x tais que xRa. Em símbolos:

$$\overline{a} = \{x \in E \mid xRa\}\,.$$

Notação: O conjunto das classes de equivalência módulo R será indicado por $\dfrac{E}{R}$ e chamado *conjunto quociente de* E por R.

Exemplo 2.7. A relação $a \equiv b(mod\ m)$ é uma relação de equivalência.

2.4 Sobre Grupo

Definição 2.8. Diz-se que um conjunto G de elementos, não vazio, forma um *grupo* se em G está definida uma operação binária, indicada por $(*)$, tal que:

(i) a, $b \in G$ implica que $a * b \in G$ (*fechamento*).

(ii) a, b, $c \in G$ implica que $a * (b * c) = (a * b) * c$ (*lei associativa*).

(iii) Existe um elemento $e \in G$ tal que $a * e = a = e * a = a$, para todo $a \in G$ (*existência de um elemento unidade em* G).

(iv) Para todo $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a * a^{-1} = e = a^{-1} * a$ (*existência de inverso em* G).

Notação:$(G, *)$.

Definição 2.9. Diz-se que um grupo G é *abeliano* ou (*comutativo*) se para todo a, $b \in G$, $a * b = b * a$.

Exemplo 2.8. Seja $G = \mathbb{Z}$ e define $a * b$ por $a * b := a + b$, $\forall a$, $b \in \mathbb{Z}$.

Então $(G, *)$ é um grupo abeliano infinito no qual 0 faz o papel de e, e $-a$ o de a^{-1}.

Definição 2.10. Um subconjunto H de um grupo G é um *subgrupo* de G se, com relação a operação em G, o próprio H forma um grupo.

Notação: $H \leq G$.

Lema 2.1. *Um subconjunto não vazio H do grupo G é um subgrupo de G se, e somente se,*

(i) a, $b \in H$ *implica que* $a * b \in H$.

(ii) $a \in H$ *implica que* $a^{-1} \in H$.

Demonstração. Se H é um subgrupo de G, então valem (i) e (ii). Suponha-se agora que H seja um subconjunto de G para o qual valem (i) e (ii). Afirmação: H munido da operação de G restrita a H é um grupo. De fato:

- Vale o fechamento pelo item (i) da hipótese.
- A propriedade associativa vale para H pois H é um subconjunto do grupo G.
- $e \in H$, pois para qualquer $a \in H$ pelo item (ii) $a^{-1} \in H$ e pelo item (i) $e = a * a^{-1} \in H$.
- Para todo $a \in H$, $\exists a^{-1} \in G$ tal que

$$a * a^{-1} = e = a^{-1} * a.$$

Mas por hipótese, $a^{-1} \in H$. Logo está estabelecida a existência de inverso em H. Pelas propriedades conferidas acima segue que H munido da operação de G restrita a H é ele próprio um grupo. Portanto pela definição 2.10, H é subgrupo de G.

□

Daqui em diante usa-se a notação $(\cdot)$ para expressar a operação $(*)$ de um grupo.

A seguir enuncia-se o Teorema de Lagrange, cuja necessidade justifica-se para estabelecer relações importantes entre números inteiros. Para tanto, chama-se ordem de um grupo finito (ou de um subgrupo deste), o número de elementos que o compõe; no caso de grupo infinito dizemos que G tem ordem infinita.

Definição 2.11. Se G é um grupo e $a \in G$, a *ordem* (ou *período*) de a é o menor inteiro positivo m tal que $a^m = e$, em que $a^m := \underbrace{a \cdot a \cdots a}_{m\ -\ fatores}$.

Notação: $\theta(a)$.

Teorema 2.4 (Teorema de Lagrange)**.** *Se G é um grupo finito e $H \leq G$ então, a ordem de H divide a ordem de G.*

Demonstração. Vide página 42 de [4]. □

Corolário 2.3.

(i) Se G é um grupo finito e $a \in G$, então $\theta(a)|\theta(G)$.

(ii) Se G é um grupo finito e $a \in G$, então $a^{\theta(G)} = e$.

Demonstração.

(i) Pelo teorema 2.4 basta exibir um subgrupo de G de ordem $\theta(a)$. Observe que o próprio elemento a fornece este subgrupo, a saber, o subgrupo cíclico $\langle a \rangle$, de G, gerado por a, definido por todas as potências de a, ou seja, $\langle a \rangle = \{\ e,\ a,\ a^2,\ a^3 \cdots \}$. Mostremos $\theta\langle a \rangle = \theta(a)$. De fato . Evidentemente, sendo $a^{\theta(a)} = e$, este subgrupo tem $\theta(a)$ elementos, a saber, e, a, a^2, $\cdots$, $a^{\theta(a)-1}$. Se ele tivesse um número menor de elementos do que este número, então $a^i = a^j$ para alguns inteiros $0 \leq i < j < \theta(a)$. Então $a^{j-i} = e$, mas $0 < j - i < \theta(a)$ o que contradiz o próprio significado de $\theta(a)$. Por outro lado, observe que para $p > \theta(a)$, pelo algoritmo da divisão, poderíamos escrever que $p = k\theta(a) + m$, com $0 < m < \theta(a)$. Dai, $a^p = a^{k\theta(a)+m} = a^{k\theta(a)}$. $a^m = e \cdot a^m = a^m$, $0 < m < \theta(a)$.

Assim, o subgrupo cíclico gerado por a tem $\theta(a)$ elementos; portanto, pelo teorema 2.4, $\theta(a)|\theta(G)$.

(ii) Pelo item anterior, $\theta(a)|\theta(G)$; assim $\theta(G) = m\theta(a)$, para algum $m \in \mathbb{Z}$. Portanto, $a^{\theta(G)} = a^{m\theta(a)} = (a^{\theta(a)})^m = e^m = e$.

□

Corolário 2.4. *Se n é um inteiro positivo e a e n são primos entre si, então*

$$a^{\phi(n)} \equiv 1(mod\ n);$$

em que $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+$ função de Euler definida por $\phi(1) = 1$ e, para $n > 1$, $\phi(n)$ é igual ao número de inteiros positivos menores que n e relativamente primos com n.

Demonstração.

Sejam $s_1, s_2, \ldots, s_k$ os inteiros de 1 a n, inclusive os extremos, que são primos com n (logo $k = \varphi(n)$). Dividamos cada as_i por n:

$$as_i = nq_i + r_i \ (0 \leq r_i < n).$$

Se esistisse um primo p tal que $p|n$ e $p|r_i$, dessa igualdade decorreria que $p|as_i$. Mas então $p|a$ ou $p|s_i$, o que é impossível já que o $\text{mdc}(a, n) = 1$ (hipótese) e ainda $\text{mdc}(n, s_i) = 1$, devido à escolha dos s_i. Donde n e r_i são primos entre si, para todo $i,\ 1 \leq i \leq k$.

Mostremos agora que na sequência de restos $r_1, r_2, \ldots, r_k$ não há elementos repetidos. De fato, se $r_i = r_j \ (1 \leq i, j \leq k;\ i \neq j)$, então $as_i - nq_i = as_j = nq_j$ e portanto $a(s_i - s_j) = n(q_i - q_j)$. Como $\text{mdc}(a, n) = 1$, então $n|(s_i - s_j)$. Como $1 \leq s_i, s_j \leq n$, então teríamos que ter $s_i = s_j$, o que não é possível, posto que $i \neq j$.

Disso tudo decorre então que $s_1, s_2, \ldots, s_k = r_1, r_2, \ldots, r_k$. Assim, se multiplicarmos as congruências $as_i \equiv 1(mod\ n)$ decorrentes de $as_i = nq_i + r_i$, $(1 \leq i \leq k)$:

$$a^k s_1 s_2 \cdots s_k \equiv (as_1)(as_2) \cdots (as_k) \equiv r_1 r_2 \cdots r_k (mod\ n)$$

os produtos $s_1 s_2 \cdots s_k$ e $r_1 r_2 \cdots r_k$ que nela aparecem são iguais. Como n é primo com cada r_j (ou s_i) e, portanto, com o produto $r_1 r_2 \cdots r_k$, então esse produto pode ser cancelado na última congruência, resultado a tese:

$$a^{\varphi(n)} \equiv 1(mod\ n)$$

pois $k = \varphi(n)$.

□

Exemplo 2.9. $\phi(8) = 4$, pois 1, 3, 5, 7 são os únicos números menores que 8 e relativamente primos com 8.

Corolário 2.5. *Se $p > 1$ é um número primo que não divide o inteiro a, então:*

$$a^{p-1} \equiv 1\ (mod\ p).$$

Demonstração.

Basta lembrar que se p é primo, então $\varphi(p) = p - 1$. □

Corolário 2.6. *Se p é um número primo e a é um inteiro qualquer, então*

$$a^p \equiv a \ (mod \ p).$$

Demonstração.

Se $\text{mdc}(a, p) = 1$, então, pelo corolário anterior:

$$a^{p-1} \equiv 1(mod \ p).$$

Daí, multiplicando por p:

$$a^p \equiv p(mod \ p).$$

Se $\text{mdc}(a, p) \neq 1$, então $a \equiv 0(mod \ p)$, pois p é primo. donde:

$$a^p \equiv 0 \equiv a(mod \ p).$$

□

Exemplo 2.10. Se $a > 0$ é um número inteiro, mostremos que a e a^5 tem o mesmo algarismo das unidades.

Se a_0 e $a_0^{'}$, respectivamente, indicam esses algarismos, então

$$a = 10q + a_0$$

e

$$a^5 = 10q + a_0^{'}$$

Assim:

$$a^5 - a = 10(q^{'} - q) + (a_0^{'} - a_0).$$

Note que se $a_0 = a_0^{'}$, então $10|(a^5 - a)$. Por outro lado, se $10|(a^5 - a)$, então $10|(a_0^{'} - a_0)$ e portanto $a_0^{'} = a_0$, já que $0 \leq a_0, a_0^{'} \leq 9$. Basta provar então que $a^5 = a$ é múltiplo de 10.

Mas o corolário 2.6 nos assegura que $a^5 \equiv a(mod \ 5)$, do que segue: $5|(a^5 - a)$. Por outro lado, como $a \equiv 0, \ 1(mod \, 2)$, então $a^5 \equiv 0, \ 1(mod \, 2)$ e portanto $a^5 - 5 \equiv 0(mod \, 2)$, ou seja, $2|(a^5 - a)$. O fato de 2 e 5 serem primos entre si garante então que $10|(a^5 - a)$.

Portanto a^5 e a tem a mesma paridade, uma vez que sendo $a = 2n$ um número par, a^5 será também um número par. Pois a soma de qualquer quantidade de inteiros pares é um inteiro par.

3 Criptografia de Chave Pública, Criptografia RSA

A grande utilização dos correios eletrônicos na atualidade, requer a garantia de duas propriedades importantes, a saber, preservam:

(a) *privacidade das mensagens*;

(b) *assinatura destas mensagens.*

Neste capítulo é apresentado como construir esses recursos em um sistema de correios eletrônico, cuja a essência é um novo método para estabelecer um sistema de criptografia de Chave Pública, conceito importante apresentado por Diffie e Hellman em [1]. No que segue usa-se como referência básica [7].

3.1 Sistemas de Criptografia de Chave Pública

Em um Sistema de Criptografia de Chave Pública, cada usuário coloca em um arquivo público um procedimento de codificação, E. Isto é, o arquivo público é um diretório em que é armazenado o procedimento de codificação de cada usuário. O usuário por sua vez mantém em segredo os detalhes do correspondente, procedimento de decodificação, D.

Estes procedimentos têm as seguintes propriedades:

(a) Aplicando o procedimento de codificação em uma mensagem M e após efetuar o procedimento de decodificação,

$$D(E(M)) = M \tag{3.1}$$

recuperamos M; e reciprocamente, ou seja:

$$E(D(M)) = M \tag{3.2}$$

(b) Ambas E e D são fáceis de calcular;

(c) Revelar publicamente E não põe em risco a definição de D;

A relação 3.1 é fundamentalmente para preservar a privacidade de mensagem, enquanto que a relação 3.2 é essencial para a segurança da assinatura.

Procedimentos de codificação e decodificação consistem em dois elementos básicos, a saber: de um *Método Geral* e uma *Chave de Codificação*. O Método Geral, controlado pela Chave especificada, codifica uma mensagem M, o resultado após esse processo é denominado texto cifrado C.

Em geral usa-se o mesmo Método Geral, sendo que a segurança do procedimento está na segurança da Chave escolhida; revelar o algoritmo de codificação significa portanto revelar a Chave.

Quando o usuário revela E, o caminho natural para conseguir D é testando todas as mensagens possíveis M até encontrar alguma, tal que $E(M) = C$; porém o número de mensagens a testar é ser tão grande que este caminho torna-se impraticável.

Observe que pode-se vislumbrar E e D como funções e nesse caso específico, uma vez que essas funções satisfazem 3.1 e 3.2, segue que uma é a inversa da outra e consequentemente, é uma função bijetora. Mais ainda a função bijetora E deve ter a característica de que sua inversa D seja bem difícil de ser obtida.

3.2 Privacidade

A criptografia é o modo padrão de tornar uma comunicação segura. O remetente codifica cada mensagem antes de transmiti-la ao destinatário. O destinatário conhece a função decodificadora apropriada a aplicar à mensagem recebida para obter a mensagem original. Um espião que escuta a mensagem transmitida escuta apenas "refugo", o texto codificado, que não faz nenhum sentido para ele a menos que este saiba como decodificá-la.

O grande volume de informações pessoais e confidenciais atualmente que é guardado em bancos de dados computadorizados e transmitido por linhas telefonicas torna a criptografia crescentemente importante. Reconhecendo o fato de que técnicas de criptografia eficientes e de alta qualidade são muito necessárias, porém em falta, o **National Bureau of Standards**, [sigla **NBS**], adotou um "*Padrão de Criptografia de Dados*", desenvolvido na IBM. Porém este Padrão é um procedimento que não garante a relação 3.2, necessária para implementar um Sistema de Criptografia de Chave Pública.

A maioria dos métodos clássicos de Criptografia (inclusive o padrão **NBS**) sofrem do "problema da distribuição da chave". O problema é que antes que uma comunicação privativa possa ser iniciada, uma outra transação privativa é necessária para distribuir as chaves de codificação e decodificação para o remetente e para o destinatário, res-

pectivamente. Geralmente um sistema de *e-mails* privado, é usado para enviar uma chave do remetente ao destinatário. Tal prática não é possível se um sistema de e-mails eletrônico deve ser rápido e barato. Entretanto no Sistema de Criptografia de Chave Pública abordado aqui, as chaves podem ser distribuidas através dos canais de comunicação considerados "não-seguros", o que é um grande avanço.

No que segue estabelece-se que A e B (também conhecidos como Alice e Bob) são dois usuários de um sistema de Criptografia de Chave Pública. Diferencie seus processos de codificação e decodificação com os subescritos E_A (codificação *de Alice*), D_A (decodificação *de Alice*), E_B (codificação *de Bob*) e D_B (decodificação *de Bob*).

Como poderá Bob enviar uma mensagem privada M a Alice num sistema de criptografia de chave pública? Primeiramente, ele recupera E_A do arquivo público. Então ele envia a mensagem codificada por $E_A(M)$. Alice descodifica a mensagem por obter $D_A(E_A(M)) = M$. Pela relação 3.1 do Sistema de Criptografia de Chave-Pública, apenas ela poderá decodificar $E_A(M)$. Esta pode codificar uma resposta privada com E_B, também disponível no arquivo público.

Dois usuários também podem estabelecer uma comunicação privativa em canais de coumunicação não-seguras sem consultar um arquivo público. Cada remetente envia sua chave de criptografia ao outro. Depois disso, todas as mensagens são codificada com a chave de codificação do destinatário como em um sistema de chave-pública. Um intrumento escutando a mensagem neste canal não poderá decifrar quaisquer mensagem, uma vez que não é possível obter as chaves de decodificação a partir das chaves de codificação. (Assume-se aqui que o intruso não pode modificar nem inserir mensagens no canal). Ralph Merkle desenvolveu outra solução para este problema em [6].

Um Sistema de Criptografia de Chaves-Pública pode ser usado para inicializar o esquema de codificação, assim como no método NBS. Uma vez que comunicações seguras já foram estabelecidas, a primeira mensagem transmitida pode ser uma chave para usar no esquema NBS, para codificar todas as mensagens seguintes. Isto pode ser necessário se o método de codificação é mais lento que com o esquema padrão. Observe que o esquema NBS é provavelmente mais rápido se houver algum hardware específico para codificação no computador; o esquema pode ser mais rápido em um computador com equipamentos comuns, uma vez que a multiprecisão das operações aritméticas são mais fáceis de implementar que as complicadas manipulações de bits.

Como foi observado anteriormente este procedimento cumpre dois requisitos importantíssimo:

(a) preserva a *privacidade das mensagens*;
(b) preserva a *assinatura destas mensagens.*

O primeiro item é o objetivo mais comum entre as técnicas de codificação, ao passo que a segunda é na atualidade mais importante. Com efeito, se o sistema de correios eletrônicos forem substituir o atual sistema de correios físico para transações de negócios, assinar uma mensagem deve ser exigido. O destinatário de uma mensagem assinada tem a prova de que a mensagem é oriunda daquele remetente. Esta qualidade é mais forte que uma mera autenticação (onde o destinatário pode verificar que a mensagem veio do remetente). O destinatário pode convencer um juiz que a pessoa que assinou é a mesma que enviou a mensagem. Para fazer isto, ele deve provar ao juiz que não forjou a mensagem assinada! Em um problema de autenticação o destinatário não precisa se preocupar com esta possibilidade, uma vez que ele quer apenas convencer a si próprio que a mensagem veio daquele remetente.

Uma assinatura eletrônica deve depender da mensagem, bem como do signatário. Se não for assim, o destinatário poderia modificar a mensagem antes de mostrar a mensagem-assinada a um juiz. Ou ele poderia anexar a assinatura a qualquer mensagem, uma vez que é impossível detectar recortagens e colagens eletrônicas. Para implementar assinaturas, o Sistema de Criptografia de Chave-Pública deve ser implementado com funções que cumprem a relação 3.2.

Voltando ao exemplo como o usuário Bob poderá enviar a Alice uma mensagem assinada M em um Sistema de Criptografia de Chave-Pública? Primeiramente ele calcula sua assinatura S para a mensagem M usando D_B :

$$S = D_B(M)$$

(Decifrar uma mensagem não codificada faz sentido à relação 3.2. de um sistema de criptografia de chave-pública: cada mensagem é um texto codificado para alguma outra mensagem). Ele então codifica S usando E_A e envia o resultado $E_A(S)$ para Alice. Ele não precisa enviar M junto; M pode ser calculada a partir de S.

Alice primeiramente decodifica o texto cifrado com D_A para obter S. Ela sabe quem é o suposto remetente da assinatura (neste caso, Bob); isto pode ser dado, se necessário for, no próprio texto anexado a S. Ela então extrai a mensagem com o procedimento de codificação do remetente, neste caso E_B (disponível no arquivo público):

$$M = E_B(S).$$

Ela agora possui um par $(M; S)$ mensagem-assinatura, com propriedades similares àquelas de um documento assinado em papel.

Bob não poderá, posteriormente negar ter enviado a Alice esta mensagem, uma vez que ninguém mais poderia ter criado $S = D_B(M)$. Alice pode convencer um juiz que

$E_{B(S)} = M$, de modo que ela tem a prova de que Bob assinou naquele documento.

Claramente, Alice não pode modificar M em uma versão diferente M', uma vez que, para isto ela teria que criar também a assinatura correspondente, $S' = D_B(M')$, pois D_B é uma função injetora.

Portanto Alice recebeu uma mensagem assinada de Bob, que ela pode provar ter sido ele quem a enviou, e ainda garantir que ela não a modificou. (Ela tampouco pode forjar sua assinatura para qualquer outra mensagem.)

Um sistema de checagem eletrônica poderia ser baseado num sistema de assinaturas como acima. É fácil imaginar um aparelho de codificação no seu terminal doméstico lhe permitindo assinar cheques que são enviados por correio eletrônico ao sacador. Seria apenas necessário incluir um único número de cheque de modo que, mesmo que o sacador copie o cheque, o banco apenas descontará a primeira versão que aparecer. Outra possibilidade surge se os aparelhos de codificaçao puderem ser rápidos o suficiente: seria possível ter uma conversa por telefone na qual cada palavra dita é assinada pelo aparelho de codificação antes da transmissão.

Quando a codificação é usada como acima, é importante que o aparelho de codificação não esteja conectado entre o terminal (ou computador) e o canal de comunicação, uma vez que uma mensagem pode ser sucessivamente codificada com várias chaves.

Assumi-se acima que cada usuário pode sempre acessar arquivo público de modo confiável. Numa rede de computadores isto pode ser difícil; um "intruso" pode forjar mensagens fingindo serem do Arquivo Público, o que pode ser evitada se o Arquivo Público assinar cada mensagem que envia ao usuário.

O usuário pode checar a assinatura como o algoritmo de codificação do Arquivo Público denominado E_{AP}. O problema de procurar E_{AP} no Arquivo Público é evitado dando a cada usuário a descrição de E_{AP} para colocá-lo no Sistema de Criptografia de Chave Pública e depositar seu procedimento público de codificação. Ele então armazena esta descrição ao invés de conferi-la de novo.

A necessidade de um correio entre cada par de usuários foi então substituida pela exigência de apenas um encontro seguro entre cada usuário e o gerente do arquivo público assim que esse entra no sistema. Outra solução é dar a cada usuário, quando ele se conecta, um livro (como uma lista telefônica) contendo todas as chaves de codificação dos usuários no sistema.

3.3 Métodos de Codificação e Decodificação

Sejam e e n números inteiros positivos quaisquer. Para Codificar uma mensagem M utilizando uma Chave Pública, denotada (e, n), primeiramente, representa-se a mensagem M como um inteiro entre 0 e $(n-1)$. Se a mensagem for longa, decomponha-a em uma série de blocos, e represente cada bloco como um inteiro. Use qualquer representação padrão. O propósito não é codificar a mensagem, mas apenas introduzir a forma numérica necessária para a codificação.

Então, codifique a mensagem elevando-a a e-ésima potência módulo n. Isto é, o Texto Cifrado C é o resto obtido quando M^e é dividido por n.

Para decodificar C, eleve-o a outra potência d, módulo n.

Os algoritmos de codificação e decodificação, E *e* D, são portanto:

$$C = E(M) \equiv M^e \ mod(n), \text{ para uma Mensagem } M.$$

$$D(C) \equiv C^d \ mod(n), \text{ para um Texto Cifrado } C.$$

Note que a codificação não aumenta o tamanho de uma mensagem; ambos, a Mensagem e o Texto Cifrado são inteiros entre 0 e $(n-1)$.

A chave de codificação é portanto o par de inteiros positivos (e, n), bem como a chave de decodificação é o par de inteiros positivos (d, n).

Cada usuário faz sua chave de codificação pública, e mantém a chave de decodificação correspondente segura. Inclusive o ideal seria denotar estes objetos por $n_A,\ e_A,\ d_A$, para cada usuário A.

Como escolher as chaves de codificação $(e,\ n)$ e de decodificação $(d,\ n)$? Ou seja, como escolher os números inteiros $n,\ e$ e d?

Primeiramente, se deve escolher n como sendo o produto de dois primos p *e* q,

$$n = pq.$$

Estes primos devem ser muito grandes e aleatórios.

Observe que apesar de tornar n público, os fatores p *e* q ficarão efetivamente ocultos de qualquer pessoa devido à enorme dificuldade de fatorar n.

Esta escolha também influencia a segurança da escolha de e a partir de d, a saber:

Escolha d como sendo um inteiro muito grande e que seja relativamente primos com produto $(p-1)(q-1)$.

Isto é, observe que d satisfaz:

$$MDC(d, (p-1)(q-1)) = 1.$$

Por sua vez o inteiro e é finalmente calculado a partir de $p,\ q$ e d como sendo o inverso multiplicativo de d módulo $(p-1)(q-1)$.

Logo,

$$ed \equiv 1 \; mod \; ((p-1)(q-1)).$$

O próximo passo é verificar se E e D, assim definidos, são funções que cumprem 3.1 e 3.2, ou seja, se E, D são funções bijetoras e uma inversa da outra.

Primeiramente do corolário 2.4 segue que

$$M^{\phi(n)} \equiv 1 \; (mod \; n), \tag{3.3}$$

em que ϕ é a função de Euler.

Observe que a função de Euler tem certas propriedades interessantes (conforme pode ser conferido em [4]):

- se p é um número primo então

$$\phi(p) = p - 1$$

- se $n = pq$, então

$$\phi(n) = \phi(p)\phi(q).$$

Desta maneira, segue que

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1.$$

Ou seja,

$$\phi(n) = n - (p+q) + 1. \tag{3.4}$$

Como d é relativamente primo com $(p-1)(q-1) = \phi(n)$, esse admite inverso, digamos e, no anel dos inteiros módulo $\phi(n)$, $\mathbb{Z}_{\phi(n)}$, e é tal que:

$$ed \equiv 1(mod\phi(n)), \tag{3.5}$$

isto é

$$ed = k\phi(n) + 1,$$

para algum $k \in \mathbb{Z}$.

Nessas circunstâncias tem-se

$$D(E(M)) = (E(M))^d = (M^e)^d \; (mod \; n) = M^{ed} \; (mod \; n).$$
$$E(D(M)) = (D(M))^e = (M^d)^e \; (mod \; n) = M^{ed} \; (mod \; n).$$

Entretanto, de 3.5,

$$M^{ed} = M^{k\phi(n)+1}(mod\ n).$$

Agora, de 3.3, vê-se que para todo M tal que p não divide M,

$$M^{p-1} \equiv 1\ (mod\ p).$$

E como $(p-1)$ divide $\phi(n)$,

$$M^{k\phi(n)+1} \equiv M\ (mod\ p), \forall M \in \mathbb{Z}. \tag{3.6}$$

Analogamente,

$$M^{k\phi(n)+1} \equiv M\ (mod\ q), \forall M \in \mathbb{Z}. \tag{3.7}$$

De 3.6 e 3.7 tem-se:

$$M^{ed} = M^{k\phi(n)+1} \equiv M\ (mod\ n).$$

Consequentemente,

$$M^{ed} \equiv M\ (mod\ n), \text{para todo } M,\ 0 \leq M < n.$$

Portanto,

$$D(E(M)) = M$$

e

$$E(D(M)) = M,$$

como queríamos.

3.4 Implementação do Algoritmo

Para mostrar que o método exposto é prático, descreve-se em seguida um algoritmo eficiente para cada operação requerida.

Calcular $M^e\ (mod\ n)$ requer, no máximo, $2 \cdot log_2(e)$ multiplicações e $2 \cdot log_2(e)$ divisões, usando o seguinte procedimento (a decodificação pode ser feita de modo análogo, apenas trocando d por e):

Passo 1. Seja $e_k e_{k-1} \ldots e_2 e_1 e_0$ a representação binária de e.

Passo 2. Fixe a variável C em 1.

Passo 3. Repita os passos $3a$ e $3b$ descrito abaixo para $i = k, k-1, \ldots, 1, 0$:

Passo $3a$. Tome C como o resto da divisão de C^2 por n;

Passo 3*b*. Se $e_i = 1$, então considere C como sendo o resto de $(C \cdot M)$ dividido por n.

Passo 4. Pare. Agora C é forma codificada de M.

Este procedimento é um dos melhores processos para estabelecer uma codificação(ou decodificação); para detalhes consulta [6].

Usando este algoritmo, um computador de alta velocidade de processamento e de grande capacidade de memória, onde são usados para cálculos muito complexos e tarefas intensívas, pode codificar uma mensagem de 200 dígitos em poucos segundos; um hardware de finalidade especial seria bem mais rápido. O tempo de decodificação por blocos aumenta menos que o cubo do número de dígitos em n.

Lembre-se que cada usuário deve (privadamente) escolher dois primos aleatórios muito grandes p e q para criar suas próprias chaves de codificação e decodificação. Esses números devem ser grandes a fim de que não seja computacionalmente praticável fatorar $n = pq$. Lembre-se que n, mas não p ou q, estará no arquivo público.

Recomenda-se usar um primo de 100 dígitos decimais p e q, de modo que n tenha 200 dígitos.

Para testar a primalidade de um número grande b, recomenda-se o elegante algorítmo probabilístico devido a Solovay e Strassen. [9]

Um computador de alta velocidade de processamento e de grande capacidade de memória, onde são usados para cálculos muito complexos e tarefas intensívas, também pode determinar em segundos se um número de 100 dígitos é primo, e pode encontrar o primeiro primo depois de um dado ponto em minuto ou dois. Outra abordagem para encontrar grandes números primos é tomar um número de fatoração conhecida, adicionar 1, e testar a primalidade do resultado. Se um primo p é encontrado, é possível provar que este é realmente primo usando a fatoração de $(p - 1)$.

Agora escolher um número d que é relativamente primo com $\phi(n)$ não é uma tarefa difícil. Por exemplo, qualquer número primo maior que $\max(p, q)$ o será. É importante que d seja escolhido em um conjunto grande o suficiente de modo que um criptanalista não possa encontrá-lo por busca direta.

Por outro lado, para determinar e é preciso mais atenção. A saber, usa-se o seguinte procedimento: primeiramente é preciso determinar o $mdc\{\phi(n),\ d\}$. Para tanto, estabeleça uma série $x_0, x_1, \ldots, x_k$, em que $x_0 = \phi(n), x_1 = d$ e $x_{i+1} \equiv x_{i-1}\ (mod\ x_i),\ 1 < i < k$, até que apareça $x_k = 0$; com isso tem-se que $mdc\{\phi(n),\ d\} = mdc(x_0, x_1) = x_{k-1}$.

Após esta etapa, para cada x_i, determine números a_i e b_i tais que $x_i = a_i x_0 + b_i x_1$. Se $x_{k-1} = 1$, então b_{k-1} é o inverso multiplicativo de $x_1\ (mod\ x_0)$. Como k será menor que $2log_2(n)$, este cálculo é muito rápido.

Se acontecer de e ser menor $log_2(n)$, comece escolhendo outro valor de d. Isto garante que cada mensagem codificada (exceto $M = 0$ *e* $M = 1$) sofra alguma repetição

(redução módulo n).

Exemplo 3.1. Considere $p = 47,\ q = 59,\ n = pq = 47 \cdot 59 = 2773$, seja que $\phi(2773) = \phi(47) \cdot \phi(59) = 46 \cdot 58 = 2668$. Então $d = 157$, e e é obtido seguindo o processo explicado anteriormente,

$$\begin{array}{llllll} x_0 = 2668, & a_0 = 1, & b_0 = 0, \\ x_1 = 157, & a_1 = 0, & b_1 = 1, \\ x_2 = 156, & a_2 = 1, & b_2 = -16 \text{ (uma vez que } 2668 = 157 \cdot 16 + 156), \\ x_3 = 1, & a_3 = -1, & b_3 = 17 \text{ (uma vez que } 157 = 1 \cdot 156 + 1). \end{array}$$

Portanto $e = 17$, o inverso multiplicativo módulo 2668 de $d = 157$.

Com $n = 2773$, pode-se codificar duas letras por bloco, substituindo um número de dois dígitos por cada letra: espaços em brancos considere como sendo = 00, e o alfabeto como segue: $A = 01$, $B = 02, \ldots, Z = 26$.

Assim a mensagem:

ITS ALL GREEK TO ME

é codificada por:

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

Como $e = 10001$ em binário, o primeiro bloco ($M = 920$) é cifrado:

$$M^{17} = (((((1)^2 \cdot M)^2)^2)^2)^2 \cdot M = 948 \ (mod\ 2773).$$

A mensagem inteira é cifrada como:

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655.

Exemplo 3.2. Considere $p = 11,\ q = 13,\ n = pq = 11 \cdot 13 = 143$, seja que $\phi(143) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120$. Então $e = 7$, é o menor primo que não divide120, ou seja é um inteiro positivo inversível módulo $\varphi(n)$ em que o $\text{mdc}(e, \varphi(n)) = 1$ e $d = 103$ é o menor inteiro positivo congruente a -17 módulo 120. Lembre se que $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$ Portanto o par (n, e) é chamado de *chave de codificação* do sistema RSA. Substitue-se um número de dois digitos por cada letra. Os espaços em brancos considere como sendo = 99 e o alfabeto como segue: $A = 10$, $B = 11, \ldots, Z = 35$.

Assim a mensagem:

PARATY É LINDA

é codificada por:

25102710293499149921182313 10

que quebrado em blocos b (que é um número inteiro positivo menor que) n. Deve-se evitar que o bloco comece por 0 porque isto traria problemas na hora de decodificar. Assim cada bloco fica representado por:

25 102 7 102 93 49 91 49 92 118 23 13 10.

Denota-se o bloco codificado por $C(b)$. A receita para calcular $C(b)$ é a seguinte:

$$C(b) = \text{resto da divisão de } b^e \text{por } n.$$

Em termos de aritmética modular, $C(b)$ é a forma reduzida de b^e módulo n.

Assim, o bloco 102 da mensagem é codificada como o resto da divisão de 102^7 por 143, fazendo as contas, obtém-se $C(b) = 119$.

Executa esta conta, calculando a forma reduzida de 102^7 módulo 143:

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv -81 \cdot 138 \equiv -24 \equiv 119(mod\ 143).$$

A mensagem inteira é cifrada como:

64 119 6 119 102 36 130 36 27 79 23 117 10.

Exemplo 3.3. Para codificar a palavra UNIVERSO, considere $p = 43$, $q = 59$, $n = pq = 43 \cdot 53 = 2279$, seja que $\varphi(2279) = \varphi(43) \cdot \varphi(53) = 2184$, $e = 5$ e $d = 437$.

Realiza-se uma pré codificação, deve-se associar cada letra a um número. Em seguida deve-se quebrar esse número em blocos de modo que o valor numérico de cada bloco seja menor que 2279. Dessa forma tem-se:

2114 0922 0518 1915.

Codifica-se utilizandos os seguintes cálculos:

$$2114^5 \equiv 1499(mod\ 2279).$$

$$922^5 \equiv 2094(mod\ 2279).$$

$$518^5 \equiv 1752(mod\ 2279).$$

$$1915^5 \equiv 748(mod\ 2279).$$

Logo a mensagem inteira é codificada como:

1499 2094 1752 0748.

Que substituindo pelas letras do alfabeto, temos o texto cifrado:

C = NIITIDQETGDH.

Para decodificar, tendo o valor de $d = 437$ basta calcular:

$$1499^{437} \equiv 2114(mod\ 2279).$$

$$2094^{437} \equiv 922(mod\ 2279).$$

$$1752^{437} \equiv 518(mod\ 2279).$$

$$748^{437} \equiv 1915(mod\ 2279).$$

Exemplo 3.4. Um exemplo sugestivo de sistema de criptografia de chave pública, apesar de infelizmente ser inútil pela fragilidade da escolha da chave pública, é utilizar uma matriz $E_{n\times n}$, como sendo chave pública.

Então para cifrar uma mensagen representado por n-vetor M, basta multiplicar por $E_{n\times n}$, que se tem como resultado $C = E \cdot M$.

Fazendo $D = E^{-1}$, encontra-se como resultado a mesma mensagem $M = D \cdot C$.

A fragilidade deste exemplo fica evidente uma vez que, para decifrar a mensagem (M), basta encontrar a matriz inversa da chave pública, que é a matriz $E_{n\times n}$ inversível.

Portanto temos:

a) Escolhe-se uma matriz $E_{n\times n}$ e a partir dela se obtém uma matriz $D = E^{-1}$.

$$E = (a_{ij})_{2\times 2} = \begin{pmatrix} 2 & 1 \\ 3 & 3 \end{pmatrix} \quad e \quad D = (a_{ij})_{2\times 2} = \begin{pmatrix} 1 & -1/3 \\ -1 & 2/3 \end{pmatrix}.$$

b) Para codificar a frase abaixo, utiliza-se a relação que associa cada letra a um número.

M	E	I	O	A	M	B	I	E	N	T	E	(frase)
13	5	9	15	1	13	2	9	5	14	20	5	(sequência de números)

A matriz M com a sequência numérica da mensagem que se deve enviar é:

$$M = (a_{ij})_{2\times 6} = \begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix},$$

codificando a frase temos: $C = E \cdot M = \begin{pmatrix} 2 & 1 \\ 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix} =$

$$= \begin{pmatrix} 31 & 33 & 15 & 13 & 24 & 45 \\ 54 & 72 & 42 & 33 & 57 & 75 \end{pmatrix}.$$

Portanto a frase MEIO AMBIENTE codificada fica:

C	O	D	C	C	G	B		O	D	U	C	C	C	X	E	G	D	E	G	E
3	15	4	3	3	7	2		15	4	21	3	3	3	24	5	7	4	5	7	5

c) Para decodificar a mensagem utiliza-se a identidade matricial $D = E^{-1}$ que é obtida a partir da chave pública $E_{n\times n}$, o que torna esse sistema frágil e a segurança totalmente comprometida. Assim temos que:

$$M = E^{-1} \cdot (EM) = \begin{pmatrix} 1 & -1/3 \\ -1 & 2/3 \end{pmatrix} \cdot \begin{pmatrix} 31 & 33 & 15 & 13 & 24 & 45 \\ 54 & 72 & 42 & 33 & 57 & 75 \end{pmatrix} =$$

$$\begin{pmatrix} 13 & 9 & 1 & 2 & 5 & 20 \\ 5 & 15 & 13 & 9 & 14 & 5 \end{pmatrix}.$$

Que é a matriz M com a sequência numérica da mensagem enviada.

Referências

[1] DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE Trans. Inform. Theory,*, IT22, p. 644–654, Nov1976.

[2] BUCHMANN, J. A. *Introdução à Criptografia, (tradução)*. São Paulo: Editora Berkeley, 2002.

[3] COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 2. ed. Rio de Janeiro: IMPA, 2011.

[4] HERSTEIN, I. N. *Tópicos de Álgebra; tradução de Adalberto P. Bergam e L. H. Jacy Monteiro*. São Paulo: Editora da Universidade e Polígono, 1970.

[5] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 2. ed. São Paulo: Atual Editora, 1982.

[6] KNUTH, D. E. *The Art of Computer Programming - Volume 2: Seminumerical Algorithms*. [S.l.]: Addison-Wesley, Reading, Mass., 1969.

[7] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *CACM*, l21, p. 120–126, 1978.

[8] SINGH, S. *O Livro dos Códigos, (tradução)*. São Paulo: Editora Record, 2004.

[9] SOLOVAY, R.; STRASSEN, V. A fast monte-carlo test for primality. *SIAM J.Comptng*, p. 84–85, 1977.

[10] DOMINGUES, H. H. *Fundamentos de Aritmética*. 1. ed. São Paulo: Atual Editora, 1981.