UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

SISTEMA DE CRIPTOGAFIA RSA

JOÃO GREGÓRIO CORRÊA NETO

RIO DE JANEIRO/RJ
2013

João Gregório Corrêa Neto

SISTEMA DE CRIPTOGAFIA RSA

Trabalho de Conclusão de Curso apresentado
ao Programa de Pós-graduação em
Matemática PROFMAT da UNIRIO, como
requisito para a obtenção do grau de MESTRE
em Matemática.

Orientador: Silas Fantin
Doutor em Matemática – USP

Rio de Janeiro
2013

Gregório, João Corrêa Neto

Sistema de criptografia RSA / João Gregório Corrêa Neto – 2013
84.p

1.Matemática 2. Álgebra. I. Título

João Gregório Corrêa Neto

SISTEMA DE CRIPTOGAFIA RSA

Trabalho Final de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da Universidade Federal do Estado do Rio de Janeiro, como requisito para a obtenção do grau de Mestre em Matemática.

Aprovada em 20 de agosto de 2013.

BANCA EXAMINADORA

Silas Fantin
Doutor em Matemática - USP

Fabio Xavier Penna
Doutor em Matemática - IMPA

Rodrigo Salomão
Doutor em Matemática - IMPA

Dedicatória

Dedico a Deus, por ter consentido que eu realizasse este trabalho iluminando, nas horas mais difíceis, a minha caminhada para que eu atingisse os meus objetivos, a minha esposa Ana Paula que me apoiou nos momentos de dificuldade, meus filhos Ana Beatriz e João Guilherme que se privaram da minha presença em muitos finais de semana e feriados e souberam entender que é o melhor para todos, ao meu pai em memória, pois esse era um dos sonhos dele, minha mãe e a todos meus amigos que de alguma maneira puderam me ajudar.

Resumo

Este trabalho de conclusão de curso do programa de Pós-graduação em matemática PROFMAT da UNIRIO apresenta um resumo histórico sobre o desenvolvimento da criptografia, as ideias a partir das quais foram criados alguns dos métodos de criptografia atuais e culmina na apresentação do sistema de criptografia RSA.

Esse trabalho foi desenvolvido em conjunto com o trabalho do professor Sérgio Santos Corrêa Junior cujo tema é Criptografia Via Curvas Elípticas. Em ambos há pré-requisitos comuns e o mesmo resumo histórico.

Houve uma grande preocupação com o uso de uma linguagem adequada a alunos do ensino médio, por isso algumas demonstrações foram adaptadas e outras omitidas, por exigirem conhecimentos específicos que vão muito além da grade curricular desses estudantes Ao final do trabalho há uma proposta de algumas atividades que podem ser aplicadas a esses alunos. Tanto ao longo do desenvolvimento do trabalho quanto nas atividades propostas ao final, foi usado o programa computacional gratuito Geogebra e a calculadora do Windows.

Palavras-chaves: Criptografia, RSA**,** PLD, PDH.

Abstract

This Graduate final project of the Graduation program in Mathematics, PROFMAT, of UNIRIO presents a summary of the historical development of cryptography, the ideas from which were created some of its current methods and culminates with the RSA cryptosystem.

This work was developed jointly with Professor Sergio dos Santos Correia Junior whose theme is based on Crytography *via* Eliptic Curves. These works have both the same pre requisites and the same common historical summary.

There was a great concern with the use of appropriate language for high school students. So, some demonstrations were adapted and others omitted for going far beyond the mathematics high school curriculum. In the final part of this project we present some activities that can be applied to the high school students. The technology tools used in the proposed activities are the free software Geogebra and the windows calculator.

Keywords: Crytography, RSA**,** PLD, PDH.

Agradecimento

Agradeço, sinceramente

A minha querida e amada esposa Ana Paula que me apoiou nos momentos de dificuldade e aguentou meus momentos de stress.

Aos meus maravilhosos filhos Ana Beatriz e João Guilherme que são tudo para mim.

Ao professor Silas, o orientador desse trabalho, que com muita dedicação e talento soube ajudar e contribuir de modo decisivo para essa obra.

A todos os professores da UNIRIO, porque levaram a sério com dedicação e profissionalismo o curso de mestrado e fortaleceram a minha formação.

Ao meu pai que sempre me incentivou e partiu durante o curso e não pode realizar o seu sonho de ver seu filho mestre, minha mãe que eu amo.

Ao meu amigo Daniel que me incentivou e ajudou sempre no que pode.

A PMDC, que me concedeu uma licença para estudos, pois sem isso eu não teria conseguido.

A CAPES, pelo suporte financeiro, que permitiu a realização deste trabalho.

Sumário

INTRODUÇÃO

A necessidade de troca de informações entre os seres humanos, sem perigo de interceptação, existe desde os tempos da Roma antiga. Foi lá que surgiu o código de César, que consistia numa forma de embaralhar as letras de uma mensagem.

Em virtude da proliferação dos meios de comunicação e da necessidade de enviar numerosas mensagens – transferências bancárias, cartas de instruções para compra de ações, informações diplomáticas secretas, relatórios de atividades de espionagem – tornou-se muito desejável desenvolver métodos confiáveis de codificação de mensagens.

No passado os códigos eram secretos, apenas pelos que enviavam e recebiam as mensagens, mas sempre havia a possibilidade de estudar mensagens interceptadas e decifrá-las.

A criptografia (do grego Kryptós "escondido" e gráphein "escrita") é a ciência que estuda as formas e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível aos que não tem acesso as convenções previamente estabelecidas, e a criptoanálise é a ciência que estuda as formas de se decifrar tais informações.

Com o aparecimento dos computadores, novas formas de codificar as mensagens foram criadas, de modo que os usuários pudessem se comunicar com proteção. Entretanto, essa tecnologia estava restrita a governos e organizações militares.

Atualmente a criptografia consiste em uma série de fórmulas matemáticas, em que se utiliza um segredo (chamado de chave) para cifrar e decifrar as mensagens. Este segredo pode ser o mesmo para as duas operações (criptografia simétrica) ou pode haver segredos diferentes, um para cifrá-la e outro para decifrá-la (criptografia assimétrica).

O objetivo principal deste trabalho é estudar **as principais características de alguns sistemas de criptografia**, onde explanaremos sobre sua simplicidade e a extrema dificuldade de se violar o código através da utilização de alguns destes sistemas, onde tentaremos situar os leitores cronologicamente sobre os personagens que contribuíram com o assunto abordado. A contribuição inicial para os sistemas de

criptografia modernos foi proposta em 1976 por Diffie e Hellman e sua efetiva execução foi conseguida por Rivest, Shamir e Adleman, conhecido como sistema de criptografia RSA.

No primeiro capítulo, apresentaremos alguns métodos de criptografia antigos e um resumo histórico, mostrando como a criptografia contribuiu para o desenvolvimento tecnológico.

No segundo capítulo, apresentaremos os conceitos preliminares e a noção de número primo, que será o ingrediente fundamental para o desenvolvimento deste trabalho, além de alguns algoritmos de fatoração, em virtude da fatoração de grandes inteiros ser um problema extremamente difícil, e de algoritmos para o cálculo de potências de números com centenas de dígitos.

No terceiro capítulo, apresentaremos o Problema do Logaritmo Discreto (PLD), o Protocolo de Diffie e Hellman (PDH) e o sistema público de criptografia ElGamal, que servem de base para alguns sistemas de criptografia. O sistema ElGamal é um meio alternativo de criptografia, isento de patente, que foi criado para competir com o patenteado sistema de criptografia RSA.

No quarto capítulo descreveremos o sistema de criptografia RSA, explicando, dando exemplos e mostrando a segurança do método. .

Finalmente, no quinto capítulo, proporemos algumas atividades, que podem ser aplicadas em sala de aula, relacionadas com a abordagem desenvolvida neste trabalho.

CAPÍTULO 1

Durante milhares de anos, reis, rainhas e generais dependeram de uma comunicação eficiente para governar e comandar seus exércitos. Ao mesmo tempo, todos conheciam as consequências de suas mensagens caírem em mãos inimigas, revelando segredos preciosos. O risco da interceptação pelo inimigo motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de maneira que só o destinatário possa ler seu conteúdo.

Esta busca pelo segredo levou as nações a criarem departamentos especializados em elaborar códigos que garantissem a segurança das comunicações. Ao mesmo tempo, os decifradores de códigos inimigos tentavam quebrar esses códigos, para descobrir seus segredos. Esta batalha entre criadores de códigos e decifradores desenvolveu uma corrida armamentista intelectual que teve um grande impacto no curso da história humana. Seus esforços para preservar ou destruir o sigilo enriqueceram várias áreas, como a linguística, a teoria quântica e a Matemática.

1.1 O código de César

Um dos códigos mais simples consiste em substituir cada letra do alfabeto por outra. Este método recebe o nome de substituição monoalfabética. O primeiro documento, de que se tem notícia, que usou uma cifra de substituição para propósitos militares aparece na guerra da Gália de Júlio César. Segundo *As vidas dos Césares*, escrito no século II por Suetônio, um dos tipos de cifra de substituição usada por Júlio César consistia em substituir cada letra do alfabeto por outra que estivesse três casas à frente, onde a **primeira linha** consiste do alfabeto original e a **segunda linha** o alfabeto codificado. Na cifra de César, não eram considerados acentos nem os espaços entre as palavras.

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
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

Como exemplo, o texto codificado "PDWHPDWLFDHGLYHUWLGR" significa "Matemática é divertido".

Apesar de Suetônio só mencionar que César deslocava as letras em três casas, não é difícil imaginar que podemos deslocar de uma a vinte cinco casas, obtendo 25 codificações distintas. Também é claro que se um inimigo souber que a cifra foi feita deslocando-se as letras em algum número de casas, ele poderá, em no máximo 25 tentativas, descobrir a chave e cifrar a mensagem. No entanto, se permitirmos que a cifra seja feita por qualquer rearranjo do alfabeto original, então teremos muitas possibilidades, dificultando o trabalho do inimigo, conforme apresentado na **primeira linha** o alfabeto original e na **segunda linha** o alfabeto cifrado.

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

Esse é um exemplo de uma permutação das letras, obtendo uma nova cifra. Sabemos que são muitas cifras possíveis, mas podemos calcular o número exato. Se aceitarmos que cada letra possa ser substituída por outra ou por ela mesma, mas sem repetição de letras, ou seja, duas letras distintas não podem ser substituídas pela mesma letra, então podemos usar um raciocínio bem conhecido:

Para substituirmos a letra **a** existem 26 possibilidades e, para cada uma dessas, existem 25 possibilidades para substituirmos a letra **b** (uma já foi usada pela letra a) e, para cada modo de substituir a e b, há 24 substituições possíveis para a letra **c** (já foram usadas duas possibilidades, uma para a letra a e outra para a letra b), e assim por diante até que para a letra **z** restará uma única possibilidade. Pelo princípio multiplicativo, chegamos ao número.

$$26 \,.\, 25 \,.\, 24 \ldots 2 \,.\, 1 = 26\,!\,(\,vinte\ e\ seis\ fatorial\,)$$

Com o auxílio de um computador encontramos

$$26! = 403.291.461.126.605.635.584\ \ x\ 10^6$$

Observe que 26! é um número gigantesco de cifras, mas neste cálculo admitimos que uma letra seja substituída por ela mesma, o que obviamente não é uma boa ideia, principalmente se isso ocorrer com várias letras.

Uma pergunta natural que surge é como podemos calcular o número de permutações em que nenhuma letra é substituída por ela mesma?

O matemático **Leonhard Euler (1707-1783)** encontrou uma solução genial para esse tipo de problema. As permutações em que nenhum elemento aparece em sua posição original são chamadas de PERMUTAÇÕES CAÓTICAS ou DESARRANJOS.

O número de cifras de substituição simples em que nenhuma letra seja substituída por ela mesma é dado por

$$D_n = 26!\left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots + (-1)^{26}\frac{1}{26!}\right)$$

Usando um computador encontramos

$$D_{26} = 148.362.637.348.470.135.821.287.825 \cong 148\,x\,10^{24}$$

Mesmo que alguém conseguisse verificar uma cifra por segundo, seriam necessários a seguinte quantidade de anos para se **verificar manualmente** todas as cifras possíveis

$$N = 4.704.548.368.482.690.760 \cong 4\,x\,10^{18}$$

A simplicidade e a força da cifra de substituição fizeram com que ela dominasse a arte da escrita secreta durante o primeiro milênio. Os estudiosos achavam que as cifras de substituição eram indecifráveis.

Os criptoanalistas árabes descobriram um método para quebrar a cifra de substituição monoalfabética. Eles perceberam que algumas letras aparecem com mais frequência que outras. As letras **a** e **i** são as mais comuns no idioma Árabe, enquanto que a letra **j** aparece com uma frequência dez vezes menor.

Embora não se saiba quem foi o primeiro a perceber que a frequência das letras podia ajudar a quebra de códigos, a descrição mais antiga desta técnica vem de um cientista do século IX, Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn Omran ibn Ismail al-Kindi, conhecido como o "filósofo dos Árabes".

Para decifrar uma mensagem através desse método, é necessário, em primeiro lugar, conhecer o idioma e contar a frequência com que cada letra aparece em um texto bastante longo. Em seguida, deve-se contar a frequência com que cada símbolo aparece no criptograma que se deseja decifrar.

Deste modo, o símbolo mais comum no criptograma deve ser substituído pela letra mais comum; o segundo símbolo mais frequente deve ser transformado na segunda letra com maior frequência e assim por diante.

Por exemplo, a frequência média de cada letra na língua portuguesa é dada na tabela.

Letra	**%**	**Letra**	**%**	**Letra**	**%**	**Letra**	**%**
A	14,64	G	1,3	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Assim, apenas contando a frequência de cada símbolo no texto, podemos descobrir a que letra correspondem os símbolos mais frequentes. Isto geralmente é suficiente para decifrar o código, mas só funciona bem se a mensagem for longa. É fácil escrever uma mensagem curta cuja contagem de frequência seja totalmente diferente da contagem de frequência média do português.

Por exemplo, em "Zuza zoou da Zezé" a letra mais frequente é o Z que aparece 5 vezes em um texto com 14 letras. Com $\frac{5}{14} \cong \mathbf{35\%}$, a porcentagem do Z no texto acima é muito maior que os usuais 0,47%. Já o A aparece uma só vez, o que da uma porcentagem de cerca de 7%; portanto abaixo dos 14% usuais.

1.2. A Cifra Indecifrável

Como a análise de frequência destruiu a segurança da cifra de substituição monoalfabética, os cifradores se empenharam na criação de outras cifras.

O diplomata Francês **Blaise de Vigenère (1523-1596)**, se destacou nessa tarefa, criando uma cifra poderosa conhecida como Le Chiffre Indéchiffrable (a cifra indecifrável).

A ideia de Vigenère foi usar não apenas um, mas 26 alfabetos cifrados distintos. Para isso criou uma tabela com o alfabeto real e mais 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior.

	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

Com o auxílio dessa tabela, cada letra pode ser cifrada usando qualquer uma das 26 linhas. Por exemplo, a letra G cifrada pela linha 16 se transforma na letra W e a letra P cifrada pela linha 23 se transforma na letra M, conforme pode ser observado na tabela a seguir.

	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

Assim, o remetente de uma mensagem pode usar, por exemplo:

- A linha 09 para cifrar a primeira letra de seu texto,
- A linha 15 para a segunda letra,
- A linha 05 para a terceira letra e assim por diante,

evitando que uma determinada letra seja sempre substituída por uma mesma letra.

Para que o destinatário possa decifrar a mensagem é necessário que ele saiba que linha foi utilizada em cada posição da mensagem, exigindo um sistema previamente combinado para a mudança entre as linhas. Para isso utilizava-se uma palavra chave, que precisava ser compartilhada previamente entre o remetente e o destinatário da mensagem, o que muitas vezes era um problema, principalmente quando essas pessoas não podiam se encontrar para combinar a chave.

Cada letra da palavra-chave identificava uma linha da tabela e cada linha era identificada pela primeira letra à sua direita:

- A linha 1 era identificada pela letra B,
- A linha 2 pela letra C,
- A linha 3 pela letra D e assim por diante,

até a linha 26, que era identificada pela letra A.

	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

Para entendermos como funcionava a palavra-chave, vamos cifrar a frase “Estou de férias” usando a palavra-chave “PONTE”. Primeiro escrevemos a palavra-chave repetidas vezes, até que cada letra da palavra-chave corresponda a uma letra da frase que se deseja enviar.

P	O	N	T	E	P	O	N	T	E	P	O	N
E	**S**	**T**	**O**	**U**	**D**	**E**	**F**	**E**	**R**	**I**	**A**	**S**

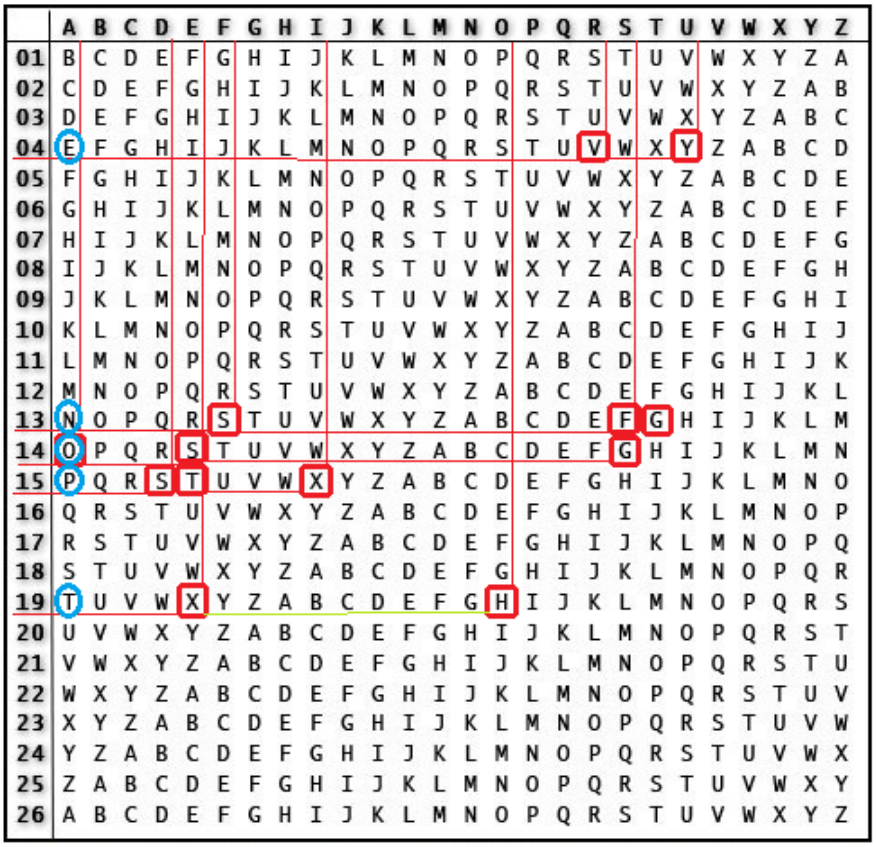
Desta forma, temos que:

- A letra **E**, será cifrada pela linha 15 (correspondente à letra P na tabela), transformando-se em **T**
- A letra **S** será cifrada pela linha 14 (correspondente à letra O na tabela), transformando-se em **G**
- A letra **T** será cifrada pela linha 13 (correspondente à letra N na tabela), transformando-se em **G**
- A letra **O** será cifrada pela linha 19 (correspondente à letra T na tabela), transformando-se em **H**
- A letra **U** será cifrada pela linha 04 (correspondente à letra E na tabela), transformando-se em **Y**
- A letra **D** será cifrada pela linha 15 (correspondente à letra P na tabela), transformando-se em **S**
- A letra **E** será cifrada pela linha 14 (correspondente à letra O na tabela), transformando-se em **S**
- A letra **F** será cifrada pela linha 13 (correspondente à letra N na tabela), transformando-se em **S**
- A letra **E** será cifrada pela linha 19 (correspondente à letra T na tabela), transformando-se em **X**
- A letra **R** será cifrada pela linha 04(correspondente à letra E na tabela), transformando-se em **V**
- A letra **I** será cifrada pela linha 15(correspondente à letra P na tabela), transformando-se em **X**
- A letra **A** será cifrada pela linha 14(correspondente à letra O na tabela), transformando-se em **O**
- A letra **S** será cifrada pela linha 13(correspondente à letra N na tabela), transformando-se em **F**

A frase cifrada (codificada) fica

TGGHYSSSXVXOF

Conforme pode ser observado na tabela abaixo



	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

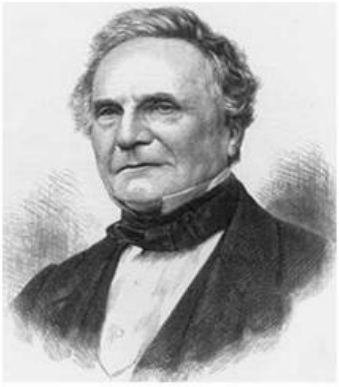
É óbvio que qualquer pessoa que conheça a palavra-chave pode decifrar uma mensagem cifrada pelo método de Vigenère. Mas e sem essa chave? **Você conseguiria decifrar as mensagens abaixo sem a palavra-chave?**

TPICQFZCTUFSMQPUD	QOPVNVSERYNQFV
PJSWLZFVZJCUZXNYOPVCOI	RSOCAIPCZHSFUUNIB
UODTYXYHLGTRLPABSIXDU	LDVKOEOLEIAACBEONIEV
BPONPUFVZJCUZ	

Se você não conseguiu não fique frustrado, pois realmente é muito difícil decifrar sem conhecer a chave. Para se ter uma ideia, foram necessários mais de 300

(trezentos) anos para que alguém conseguisse decifrar uma mensagem sem conhecer a palavra-chave.

Charles Babbage (1791-1871) na foto ao lado e Friedrich Kasiski conseguiram tal feito, independentemente um do outro. Kasisk ainda publicou este avanço da criptoanálise no *Die Geheimschriften und die Dechiffrir-kunst* (**A escrita secreta e a arte de decifrá-la**).



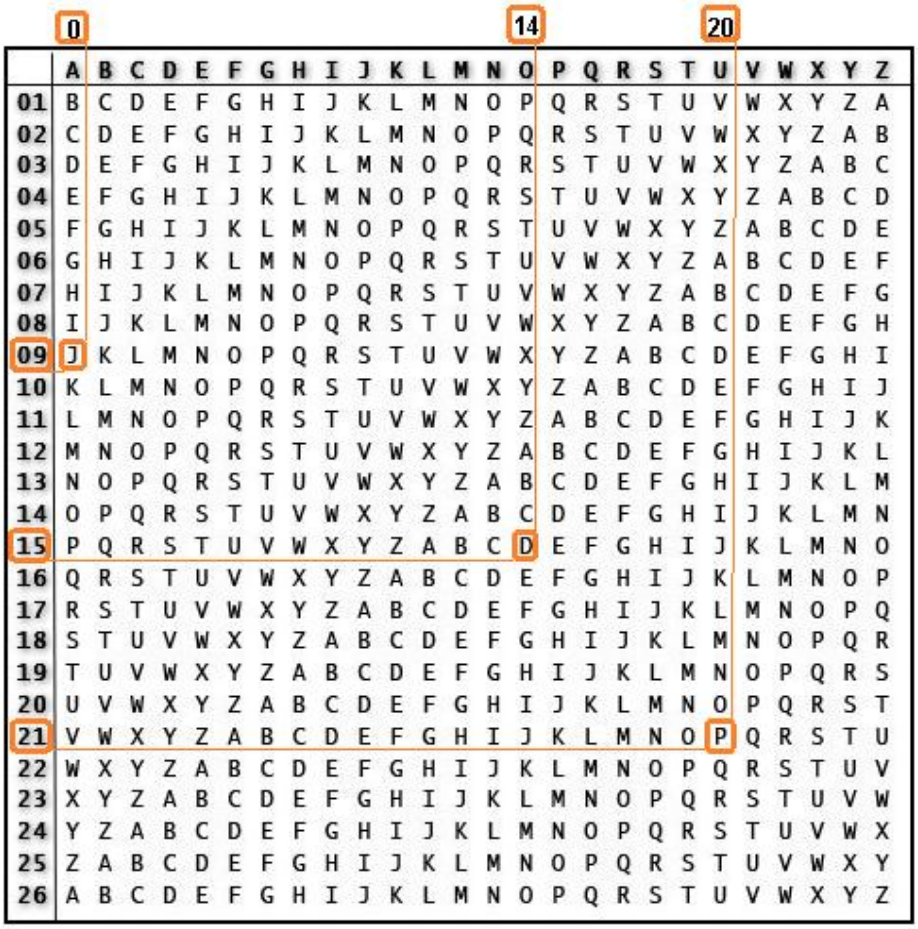
Mesmo conhecendo as técnicas desenvolvidas por Babbage e Kasisk pode-se levar bastante tempo tentando decifrar uma mensagem sem conhecer a palavra-chave. A palavra-chave usada na cifra da mensagem anterior é PAULINHO. Tente decifrar a mensagem. A resposta é um trecho da música "Solução de vida" de Paulinho da Viola.

E por isso eu lhe digo	Que não é preciso
Buscar solução para a vida	Ela não é uma equação
Não tem que ser resolvida	A vida, portanto, meu caro
Não tem solução	

Podemos equacionar a criptografia e a descriptografia da cifra de Vigenère. Como são 26 letras, podemos pensar em congruência módulo 26, ou seja, nos restos das divisões por 26. Assim teremos

$B = 1$	$C = 2$	$D = 3$	...	$Z = 25$	$A = 0$

Observe que o valor de cada letra na tabela de Vigenère é côngruo à soma dos valores da linha e da coluna à qual ela pertence, módulo 26.



	0													14					20					
	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

- A letra **J** destacada acima está na linha 9 e coluna 0(zero).

  $0 + 9 \equiv 9\ (mod\ 26)$ e 9 é o valor atribuído à letra J.

- A letra **D** destacada acima está na linha 15 e coluna 14.

  $15 + 14 \equiv 3\ (mod\ 26)$ e 3 é o valor atribuído à letra D.

- A letra **P** destacada acima está na linha 21 e coluna 19.

  $21 + 19 \equiv 14\ (mod\ 26)$ e 14 é o valor atribuído à letra P.

Se quisermos saber que letra se encontra na linha 17 e coluna 22, basta calcular

$$17 + 22 \equiv 13\ (mod\ 26).$$

A letra que está nesta posição é a letra representada pelo número 13, ou seja, é a letra N.

Portanto, para criptografar podemos somar o número que representa a letra que queremos cifrar (coluna) com a letra da palavra-chave que será utilizada (linha) e tomar o resto da divisão dessa soma por 26. O valor desse resto é a letra criptografada.

De modo geral, se α representa o número de uma letra do texto real, λ o número da letra da palavra-chave correspondente a essa letra real, podemos calcular β, o valor da letra codificada, pela equação:

$$\beta \equiv \alpha + \lambda \, (mod\ 26)$$

Analogamente, para decodificada, basta calcular α tal que:

$$\alpha \equiv \beta - \lambda \, (mod\ 26)$$

Por exemplo, vamos codificar a palavra MESTRADO usando a palavra-chave KZW

K	**Z**	**W**	**K**	**Z**	**W**	**K**	**Z**
10	25	22	10	25	22	10	25
M	**E**	**S**	**T**	**R**	**A**	**D**	**O**
12	4	18	19	17	0	3	14

Codificando, temos que:

$10 + 12 \equiv 22\ (mod\ 26) \Rightarrow letra\ W$	$25 + 4 \equiv 3\ (mod\ 26) \Rightarrow letra\ D$
$22 + 18 \equiv 14\ (mod\ 26) \Rightarrow letra\ O$	$10 + 19 \equiv 3\ (mod\ 26) \Rightarrow letra\ D$
$25 + 17 \equiv 16\ (mod\ 26) \Rightarrow letra\ Q$	$22 + 0 \equiv 22\ (mod\ 26) \Rightarrow letra\ W$
$10 + 3 \equiv 13\ (mod\ 26) \Rightarrow letra\ N$	$25 + 14 \equiv 13\ (mod\ 26) \Rightarrow letra\ N$

A palavra codificada ficou WDODQWNN, vamos agora decodificar:

$22 - 10 \equiv 12\ (mod\ 26) \Rightarrow letra\ M$	$3 - 25 \equiv -22\ (mod\ 26) \Rightarrow letra\ E$
$14 - 22 \equiv -8\ (mod\ 26) \Rightarrow letra\ S$	$3 - 10 \equiv -7\ (mod\ 26) \Rightarrow letra\ T$
$16 - 25 \equiv -9\ (mod\ 26) \Rightarrow letra\ R$	$22 - 22 \equiv 0\ (mod\ 26) \Rightarrow letra\ A$
$13 - 10 \equiv 3\ (mod\ 26) \Rightarrow letra\ D$	$13 - 25 \equiv -12\ (mod\ 26) \Rightarrow letra\ O$

1.3. MECANIZAÇÃO DO SIGILO

Desde que Babbage e Kasiski destruíram a segurança da cifra de Vinegère, nenhum outro método eficaz de criptografia foi inventado. Com o surgimento do telégrafo, no século XIX, e principalmente após a invenção do rádio, por Guglielmo Marconi, na virada do século, era desejada a criação de uma nova cifra que permitisse que os homens de negócio e os militares explorassem a rapidez das telecomunicações com segurança.

Em 1918 o inventor alemão **Arthur Scherbius (1878 -1925)** desenvolveu uma máquina criptográfica chamada ENIGMA, que ficou muito conhecida na 2ª guerra mundial.

A máquina Enigma consistia em um certo número de componentes engenhosos, como os modificadores, que eram peças que giravam a cada tecla usada, alterando a cifra.

Em 1925 Scherbius começou a produção em massa das máquinas enigmas. Nas duas décadas seguintes os militares alemães compraram 30 mil dessas máquinas. As Máquinas Enigmas se mostraram tão eficientes que os Britânicos e Franceses desistiram de tentar decifrar as mensagens criptografadas por essas máquinas e passaram essa tarefa para os Poloneses.

Somente em 1939 os segredos da Enigma foram completamente desvendados pelos **matemáticos Polacos** Marian Rejewski, *Jerzy Różycki e Henryk Zygalski apresentados abaixo:*

Marian Rejewski

Jerzy Różycki

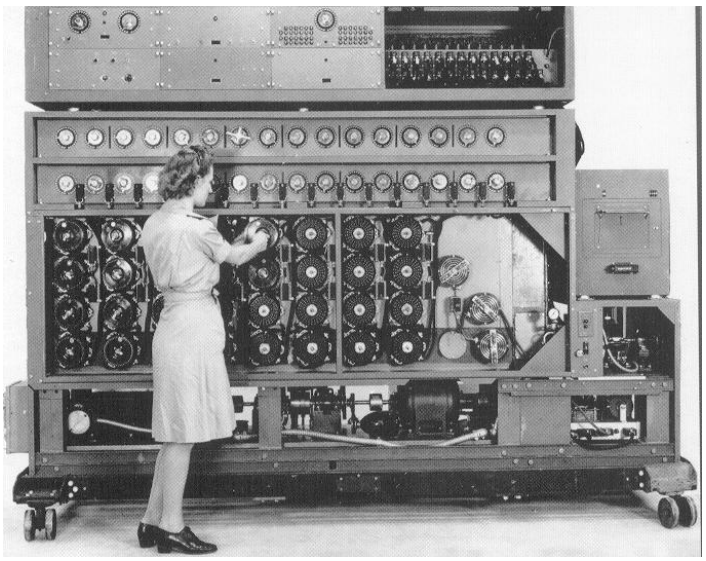
Henryk Zygalski

Essa façanha exigiu muito trabalho e dedicação e contou até com a traição de um Alemão chamado Hans-Thilo Schmidt, que vendeu, para um agente secreto Francês, dois documentos que explicavam o uso da máquina enigma. A busca por novos atalhos criptográficos era necessária, pois a máquina Enigma continuou evoluindo durante a guerra.

Os criptoanalistas eram continuamente desafiados a melhorar ou criar estratégias inteiramente novas. Houve muitos criptoanalistas notáveis e muitos avanços significativos, mas um deles merece ser destacado:

Alan Turing (1912-1954) identificou a maior fraqueza da máquina Enigma, conseguindo quebrar a cifra nos momentos mais difíceis.

Com suas ideias, Turing finalizou, no início de 1940, o projeto de uma máquina capaz de quebrar as cifras da Enigma. Tal máquina tinha dois metros de altura, por dois de comprimento e um metro de largura e recebeu o nome de Bomba de Turing.



Uma Máquina de Turing em ação

Antes de Turing ser convidado para trabalhar como criptoanalista, ele escreveu, aos 26 anos, um artigo sobre uma máquina hipotética capaz de se adaptar a diversos problemas de lógica. Esse equipamento imaginário recebeu o nome de máquina universal de Turing e foi a primeira ideia para o nosso computador atual.

Durante a Segunda Guerra Mundial os decifradores de códigos britânicos levaram a melhor sobre os criadores de códigos alemães. Além das maquinas de Turing, usadas para quebrar as cifras da Enigma, os britânicos criaram a máquina Colossus, usada para combater uma cifra ainda mais poderosa, a cifra alemã Lorenz.

A cifra Lorenz, feita pela máquina Lorenz SZ40, era usada para codificar a comunicação entre Hitler e seus generais. Essa nova cifra era muito mais complicada e trouxe um grande desafio para os decifradores de códigos. Certo dia, **Max Newman**, um matemático de Bletchley, apresentou, baseando-se nas ideias de Turing, um modo de mecanizar a criptoánalise da cifra Lorenz.

Max Newman (1897-1984) projetou a máquina **Colossus**, considerada a mãe de todos os computadores.

CAPÍTULO 2

Os métodos de criptografia mais modernos, assim como suas ideias principais, exigem alguns conceitos e teoremas da teoria dos números, que é o ramo da matemática pura que estuda propriedades dos números em geral, e em particular dos números inteiros. Por isso, neste capítulo, apresentaremos alguns tópicos dessa teoria que são essenciais para a perfeita compreensão dos próximos capítulos.

2.1. Principio da Indução e congruência

O principio da indução é um método poderoso e eficaz para verificar se uma proposição válida para um natural n, também é válida para todos os naturais maiores que n. O princípio de indução consiste em duas etapas:

1. Mostrar que a proposição é verdadeira para um natural n qualquer;
2. Mostrar que se a proposição vale para um natural k (hipótese de indução), então vale para o seu sucessor $k + 1$ (tese de indução).

Definição (congruência): Seja m um inteiro positivo. Definimos a relação de equivalência $\equiv (mod\ m)$ para todo $a, b \in \mathbb{Z}$ da seguinte maneira

$$a \equiv b\ (mod\ m) \quad \Leftrightarrow \quad a - b = k\,m \quad com \quad k \in \mathbb{Z}$$

Dizemos neste caso, que a é côngruo a b módulo m. É fácil ver que $\equiv (mod\ m)$ é uma relação de equivalência, isto é, que vale as seguintes propriedades:

- **Simetria**: $a \equiv a\ (mod\ m)$
- **Reflexiva**: $a \equiv b\ (mod\ m) \Rightarrow b \equiv a\ (mod\ m)$
- **Transitiva**: $a \equiv b\ (mod\ m)\ \ e\ \ b \equiv c\ (mod\ m) \Rightarrow a \equiv c\ (mod\ m)$

Sabemos que na divisão Euclidiana o resto é um número **não negativo**, porém, para facilitar os cálculos, muitas vezes trabalhamos com "restos negativos" na teoria de congruência. Por exemplo, $46 \equiv 4\ (mod\ 6)$ ou $46 \equiv -2\ (mod\ 6)$.

Propriedades de congruência:

1) **Soma:** $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m) \Rightarrow a + c \equiv b + d\ (mod\ m)$
2) **Produto:** $a \equiv b\ (mod\ m)\ e\ c \equiv d\ (mod\ m) \Rightarrow a * c \equiv b * d\ (mod\ m)$
3) **Potência**: $a \equiv b\ (mod\ m) \Rightarrow a^n \equiv b^n\ (mod\ m)$
4) **Divisão:** $a * c \equiv b * c\ (mod\ m)\ e\ mdc(c,m) = 1 \Rightarrow a \equiv b\ (mod\ m)$
5) **Corte:** $a * c \equiv b * c\ (mod\ m)\ e\ mdc(c,m) = d \Rightarrow a \equiv b\ (mod\ \frac{m}{d})$

Estas propriedades de congruências são de fácil verificação e serão uteis no decorrer do texto. Uma relação de equivalência define uma classe de equivalência. Dado $a \in \mathbb{Z}$, sua classe de equivalência módulo m consiste no conjunto

$$\bar{a} = \{ x \in \mathbb{Z};\ x \equiv a\ (mod\ m) \} = \{ x = a + km;\ k \in \mathbb{Z} \}$$

Temos que se $b \in \bar{a}$ então $\bar{b} = \bar{a}$. Dizemos que a é o representante da classe, porém podemos escolher qualquer elemento da classe como representante. Denotaremos por $\frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m$ o conjunto das classes de equivalência módulo m. Obviamente

$$\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1} \}$$

Sobre $\mathbb{Z}_m$ podemos definir uma soma quanto um produto cujo resultado independe da escolha dos representantes das classes:

- **Soma:** $\bar{a} + \bar{b} = \overline{a + b}$
- **Produto:** $\bar{a} * \bar{b} = \overline{a * b}$

Definição de Grupo: Um conjunto $(\boldsymbol{G}, *)$ não vazio munido de uma operação é denominado um grupo se satisfaz as seguintes condições:

- (Existência do Elemento Neutro): $\exists\ e \in G;\ a * e = e * a = a\ \forall\ a \in G$
- (Existência do Inverso): $\forall\ a \in G,\ \exists\ b \in G;\ a * b = e$
- (Associativa): $a * (b * c) = (a * b) * c\ \ \forall\ a, b, c \in G$

Proposição: $[\ \bar{a} \in \mathbb{Z}_m$ é $invertivel\ ] \Leftrightarrow [\ mdc\ (a,m) = 1\ ]$

Prova:

(⇒) $a \in \mathbb{Z}_m$ é invertível $\Rightarrow \exists\ \bar{b} \in \mathbb{Z}_m\ ;\ \bar{a}\,\bar{b} = \bar{1} \Rightarrow ab \equiv 1\ (mod\ m) \Rightarrow ab - 1 = (-k)\ m \Rightarrow ab + km = 1$. Como $mdc\ (a,m)$ divide a e m. Segue $mdc\ (a,m) = 1$.

(⇐) mdc (a,m) $= 1 \Rightarrow \exists\, b, k \in \mathbb{Z}\ tq\ \ ab + km = 1 \Rightarrow \bar{1} = \overline{ab + km} = \bar{a}\,\bar{b} + \bar{k}\,\bar{m}$ $\Rightarrow \bar{1} = \bar{a}\,\bar{b}$ em $\mathbb{Z}_m \Rightarrow a \in \mathbb{Z}_m$ é invertível.

Denotaremos por

$$(\mathbb{Z}_m)^* = \text{Conjunto dos elementos invertíveis de } \mathbb{Z}_m$$

Um número primo é um número inteiro maior do que 1, que só admite como divisores positivos ele próprio e 1. Os demais inteiros maiores que 1 são chamados de números compostos. Temos que $(\mathbb{Z}_{12})^* = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$, isto é, são os elementos de $\mathbb{Z}_{12}$ que são primos com 12.

Temos que $(\mathbb{Z}_m^*, *)$ formado pelos elementos invertíveis de $\mathbb{Z}_m$ formam um grupo que será utilizado no sistema RSA, onde m é o produto de dois números primos grandes.

O próximo resultado, conhecido por Pequeno Teorema de Fermat é um importante e bonito resultado da teoria dos números, devido ao Jurista e Magistrado por profissão, Pierre de Fermat (1601-1665) que dedicava à matemática seus momentos de lazer. Atuou em diversas áreas da Matemática, como Cálculo Infinitesimal, Teoria dos Números e Probabilidade.

Pequeno Teorema de Fermat *(P.T.F)*:

Se p é primo e a é inteiro, então $a^p \equiv a\ (mod\ p)$

Prova: Para provarmos o pequeno teorema de Fermat, vamos usar o fato de que se p é primo, então $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\ldots(p-(i-1))}{i!}$ com $1 \leq i \leq p-1$ são divisíveis por p pois todos os fatores de $i!$ são estritamente menores do que p primo. A prova segue por indução em a.

- Vale para $a = 1: \ 1^p - 1 = 0 = 0.p$
- Suponha que vale para $a = k$: $k^p - k = c.p$
- Vamos mostrar que vale para $a = k+1$: $(k+1)^p - (k+1) = d.p$

De fato:

$$(k+1)^p = k^p + \underbrace{\binom{p}{1}k^{p-1}1 + \binom{p}{2}k^{p-2}1^2 + \cdots + \binom{p}{p-1}k1^{p-1}}_{mp} + 1^p$$

$$= k^p + mp + 1$$

Subtraindo (k+1) em ambos os termos

$$(k+1)^p - (k+1) = k^p + mp + 1 - (k+1)$$

$$= (k^p - k) + mp$$

$$= cp + mp = (c+m)\,p$$

$$= d.p \qquad \blacksquare$$

Lembremos que se p é primo e p divide $(a.b)$ então p divide a ou p divide b. De fato, supondo que p não divide b então $mdc\,(p,b) = 1$. Assim $1 = mp + nb \Rightarrow a = mpa + nba = p\,(ma+nk) \Rightarrow p\ divide\ a$.

Como consequência imediata do *P.T.F*, temos que se p é primo e p não divide a, segue que $a^{p-1} - 1 = k\,p$, em linguagem de congruência, $a^{p-1} \equiv 1\ (mod\ p)$. De fato, do *P.T.F*, $a^p - a = a\left(a^{p-1} - 1\right) = r.p$. Como p é primo e não divide a, segue que p divide $(a^{p-1} - 1)$, isto é, $a^{p-1} - 1 = k\,p$.

Definição (Função de Euler): Dado um número inteiro positivo m, define-se

$$\phi(m) = \#\{\, k \in \mathbb{Z};\ com\ \ 0 < k < m \ \ e\ \ mdc\,(k,m) = 1\,\}$$

Basicamente, a função ϕ de Euler conta a quantidade de elementos de $\mathbb{Z}_m$ que são primos com m, isto é, $\phi\,(m) = \#\{\,\mathbb{Z}_m^*\,\}$. Por exemplo, temos que $\phi\,(8) = 4$, pois temos que $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ e é chamado de sistema reduzido de resíduos módulo 8. De maneira geral, para encontrarmos o sistema reduzido de resíduos módulo m, que são os elementos de $\mathbb{Z}_m^*$, basta retirar do sistema completo $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ os que não são primos com m.

Teorema de Euler: Se a e m são inteiros positivos e $mdc(a,m) = 1$, então

$$a^{\phi(m)} \equiv 1\ (mod\ m).$$

Note que o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat, que diz que se p é primo e não divide a temos que $a^{p-1} \equiv 1\ (mod\ p)$, visto que $\phi(p) = p - 1$. Uma prova deste resultado pode ser encontrada no livro: Introdução a Teoria dos Números de José Plínio de Oliveira Santos na página 43.

2.2. Números de Fermat e de Mersenne

Um resultado clássico na literatura conhecido como **Teorema Fundamental da Aritmética** diz que: "todo número composto é produto de números primos, e a menos da ordem dos fatores, esse produto é único". Desta forma, os números primos formam os blocos de base para construção dos números inteiros por meio da operação de multiplicação.

Assim, não é de estranhar que os números primos tenham sido objeto de estudo por várias gerações de matemáticos atraídos pela fascinação desses números, para responder questionamentos do seguinte tipo:

- Quantos números primos existem?
- Como reconhecer se um dado número é primo de maneira eficiente?
- Existem fórmulas ou algoritmos para gerar números primos?

Faremos um passeio por estes questionamentos sobre números primos, visto que o mesmo será o ingrediente fundamental para o desenvolvimento da criptografia moderna nos tempos atuais.

O primeiro questionamento que gostaríamos de responder é o seguinte: **Será que existe uma infinidade de números primos?**

A resposta é afirmativa, e a prova que apresentaremos a seguir foi dada por Euclides de Alexandria (360 a 295 a.C) que viveu no século 3 antes de cristo, e ficou conhecido como o Pai da Geometria, onde sua principal obra é conhecida como o livro "Os Elementos" apresentada em 13 volumes, servindo como principal livro de matemática para época, principalmente no que se refere ao que conhecemos hoje como Geometria Euclidiana.

A prova de Euclides é a seguinte: Suponhamos que a sucessão $p_1 = 2, p_2 = 3, \ldots, p_r$ dos r números seja finita. Consideramos então $P = p_1\, p_2 \ldots p_r + 1$ e seja p um número primo p que divide P. Esse número p não pode ser igual a qualquer um dos números primos $p_1, p_2, \ldots, p_r$ porque senão p dividiria a diferença $P - p_1\, p_2 \ldots p_r = 1$, o que é impossível. Assim p é um número primo que não pertence a sucessão

e, por consequência $p_1, p_2, \ldots, p_r$ não podem formar o conjunto de todos os números primos.

A demonstração de Euclides que acabamos de apresentar, é muito simples, entretanto, ela não fornece qualquer informação sobre o novo número primo p posto em destaque, a não ser que ele é, no máximo igual ao número $P = p_1\, p_2 \ldots p_r + 1$

Em 1878, o matemático Ernst Kummer (1810-1893) deu a seguinte variante da demonstração de Euclides: Suponhamos que exista somente um número finito de primos $p_1 < p_2 < \cdots < p_n$ e seja $N = p_1\, p_2 \ldots p_n > 2$. O inteiro N – 1 sendo (como todos os inteiros) o produto de fatores primos, teria então um fator primo p_i, que dividiria também N, então p_i dividiria $1 = N - (N - 1)$, o que é absurdo.

Será que existe uma maneira recorrente de encontrarmos números primos? Em 1640 Pierre de Fermat (1601 – 1665) afirmou que os números da forma $\boldsymbol{F_n = 2^{2^n} + 1}$ para $\boldsymbol{n \geq 0}$ são números primos, onde estes números são conhecidos como números de Fermat.

Os primeiros números de Fermat são $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65.537$ e é fácil ver que são primos. Em 1732, Leonard Euler (1707-1783) mostrou que $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ não é primo.

De fato: basta observarmos que

$$(1)\ 641 = 2^4 + 5^4 \qquad \text{e} \qquad (2)\ 641 = 2^7 .5 + 1.$$

Segue de (2) que $641 = 2^7 .5 + 1 \Rightarrow 5 = \frac{641-1}{2^7} = \frac{640}{2^7}$.

Substituindo em (1)

$$641 = 2^4 + 5^4 \Rightarrow 641 = 2^4 + \left(\frac{640}{2^7}\right)^4 = 2^4 + \frac{640^4}{2^{28}}$$

$$\Rightarrow 641 = \frac{2^{32} + 640^4}{2^{28}}$$

$$\Rightarrow 641 \,.\, 2^{28} = 2^{32} + 640^4$$

Assim, vemos que $2^{32} + 640^4$ é múltiplo de 641, ou seja:

$$2^{32} + 640^4 \equiv 0 \ (mod\ 641) \Rightarrow 2^{32} + (-1)^4 \equiv 0 \ (mod\ 641)$$

$$\Rightarrow 2^{32} + 1 \equiv 0 \ (mod\ 641)$$

$$\Rightarrow 2^{32} + 1 = k \,.641 \text{ para algum } k \in \mathbb{Z}\,.$$

A saber $F_5 = 2^{32} + 1 = 641 \,.6700417$.

Os números $\boldsymbol{F_n = 2^{2^n} + 1}$ **primos** são chamados de **primos de Fermat**, e pelos menos temos 5 conhecidos, a saber, F_0 a F_4. **Convêm perguntar se existem outros primos de Fermat?**

Em 1880, Landry obteve a fatoração de F_6 antes da era dos computadores

$$F_6 = 2^{2^6} + 1 = 274177 \ x \ 67280421310721$$

Em 1970, Morrison e Brillhart obtiveram a fatoração de $F_7 = 2^{2^7} + 1 =$ 596 49589127497217 x 5704689200685129054721.

números de Fermat	**Fatorado em**	**Por**
F_8	1980	Brent e Pollard
F_9	1990	Lenstra e Manasse
F_{10}	1995	Brent
F_{11}	1988	Brent e Morain

A fatoração de grandes números é um problema difícil. Não se conhece até agora nenhum algoritmo de tempo polinomial para realizar essa operação. É também um problema importante, por sua aplicação notável na criptografia de chave pública, que envolve números que devem ser difíceis de fatorar. Qualquer um que se interesse por essas questões, quando envolvem grandes números, tem necessidade evidente de ter acesso a

computadores modernos com alto poder de processamento. Não se conhecem outras fatorações dos números de Fermat e nada pode se afirmar sobre sua primalidade.

Será que existem infinitos números primos que seguem um determinado padrão? A resposta é afirmativa, como a dada por um teorema clássico de Teoria dos números conhecido por Teorema de Dirichilet que diz: "Se $mdc(a,b) = 1$ então a progressão aritmética $ak + b$ com $k = 1, 2, 3, \ldots$ contem infinitos primos".

Não é difícil mostrar que existem infinitos números primos da forma $4k + 3$ e $6k + 5$ com $k = 1, 2, 3 \ldots$ **que proporemos como atividades em sala de aula no capítulo 5**, imitando a prova dada por Euclides no século 3 antes de cristo.

Continuando a linha de números primos que segue um determinado padrão, convêm destacar Marin Mersenne, matemático amador do século XVII, onde $\boldsymbol{M_q = 2^q - 1}$ **(com q primo)** são chamados **números de Mersenne**. Desde o tempo de Mersenne era sabido que certos números de Mersenne são primos e que outros são compostos. Por exemplo $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ são primos, enquanto que $M_{11} = 23 * 89$.

Em 1640, Mersenne afirmou que M_q é primo para $q = 13, 17, 19, 31, 67, 127$ e 257; estava ele enganado em relação a 67 e 257; também não incluíra $61, 89$ e 107 (entre os números inferiores a 257) que também fornecem números de Mersenne primos. Sua afirmação era extraordinária, em face da grandeza dos números envolvidos.

Em relação aos números de Mersenne, o problema que se apresenta naturalmente, é de saber se são primos ou compostos e, neste ultimo caso, determinar seus fatores primos.

O seguinte resultado clássico sobre os fatores primos foi enunciado por Euler em 1750 e demonstrado por Lagrange em 1775 e ainda por Lucas em 1878: Se q é um número primo e $q \equiv 3\ (mod\ 4)$ então $2q + 1$ divide M_q se e somente se $2q + 1$ é primo; neste caso, se q > 3, então M_q é composto.

Assim se $q = 11, 23, 83, 131, 179, 191, 239$ ou 251 então M_q tem por fator $2q + 1$ dado por $23, 47, 167, 263, 359, 383, 479$ ou 503 respectivamente.

Exatamente como acontece com os números de Fermat, ainda existem vários problemas em aberto sobre os números de Mersenne:

- Existe uma infinidade de números de Mersenne primos?
- Existe uma infinidade de números de Mersenne compostos?

Até hoje são conhecidos 48 números de Mersenne M_q que são primos. O penúltimo deles com $q = 43.112.609$ com $12.978.189$ algarismos foi descoberto em 2008 por E. Smith, G.F Woltman, S. Kurowski e Gimps, sendo o primeiro número primo com mais de 10 (dez) milhões de algarismos, o que valeu aos descobridores o prêmio de 100.000 US dólares, outorgado pela Eletronic Frontier Foundation.

Números primos com mais de 1 (um) milhão de algarismos são chamados de megaprimos. Hoje já se conhecem 30 megaprimos, do quais 11 são números de Mersenne primos.

O maior deles com $q = 57.885.161$ com $17.425.170$ algarismos foi descoberto durante a realização desta monografia, em 25 de janeiro de 2013 por GIMPS (Great Internet Mersenne Prime Search) e Curtis Cooper.

CAPÍTULO 3

Neste capítulo, veremos como é possível enviar mensagens por um meio inseguro sem o contato prévio entre os participantes. Este avanço da criptografia é baseado no princípio da troca de uma caixa com cadeados.

Suponha que Joãozinho queira enviar uma caixa para Serginho por um meio inseguro, de modo que apenas Serginho possa abri-la.

- Joãozinho envia a caixa fechada com um cadeado para Serginho;
- Serginho coloca outro cadeado na caixa e a envia para Joãozinho;
- Joãozinho retira seu cadeado e reenvia a caixa para Serginho que consegue abri-la.

Em 1976, Whitfield Diffie e Martin Hellman publicaram um método que permite a troca de chaves, por um canal de comunicação inseguro, entre duas partes que não possuem nenhum conhecimento prévio, uma sobre a outra. Este método é conhecido como a troca de chaves de Diffie-Hellman.

Taher Elgamal, em 1984, baseando-se na ideia de Diffie e Hellman, construiu um método para enviar mensagens criptografadas por um meio de comunicação inseguro. Tal método é a base para alguns sistemas de criptografia, entre eles o método de criptografia via curvas elípticas.

Veremos a seguir que é fácil calcular potências, mesmo grandes, de um número g módulo N, no entanto, é muito difícil descobrir o expoente ao qual g foi elevado para gerar tal potência. Esse problema, conhecido como PROBLEMA DO LOGARITMO DISCRETO, é a ferramenta principal para as ideias brilhantes de Diffie-Hellman e El Gamal.

3.1. Algoritmo para o Cálculo de Potências:

Veremos como calcular potências grandes de um numero g módulo outro número N, onde N pode ter centenas de dígitos. O modo ingênuo de calcular g é por repetidas multiplicações por g.

$g_1 \equiv g \ mod\ N$	$g_2 \equiv g \,.\, g_1 \ mod\ N$	$g_3 \equiv g \,.\, g_2 \ mod\ N,$
$g_4 \equiv g \,.\, g_3 \ mod\ N$	$g_5 \equiv g \,.\, g_4 \ mod\ N$	$g_6 \equiv g \,.\, g_5 \ mod\ N$
	...	

É evidente que $g_A \equiv g^A \, mod \, N$, mas se A é grande, o algoritmo é completamente impraticável. Por exemplo, se $A \approx 2^{1000}$, então o algoritmo ingênuo levaria mais tempo do que a idade estimada do universo. Claramente, se isto é para ser útil, temos de encontrar uma melhor maneira de calcular $g^A \, mod \, N$.

Uma boa ideia é usar a expansão binária para o expoente A, ou seja, escrever $A = A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + \cdots + A_r \cdot 2^r$,com $A_0, A_1, \ldots, A_r \in \{0,1\}$, onde podemos assumir que $A_r = 1$.

Vale lembrar que para obtermos os valores de cada um dos A_{i_s}, podemos fazer ***divisões sucessivas*** por 2, começando pelo A, até obtermos um quociente zero. Deste modo os A_{i_s} serão os restos obtidos nessas divisões. Observe o exemplo:

Vamos escrever a expansão binária de 83

Divisões	**Quociente**	**Resto**	A_{i_s}
$83 \div 2$	41	1	$A_0 = 1$
$41 \div 2$	20	1	$A_1 = 1$
$20 \div 2$	10	0	$A_2 = 0$
$10 \div 2$	5	0	$A_3 = 0$
$5 \div 2$	2	1	$A_4 = 1$
$2 \div 2$	1	0	$A_5 = 0$
$1 \div 2$	0	1	$A_6 = 1$

Observando a tabela, podemos escrever:

$$83 = A_0 + A_1 \cdot 2^1 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + A_4 . 2^4 + A_5 . 2^5 + A_6 . 2^6$$

$$= 1 + 1 \cdot 2^1 + \mathbf{0} \cdot 2^2 + \mathbf{0} \cdot 2^3 + 1 \cdot 2^4 + \mathbf{0} \cdot 2^5 + 1 \cdot 2^6$$

$$= 1 + 2 + 2^4 + 2^6.$$

Exemplo 3.1: Suponha que desejamos calcular 7^{450} (mod 2563). O primeiro passo é escrever 450 como uma soma de potência de 2:

$$450 = 2 + 2^6 + 2^7 + 2^8 \Rightarrow 7^{450} = 7^{2+2^6+2^7+2^8} = 7^2 . 7^{2^6} . 7^{2^7} . 7^{2^8}$$

Note que é relativamente mais fácil calcular a sequência de valores abaixo, visto que, **cada número é o quadrado do anterior,** conforme observado abaixo

$$7 \quad , \quad 7^{2^1} = 7^2 \ , \quad 7^{2^2} = 7^4, \quad 7^{2^3} = 7^8 \ , \quad 7^{2^4} = 7^{16} \ , \quad \ldots$$

Além disso, visto que só precisamos destes valores módulo 2563, nunca precisaremos armazenar mais do que 4 dígitos. A tabela abaixo lista as potências de 7 módulo 2563 até 7^{2^8}.

i	0	1	2	3	4	5	6	7	8
7^{2^i} $(mod\ 2563)$	7	49	2401	614	235	1402	2346	955	2160

A criação da tabela acima, requer somente 8 multiplicações, e despista o fato de que o número $7^{2^8} = 7^{256}$ tem um expoente bastante grande, porque cada entrada sucessiva na tabela é igual ao quadrado da entrada anterior. Segue da tabela que

$$7^{450} = 7^2 . 7^{2^6} . 7^{2^7} . 7^{2^8}$$

$$\equiv 49 . 2346 . 955 . 2160 \ (mod\ 2563)$$

$$\equiv 1772 \ (mod\ 2563)$$

Note que o cálculo do produto $49 . 2346 . 955 . 2160$, pode ser reduzido módulo 2563 a cada multiplicação, não necessitando lidar com números muito grandes.

Exemplo 3.2: Determine $a, com\ 0 \leq a \leq 999,$ tal que $3^{218} \equiv a\ (mod\ 1000)$.

Como primeiro passo, escrevemos 218 como soma de potências de 2, dados por

$$218 = 2 + 2^3 + 2^4 + 2^6 + 2^7$$

Então 3^{218} torna-se

$$3^{218} = 3^{2+2^3+2^4+2^6+2^7} = 3^2 . 3^{2^3} . 3^{2^4} . 3^{2^6} . 3^{2^7}$$

Note que é relativamente mais fácil calcular a sequência de valores

$$3^{2^0} = 3 \quad , \; 3^{2^1} = 3^2 \; , \quad 3^{2^2} = 3^4, \quad 3^{2^3} = 3^8 \; , \quad 3^{2^4} = 3^{16}$$

visto que, cada número da sequência é o quadrado do anterior**.** Além disso, visto que só precisamos destes valores módulo 1000, nunca precisaremos armazenar mais do que 3 dígitos.

i	0	1	2	3	4	5	6	7
$3^{2^i} \; (mod\ 1000)$	3	9	81	561	721	841	281	961

Portanto

$$3^{218} = 3^2 . \; 3^{2^3} . 3^{2^4} . \; 3^{2^6} . \; 3^{2^7}$$

$$\equiv 9.561 \; .721 \; .281.961 \; (mod\ 1000)$$

$$\equiv 489 \; (mod\ 1000)$$

Observamos que tomamos apenas 11 multiplicações para calcular 3^{218} $(\ mod\ 1000)$, tendo uma enorme economia de tempo sobre a abordagem ingênua. E para expoentes grandes, poderíamos economizar ainda mais tempo, procedendo desta maneira.

Formalizando o Algoritmo para o Cálculo de potências

Passo 1: Calcule a expansão binária de A como

$$A = A_0 + \; A_1 2 + A_2 . 2^2 + \; A_3 \; . 2^3 + \cdots + A_r \; 2^r$$

com $A_0, \ldots A_r \in \{\, 0,1\}$ onde podemos assumir que $A_r \; = \; 1$

Passo 2: Calcule as potencias g^{2^i} $(\ mod\ N\ )$ para $0 \; \leq i \; \leq r$ por sucessivos quadraturas

$$a_0 \; \equiv g \qquad\qquad (mod\ N)$$

$$a_1 \; \equiv a_0^2 \; \equiv g^2 \quad (mod\ N)$$

$$a_2 \; \equiv a_1^2 \; \equiv g^{2^2} \quad (mod\ N)$$

$$a_3 \; \equiv a_2^2 \; \equiv g^{2^3} \quad (mod\ N)$$

. .
. .
. .

$$a_r \equiv a_{r-1}^2 \equiv g^{2^r} \pmod{N}$$

Cada termo é o quadrado do anterior, assim requeremos r multiplicações. No exemplo anterior $g = 3$ e identificamos os a_i

i	0	1	2	3	4	5	6	7
$3^{2^i} \pmod{1000}$	3	9	81	561	721	841	281	961
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7

Passo 3: Calculamos $g^A \pmod{N}$ usando a fórmula

$$g^A = g^{A_0 + A_1 2 + A_2 .2^2 + A_3 .2^3 + \ldots + A_r 2^r}$$

$$= (g)^{A_0} . (g^2)^{A_1} . \left(g^{2^2}\right)^{A_2} . \left(g^{2^3}\right)^{A_3} \ldots \left(g^{2^r}\right)^{A_r}$$

$$\equiv (a_0)^{A_0} . (a_1)^{A_1} . (a_2)^{A_2} . (a_3)^{A_3} \ldots (a_r)^{A_r} \pmod{N}$$

com $A_0, \ldots A_r \in \{0,1\}$ onde podemos assumir que $A_r = 1$

Note que os termos $a_0, a_1, \ldots, a_r$ foram calculados no Passo 2. Portanto o produto acima pode ser calculado procurando os valores de a_i cujos expoentes A_i é 1 e efetuamos sua multiplicação. Isso exige no máximo r multiplicações.

Tempo de Processamento: Executaremos no máximo $2r$ multiplicações módulo N para calcular g^A, isto é, no máximo $2 \log_2 A$ multiplicações módulo N para calcular g^A. De fato:

$$A \geq 2^r \Rightarrow \log_2 A \geq \log_2 2^r = r \Rightarrow 2r \leq 2 \log_2 A$$

Assim, mesmo se A é muito grande, digamos $A \approx 2^{1000}$, é fácil para um computador fazer aproximadamente 2.000 multiplicações necessárias para calcular 2^A módulo N

Exemplo 3.3: Segue do Pequeno Teorema de Fermat que $a^{p-1} \equiv 1 \pmod{p}$ e tomando $a = 2$ e $p = 15.485.863$ primo, que

$$2^{15.485.862} \equiv 1\ (mod\ 15.485.863)$$

Portanto, sem fazermos qualquer cálculo, sabemos que o número $2^{15.485.862} - 1$ é um número tendo mais do que 2 milhões de dígitos, é um múltiplo de 15.485.863

Observação: Um método razoavelmente eficiente para o cálculo de inversos módulo p, é obtido através do Pequeno Teorema de Fermat e do algoritmo para o Cálculo de potências, visto que

$$a^{p-1} \equiv 1\ (mod\ p)\ \ e\ \ \ a^{-1} \equiv a^{-1}\ (mod\ p) \quad \Rightarrow \quad a^{p-2} \equiv a^{-1}\ (mod\ p)$$

Isto nos dá uma alternativa para o método do Algoritmo Euclidiano Extendido. Na prática, os dois algoritmos tendem a ter aproximadamente a mesma quantidade de tempo.

Exemplo 3.4: Calcularemos o inverso de $a = 7814$ módulo $p = 17.449$ de 2 maneiras:

Primeiro, usando que: $a^{-1} \equiv a^{p-2}\ (mod\ p)$

$$7814^{-1} \equiv 7814^{17.447} \equiv 1284\ (mod\ 17.449)$$

Segundo, usando o algoritmo euclidiano extendido, temos que

$$7814\,u + 17.449\,v = 1$$

u será o inverso de $a = 7814$. A solução é $(u, v) = (1284, -575)$ assim $7814^{-1} \equiv 1284\ (mod\ 17.449)$.

Exemplo 3.5: Considere o número $m = 15.485.207$. Usando o algoritmo para o cálculo de potências, não é difícil calcular através de um computador a conta abaixo:

$$2^{m-1} = 2^{15.485.206} \equiv 4.136.685\ (mod\ 15.485.207)$$

Como não conseguimos o valor 1, parece que o Pequeno Teorema de Fermat não é verdadeiro para $m = 15.485.207$.

O que isso nos diz? Se m for primo então o pequeno Teorema de Fermat nos diz que deveríamos ter obtido 1. Portanto, o fato de não termos obtido o número 1, prova que o número $m = 15.485.207$ não é primo. Pensando nisso por um minuto,

vemos que isso é um pouco surpreendente, pois um simples cálculo mostra que m não é primo, sem sabermos nada sobre os fatores de m.

Não é fácil obter a fatoração de $m = 15.485.207 = 3853 \cdot 4019$

O Pequeno Teorema de Fermat nos diz que se a é um inteiro não divisível por p então $\boldsymbol{a^{p-1} \equiv 1\ (mod\ p)}$. No entanto, para algum valor especifico de a, podem existir potências menores de a que são congruentes a 1.

Definição: (ordem de a módulo p) Definimos a ordem de a módulo p como o menor expoente $k \geq 1$ tal que

$$a^k \equiv 1\ (mod\ p)$$

Exemplo 3.6.: Observe que $2^3 \equiv 1\ (mod\ 7)$ e que não existe número positivo menor que 3 ao qual elevamos 2 para obtermos resto 1 na divisão por 7. Logo a ordem de 2 modulo 7 é 3.

Proposição. Seja p um primo e a um inteiro não divisível por p. Suponha que $a^n \equiv 1(mod\ p)$. Então a ordem k de a módulo p divide n. Em particular, a ordem de a divide $(p-1)$.

Prova: Seja k a ordem de a módulo p, assim $a^k \equiv 1\ (mod\ p)$ e k é o menor expoente positivo com esta propriedade. Por hipótese, temos que $a^n \equiv 1\ (mod\ p)$. Dividindo n por k, obtemos que:

$$n = kq + r\ com\ 0 \leq r < k$$

Então

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^q \,.\, a^r \equiv (1)^q . a^r \equiv a^r\ (mod\ p)$$

Mas $r < k$, assim o fato de k ser a menor potência positiva inteira de a que é congruente a 1 implica que $r = 0$. Portanto, $n = k\,q$, assim k divide n. Em particular k divide $(p-1)$, pois pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1\ (mod\ p)$. ■

3.2. O Problema do Logaritmo Discreto (PLD)

O problema do logaritmo discreto é um problema matemático que surge em diversas situações, inclusive na utilização de curva elíptica para criptografia de mensagens.

O logaritmo discreto segue uma ideia análoga ao do logaritmo real que já conhecemos, porém ele é tratado módulo n. Para esclarecer vamos fazer uma comparação: para calcularmos o logaritmo de x na base a no conjunto dos números reais, devemos encontrar o número real x tal que $a^x = b$; agora, para calcularmos o logaritmo discreto de b na base a (a e b inteiros), devemos encontrar um inteiro x tal que $a^x \equiv b\ (mod\ n)$. Com essa ideia, queremos definir $x = log_a\, b$ como o logaritmo discreto de b na base a, com x em $\mathbb{Z}_n$, porém precisamos tomar alguns cuidados com as escolhas de n e de a. Veja alguns exemplos:

- $x = log_2(3)$ não existe para $n = 4$, pois $2^x \equiv 3\ (mod\ 4)$ não possui solução, visto que $2^x \equiv 0\ (mod\ 4)$ se x é par e $2^x \equiv 2\ (mod\ 4)$ se x é ímpar.
- $x = log_3(7)$ também não existe para $n = 11$. Verifique!

A impossibilidade de definir alguns logaritmos discretos pode ser evitada se trabalharmos em conjuntos onde eles sempre existam. Por isso falaremos de um importante teorema:

Proposição (**Teorema da Raiz Primitiva**): Seja p um número primo. Então existe um elemento $a \in (\mathbb{Z}_p)^*$ cujas potências geram cada elemento de $(\mathbb{Z}_p)^*$, isto é,

$$(\mathbb{Z}_p)^* = \{\, a^1, a^2, a^3, \dots, a^{p-2}, a^{p-1} = 1 \,\} = < a >$$

Elementos com esta propriedade são chamados raízes primitivas de $\mathbb{Z}_p$, ou geradores de $(\mathbb{Z}_p)^*$. Eles são os elementos de $(\mathbb{Z}_p)^*$ tendo ordem $p - 1$.

Exemplo 3.7: 2 é uma raiz primitiva de $\mathbb{Z}_{11}$. Basta observar que todos os elementos de $\mathbb{Z}_{11}^*$ são gerados por uma potência de 2.

$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	$2^4 = 5$
$2^5 = 10$	$2^6 = 9$	$2^7 = 7$	$2^8 = 3$	$2^9 = 6$
$2^{10} = 1$				

Exemplo 3.8: 2 não é uma raiz primitiva de $\mathbb{Z}_{17}$. Basta observar que ao calcularmos as potências de 2, retornamos a 1 antes de obtermos todos os 16 valores de $\mathbb{Z}_{17}^*$.

$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	$2^4 = 16$
$2^5 = 15$	$2^6 = 13$	$2^7 = 9$	$2^8 = 1$	

Exemplo 3.9: 3 é uma raiz primitiva de $\mathbb{Z}_{17}$. Basta observar que todos os elementos de $\mathbb{Z}_{17}^*$ são gerados por uma potência de 3.

$3^0 = 1$	$3^1 = 3$	$3^2 = 4$	$3^3 = 10$	$3^4 = 13$
$3^5 = 5$	$3^6 = 15$	$3^7 = 11$	$3^8 = 16$	$3^9 = 14$
$3^{10} = 8$	$3^{11} = 7$	$3^{12} = 4$	$3^{13} = 12$	$3^{14} = 2$
$3^{15} = 6$	$3^{16} = 1$			

Observação: Se p é grande então $\mathbb{Z}_p$ tem várias raízes primitivas. A fórmula precisa diz que $\mathbb{Z}_p$ tem exatamente $\phi\,(p-1)$ raízes primitivas onde ϕ é a função de Euler. Por exemplo, podemos checar que a lista completa de raízes primitivas de $\mathbb{Z}_{29}$ é dada por

$$\{\,2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27\,\}$$

A cardinalidade do conjunto coincide com o valor de $\phi\,(p-1) = \phi\,(28) = 12$.

Definição (Problema do Logaritmo Discreto) Seja a uma raiz primitiva de $\mathbb{Z}_p$, p primo, e seja b um elemento não nulo de $\mathbb{Z}_p$. O Problema do Logaritmo Discreto (PLD) é o problema de encontrar um expoente x tal que

$$a^x \equiv b \ (mod\ p)$$

O número x é chamado o logaritmo discreto de b na base a e é denotado por $\log_a(b)$.

O Problema do Logaritmo Discreto é um problema bem-posto, isto é, encontrar um expoente inteiro x tal que $a^x = b$. No entanto, se houver uma solução, então haverá infinitas soluções inteiras, pois se x é uma solução para $a^x = b$, então temos que $x + k\,(p-1)$ também é uma solução para cada valor de k em virtude do Pequeno Teorema de Fermat que diz que $a^{p-1} \equiv 1\ (mod\ p)$. De fato

$$a^{x+k(p-1)} \equiv a^x \cdot \underbrace{(a^{p-1})^k}_{\equiv 1^k,\ P.T.F.} \equiv b \cdot 1^k \equiv b\ (mod\ p).$$

Por exemplo, $2^8 \equiv 3\ (mod\ 11)$, $2^{8+10} \equiv 3\ (mod\ 11), 2^{8+2\cdot 10} \equiv 3\ (mod\ 11)$, de modo geral $2^{8+10k} \equiv 3\ (mod\ 11)$ para qualquer k inteiro.

Temos que $\log_a b$ está bem definido a menos de múltiplos de $(p-1)$. Desta forma, restringimos o contradomínio de $\mathbb{Z}$ para $\mathbb{Z}_{p-1}$ para que a função $\log_a$ esteja bem definida.

$$\log_a : (\mathbb{Z}_p)^* \rightarrow \mathbb{Z}_{p-1}$$

$$b \rightarrow x \ \ onde \ \ a^x = b$$

Em várias situações, nos referimos ao logaritmo discreto como o inteiro x situado entre 0 e $p-2$ satisfazendo a congruência $a^x \equiv b\ (mod\ p)$.

Exemplo 3.10: Por simplicidade, vamos considerar $p = 13$ e a $= 2$.

$$(\mathbb{Z}_{13})^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$$

$$= \begin{Bmatrix} 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, 2^5 = 6, 2^6 = 12 \\ 2^7 = 11, 2^8 = 9, 2^9 = 5, 2^{10} = 10, 2^{11} = 7, 2^{12} = 1 \end{Bmatrix}$$

$\log_2 : (\mathbb{Z}_{13})^* \rightarrow \mathbb{Z}_{12}$ dada por $\log_2 b = x$ onde $2^x = b$

$(\mathbb{Z}_p)^* = (\mathbb{Z}_{13})^*$ b	$b = 2^x$	$\mathbb{Z}_{p-1} = \mathbb{Z}_{12}$ $x = \log_2 b$
1	$1 = 2^{12}$	$0 = 12$
2	$2 = 2^1$	1
3	$3 = 2^4$	4
4	$4 = 2^2$	2
5	$5 = 2^9$	9
6	$6 = 2^{12}$	12
7	$7 = 2^{11}$	11
8	$8 = 2^3$	3
9	$9 = 2^8$	8
10	$10 = 2^{10}$	10
11	$11 = 2^7$	7
12	$12 = 2^6$	6

Exemplo 3.11: O número $p = 56.509$ é primo, e podemos checar que a $= 2$ é uma raiz primitiva módulo p. Como iremos calcular o logaritmo discreto de $\boldsymbol{b = 38679}$? O único método que é imediatamente óbvio, é calcular

$$2, 2^2, 2^3, 2^4, 2^5, \ldots \quad (mod\ p)$$

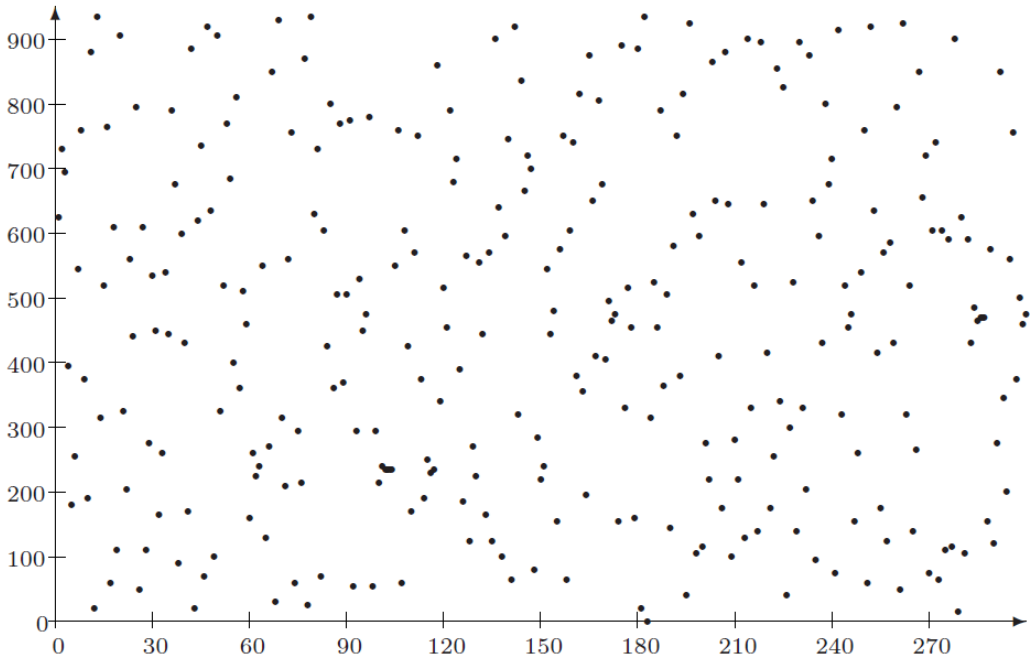
até encontrarmos alguma potência que seja côngruo a $b = 38679$ módulo $p = 56509$.

Seria difícil fazer a conta na mão, mas usando um computador, encontramos que

$$2^{11235} \equiv 38679\ (mod\ 56509),\ \text{ou seja,}\ \log_2(38679) = 11235.$$

Diferentemente dos logaritmos nos Reais, que são funções estritamente crescentes ou decrescentes (dependendo da base do log), os logaritmos discretos possuem imagens com caráter praticamente aleatório, o que torna sua resolução bastante difícil.

O exemplo anterior utilizou números pequenos, por isso foi facilmente resolvido através de um computador. No entanto, o cálculo de um logaritmo discreto pode se tornar difícil até para um computador, desde que os valores de a e p sejam cuidadosamente escolhidos. Essa dificuldade deu a Diffie e Hellman uma grande ideia, como veremos na seção a seguir.



O gráfico acima mostra a irregularidade das potências 627^x módulo $p = 941$

3.3. Protocolo de Diffie-Hellman (PDH) – Chave Trocada

O Algoritmo de Diffie –Helman ajudará a resolver o seguinte dilema. Cascão e Cebolinha desejam compartilhar uma chave secreta para uso em uma cifra simétrica, mas o seu único meio de comunicação é um canal de comunicação inseguro. Cada pedaço de informação que Cascão e Cebolinha compartilham, é observado pela Mônica.

Como é possível para Serginho e Joãozinho compartilhar uma chave sem torná-la disponível para Mônica? À primeira vista parece que Serginho e Joãozinho enfrentam uma tarefa impossível, contudo Diffie e Hellman encontraram uma solução.

No **primeiro passo**, Serginho e Joãozinho combinam a utilização de um número primo grande p e um inteiro não nulo g módulo p. Os valores de p e g, escolhidos por Serginho e Joãozinho, são tornados de conhecimento público, permitindo que qualquer pessoa, inclusive Mônica, também conheça esses números.

No **segundo passo** é Serginho escolher um inteiro secreto a que não irá revelar a ninguém, enquanto, ao mesmo tempo, Joãozinho escolhe um inteiro b, que ele manterá em segredo, não revelando a ninguém. Serginho e Joãozinho usam os inteiros secretos para calcular

$$\underbrace{A \equiv g^a \,(mod\ p)}_{Serginho\ calcula\ A} \qquad e \qquad \underbrace{B \equiv g^b \,(mod\ p)}_{Joãozinho\ calcula\ B}$$

No **terceiro passo**, Serginho envia o valor A para Joãozinho que, por sua vez, envia o valor B para Serginho. Note que Mônica começa a ver os valores de A e B, uma vez que eles são enviados através de um canal de comunicação inseguro. Novamente, Serginho e Joãozinho usam outra vez, seus inteiros secretos para calcular

$$\underbrace{A' \equiv B^a \,(mod\ p)}_{Serginho\ calcula\ A'} \qquad e \qquad \underbrace{B' \equiv A^b \,(mod\ p)}_{Joãozinho\ calcula\ B'}$$

Observe que os valores calculados, A' e B', são exatamente os mesmos, pois

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B'$$

Este valor comum onde $\boldsymbol{A' \equiv B' (mod\ p)}$ é a Chave Trocada **.**

Exemplo 3.12: Serginho e Joãozinho concordam em usar o primo $p = 941$ e a raiz primitiva $g = 627$.

- Serginho escolhe a chave secreta $a = 347$ e calcula
$$A = 390 \equiv 627^{347} \pmod{941}.$$
- Joãozinho escolhe a chave secreta $b = 781$ e calcula
$$B = 691 \equiv 627^{781} \ (mod\ 941).$$

Serginho envia para Joãozinho o número $A = 390$ e Joãozinho envia para Serginho o número $B = 691$. Ambas as transmissões são feitas por um canal de comunicação inseguro, assim, A e B podem ser considerados de conhecimento público.

Os números $a = 347$ e $b = 781$ não são transmitidos e permanecem secretos. Neste momento, Serginho e Joãozinho são capazes de calcular a chave compartilhada, que é igual a 470.

$$B^a = 470 \equiv 691^{347} \ (mod\ 941) \quad \text{e} \quad A^b = 470 \equiv 390^{781} \ (mod\ 941)$$

Suponha que Mônica tenha interceptado os inteiros $A = 390$ e $B = 691$ trocados por Serginho e Joãozinho. Para Mônica reconstituir as chaves secretas a e b de Serginho e Joãozinho, ela deverá resolver os seguintes problemas de congruência.

$$627^a \equiv 390 \ (mod\ 941) \quad \text{ou} \quad 627^{\text{b}} \equiv 691 \pmod{941}$$

Assim ela conhecerá os expoentes secretos. Tanto quanto se sabe, este é o único caminho para Mônica encontrar o valor secreto compartilhado de Serginho e Joãozinho, sem a assistência dos mesmos. É claro que os números utilizados em nosso exemplo são muito pequenos para oferecer segurança. Especialistas sugerem que o primo p escolhido tenha aproximadamente 1000 bits ($p \approx 2^{1000}$) e que o número g tenha ordem igual a um número primo próximo de $\frac{p}{2}$.

Em geral, o dilema de Mônica é este: Ela sabe quais são os valores $A = g^a$ e $B = g^b$ e também conhece os valores de p e g, por isso, se ela puder resolver o PLD, então ela poderá encontrar os valores a e b e, com isso, Mônica poderá calcular a chave secreta compartilhada $g^{ab} \ (mod\ p)$, que não foi transmitida em nenhum momento.

Aparentemente, Serginho e Joãozinho estão seguros desde que Mônica seja incapaz de resolver o PLD, mas isso não é uma verdade absoluta. É verdade que um método para encontrar o valor compartilhado entre Serginho e Joãozinho é resolver o PLD, mas talvez isso não seja necessário. A segurança da chave compartilhada de Serginho e Joãozinho repousa sobre a dificuldade de resolver o seguinte problema, potencialmente mais fácil.

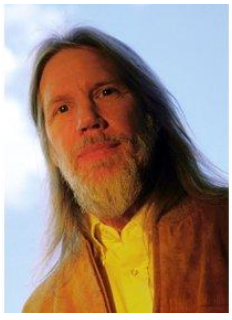
Definição: (Problema de Diffie - Hellman – *PDH*)

Seja p um número primo e g um inteiro. O Problema de Diffie-Hellman (PDH) é o problema de calcular o valor de $g^{ab}\ (mod\ p)$ a partir dos valores conhecidos de $A = g^a\ (mod\ p)$ e $B = g^b\ (mod\ p)$.

É claro que o *PDH* não é mais difícil do que o *PLD*. Se Mônica pode resolver o *PLD*, então ela pode calcular os expoentes secretos a e b de Cascão e Cebolinha que formam os valores interceptados $A = g^a$ e $B = g^b$, e então fica fácil Mônica calcular sua chave compartilhada, g^{ab} não transmitida em nenhum momento. Na verdade, Mônica necessita calcular apenas um dos valores de a e b, para conhecer a chave compartilhada.

O problema inverso é menos claro. **Suponha que Mônica tenha um algoritmo eficiente para resolver o *PDH*. Será que Mônica pode usá-lo também para resolver de maneira eficiente o *PLD*?** A resposta não é conhecida.

Diffie e Hellman perceberam, de forma brilhante, que a dificuldade do problema do Logaritmo Discreto para $(\mathbb{Z}_p)^*$ fornece uma possível solução para esse problema.



Diffie

Helman

3.4. O Sistema Público de Criptografia ElGamal

Veremos agora como funciona a ideia de Elgamal para enviar mensagens com segurança. Como esse método utiliza cálculos numéricos, surge a necessidade de substituir símbolos por números. A tabela ASCII (Código Padrão Americano para o Intercâmbio de Informação) fornece uma opção de pré-codificação.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Vamos supor que Serginho queira mandar uma mensagem para Joãozinho por um canal inseguro de modo que ninguém tenha acesso ao seu conteúdo. Digamos que essa mensagem, quando pré-codificada pela tabela ASCII, fique representada pelo número M.

Primeiramente, Joãozinho e Serginho combinam um número primo p e uma raiz primitiva g. Joãozinho utiliza uma chave secreta a com a qual calcula

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

e depois envia para Serginho o número A. Este escolhe uma chave provisória k e calcula:

$$c_1 \equiv g^k \ (mod\ p) \qquad e \qquad c_2 \equiv M\, A^k \ (mod\ p)$$

Deste modo, Serginho codifica a mensagem M criptografada pelo par (c_1, c_2), e em seguida, envia o par (c_1, c_2) para Joãozinho, que por sua vez decodifica a mensagem M através do par (c_1, c_2) com os seguintes cálculos:

Passo 1: Determina $x \equiv c_1^a \pmod p$

Passo 2: Determina x^{-1} módulo p, via Obs. página 40, pois $x^{p-2} \equiv x^{-1} \pmod p$,

Passo 3: Calcula

$$c_2\, x^{-1} \equiv (\, M\, .\, A^k\,) \cdot x^{-1} \equiv M\, .\, (g^a)^k \cdot x^{-1} \equiv M\, .\, (g^k)^a \cdot x^{-1}$$

$$\equiv M\, .\, \underbrace{(c_1)^a}_{c_1 = g^k} \cdot x^{-1} \equiv M\, .\, x \cdot x^{-1} \equiv M \pmod p$$

Agora basta que Joãozinho consulte a tabela ASCII para obter a mensagem original.

Exemplo 3.13: Joãozinho usa o primo $p = 467$, a raiz primitiva $g = 2$, escolhe $a = 153$ para ser sua **chave privada secreta** e calcula sua chave pública

$$A \equiv g^a \equiv 2^{153} \equiv 224 \pmod{467}$$

Serginho decide enviar para Joãozinho a mensagem $M = 331$(Essa mensagem é um exemplo meramente numérico, não tendo nenhuma relação com a tabela ASCII). Ele escolhe uma chave efêmera ao acaso, digamos $k = 197$ e calcula os dois números a seguir:

$$c_1 \equiv 2^{197} \equiv 87 \pmod{467} \qquad \text{e} \qquad c_2 \equiv 331 \,.\, 224^{197} \equiv 57 \pmod{467}$$

Serginho envia a mensagem criptografada em par $(c_1, c_2) = (87, 57)$ para Joãozinho.

Joãozinho, utilizando sua chave secreta $a = 153$, faz os seguintes passos

Passo 1: Calcula $x \equiv c_1^a \equiv 87^{153} \equiv 367 \pmod{467}$

Passo 2: Calcula $x^{p-2} \equiv 367^{465} \equiv 14 \equiv x^{-1} \pmod{467}$

Passo 3: Calcula $c_2\, x^{-1} \equiv 57\,.14 \equiv 331 \equiv M \pmod{467}$

e assim decodifica a mensagem $M = 331$ enviada por Serginho.

Em 1985, Taher ElGamal publicou um artigo intitulado

A Criptografia de chave pública e um esquema de assinatura com base em logaritmos discretos.

CAPITULO 4

Em virtude da proliferação dos meios de comunicação e da necessidade de enviar numerosas mensagens, tornou-se muito desejável desenvolver métodos de codificação de mensagens. No passado os códigos eram secretos, apenas pelos que enviavam e recebiam as mensagens, mas havia sempre a possibilidade de estudar mensagens interceptadas e decodificá-las.

Um grande progresso foi realizado em criptografia com o aparecimento dos criptosistemas de chave publica. As principais características desse sistema são a sua simplicidade, sua chave publica e extrema dificuldade em violar o código.

A ideia foi proposta em 1976 por Diffie e Hellman e sua efetiva execução foi conseguida por Rivest, Shamir e Adleman, onde este criptosistema é conhecido como RSA que iremos descrevê-lo. Cada letra ou sinal, ai incluído o espaço em branco, corresponde a um número de três algarismos. No *American Standard Code for Information Interchange (ASCII), isto é,* "No Código Americano Padrão para Intercâmbio de Informações", esta correspondência é a seguinte:

...	A	B	C	D	E	F	G	H
032	065	066	067	068	069	070	071	072
I	J	K	L	M	N	O	P	Q
073	074	075	076	077	078	079	080	081
R	S	T	U	V	W	X	Y	Z
082	083	084	085	086	087	088	089	090

Cada letra ou sinal da mensagem é substituído pelo numero de três algarismos que lhe corresponde produzindo assim um numero M, que representa a mensagem. Cada usuário A do sistema inscreve sua chave num fichário publico, e a mesma é um par de inteiros (n_A, s_A) positivos. O primeiro inteiro n_A é o produto de dois números primos distintos p_A, q_A, isto é, $n_A = p_A \,.\, q_A$ que são muito grande e conservados secretos. Por outro lado, s_A é escolhido bem grande de tal forma que seja primo com $p_A - 1$ e $q_A - 1$, cuja motivação será explicada no decorrer do capitulo.

Para enviar a mensagem M a outro usuário B, A codifica M - a maneira de codificar depende da pessoa que receberá a mensagem. Recebendo a mensagem codificada de A, o usuário B a decodifica, utilizando seu numero secreto próprio de decodificação, e este processo será exibido em detalhes no decorrer do texto.

4.1 Fórmula de Euler e raízes módulo pq

O método de troca de chaves Diffie-Hellman e do sistema de criptografia ElGamal de chave pública estudada no capitulo anterior, contam com o fato de que é fácil de calcular potências $a^n \ (mod\ p)$, mas é difícil recuperar o expoente conhecendo apenas os valores de $a \ (mod\ p)$ e $a^n (mod\ p)$. Um resultado essencial que usamos para analisar a segurança de Diffie-Hellman e ElGamal é o Pequeno Teorema de Fermat visto no capitulo anterior

$$a^{p-1} \equiv 1 \ (mod\ p) \quad \forall \ \ a \neq kp \ \ com\ k \in \mathbb{Z}$$

Uma pergunta natural que surge, é o que acontece se substituirmos p por um número m não primo, isto é, será que o resultado $a^{m-1} \equiv 1 \ (mod\ m)$ é válido em geral. Vemos facilmente que o resultado não vale em geral, pois se tomarmos $a = 3$ e $m = 10$ vemos que $a^9 = \ 3^{10-1} \equiv 3 \ (mod\ 10)$.

Nesta seção apresentaremos uma generalização do Pequeno Teorema de Fermat quando $m \ = \ pq$ é um produto de dois números primos distintos, uma vez que este é o caso mais relevante para aplicações em criptografia. Façamos um exemplo para clarearmos as ideias, onde $m \ = \ 3.5 \ = \ 15$. Se fizermos uma tabela de quadrados e cubos módulo 15, eles não parecem muito interessantes, mas muitas quarta potências são iguais a 1 módulo 15. Mais precisamente, temos que

- $a \ \equiv 1 \ (mod\ 15)$ para $a \ = \ 1, 2, 4, 7, 8, 11, 13\ e\ 14$;
- $a^4 \not\equiv \ 1 \ (mod\ 15)$ para $a \ = \ 3, 5, 6, 9, 10\ e\ 12$.

O que distingue a lista de números $1, 2, 4, 7, 8, 11, 13, 14$, cujo quarta potência é **igual** a 1 módulo 15 da lista de números $3, 5, 6, 9, 10, 12, 15$, cujo quarta é **diferente** de 1 modulo 15? Um momento de reflexão mostra que cada um dos números

$3, 5, 6, 9, 10, 12, 15$ tem um fator não trivial em comum com o módulo 15, enquanto que os números $1, 2, 4, 7, 8, 11, 13, 14$ são relativamente primos a 15. Isto sugere que alguma versão do Pequeno Teorema de Fermat deve ser válida se o número a é relativamente primo ao "m", mas certamente o expoente correto não é $(m - 1)$.

Para $m = 15$ descobrimos que o expoente correto é 4. Para vermos isso, observamos que $a^2 \equiv 1\ (mod\ 3) \Rightarrow a^4 \equiv 1\ (mod\ 3)$ e $a^4 \equiv 1\ (mod\ 5)$ ambas como conseqüência do *PTF*. Assim 3 divide $(a^4 - 1)$ e 5 divide $(a^4 - 1)$, logo 15 divide $(a^4 - 1)$, isto é, $a^4 \equiv 1\ (mod\ 15)$.

Se você pensar sobre essas duas congruências, verá que a propriedade fundamental do expoente 4 é que ele é um múltiplo de $(p - 1)$ para $p = 3$ e $p = 5$. Note-se que isto não é verdade para $m - 1 = 14$ como um expoente. Com essa observação, estamos prontos para a fórmula fundamental do sistema de criptografia de chave pública RSA.

Proposição 4.1: (Fórmula de Euler para pq). Sejam p e q números primos distintos e se $g = mdc\ (p - 1, q - 1)$, então

$$a^{(p-1).(q-1)/g} \equiv 1\ \ (mod\ pq)\ \ tal\ que\ \ \ mdc(a, pq) = 1$$

Em particular, se p e q são primos ímpares, então

$$a^{(p-1).(q-1)/2} \equiv 1\ \ (mod\ pq)\ \ tal\ que\ \ \ mdc(a, pq) = 1$$

Prova: como

- $mdc(a, pq) = 1 \Rightarrow p\ não\ divide\ a.$
- $g = mdc(p - 1, q - 1) \Rightarrow g\ divide\ (q - 1).$

Então

$a^{(p-1).(q-1)/g} = (a^{p-1})^{\frac{(q-1)}{g}}$ visto que g divide $(q - 1)$

$\equiv (1)^{\frac{(q-1)}{g}}\ (mod\ p)$ visto que $a^{p-1} \equiv 1\ (mod\ p)$ do PTF

$\equiv 1\ \ (mod\ p)$

O mesmo cálculo, invertendo os papéis de p e q, mostra que

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

Isto mostra que $a^{(p-1).(q-1)/g} - 1$ é divisível por p e q, e portanto é divisível por pq, o que completa a prova da proposição. ■

O método de troca de chaves Diffie-Hellman e do sistema de criptografia ElGamal de chave pública estudada no capítulo anterior, dependem para a sua segurança da dificuldade de resolver equações da forma

$$a^x \equiv b\ (mod\ p)$$

onde a, b e p são variáveis conhecidas, p é um número primo e "x" é a variável desconhecida. O criptosistema de chave pública RSA baseia-se na dificuldade de resolver equações da forma

$$x^k \equiv c\ (mod\ N)$$

onde agora as variáveis k, c e N são conhecidas e a variável x é desconhecida. Em outras palavras, a segurança do RSA baseia-se no pressuposto que é difícil tomar k-ésimas raízes módulo N.

Lema 4.2. Sejam a, m inteiros com $m \geq 1$. Então

$$a.d \equiv 1\ (mod\ m)\ \ para\ algum\ \ d \in \mathbb{Z} \quad \Leftrightarrow \quad mdc\ (a, m) = 1$$

Prova:

$(\Leftarrow)\ \ mdc\ (a.m) = 1 \ \Rightarrow \ \exists\ d, c \in \mathbb{Z}\ ;\ ad + mc = 1$

$$\Rightarrow\ ad - 1 = -c.m$$

$$\Rightarrow\ ad \equiv 1\ (mod\ m)$$

$(\Rightarrow)\ a.d \equiv 1\ (mod\ m) \Rightarrow ad - 1 = cm$ para algum $c \in \mathbb{Z}$

$$\Rightarrow\ ad - cm = 1$$

$$\Rightarrow\ mdc\ (a,m)\ divide\ 1$$

$$\Rightarrow\ mdc\ (a,m) = 1.\ \blacksquare$$

Proposição 4.3: Seja p um primo e $k \geq 1$ um inteiro satisfazendo $mdc\ (k,p-1) = 1$. Então

$$x^k \equiv c\ (mod\ p)\ \text{têm a única solução}\ x \equiv c^d\ (mod\ p)$$

Onde d é o inverso de k módulo $(p-1)$.

Prova: Se $c \equiv 0\ mod\ p$ então $x \equiv 0\ (mod\ p)$ é a única solução e acabou. Assuma que $c \not\equiv 0\ (mod\ p)$. Como $mdc\ (k,p-1) = 1$ segue do Lema 4.2 que $dk \equiv 1\ (mod\ p-1)$ o que significa que

$$dk \equiv 1 + r(p-1)$$

Vamos agora checar que $x = c^d$ é uma solução para $x^k \equiv c\ (mod\ p)$.

$(c^d)^k \equiv c^{dk}\ \ (mod\ p)$

$\equiv c^{1+k(p-1)}\ \ (mod\ p)$ visto que $dk = 1 + r(p-1)$

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

$\equiv c\ .1^k\ \ (mod\ p)$ pelo *PTF*

$\equiv c\ \ (mod\ p)$

Para mostar a unicidade, suponha que x_1 e x_2 são soluções da congruência $x^k \equiv c\ (mod\ p)$.Acabamos de mostrar que $z^{dk} \equiv z\ (mod\ p)$ para qualquer valor não nulo "z", então temos que

$$x_1 \equiv x_1^{dk} \equiv \left(x_1^k\right)^d \equiv c^d \equiv \left(x_2^k\right)^d \equiv x_2^{kd} \equiv x_2\ (mod\ p)$$

Assim x_1 e x_2 são iguais módulo p, de modo que $x^k \equiv c\ (mod\ p)$, tem no máximo uma solução. $\blacksquare$

Exemplo: Resolvendo a congruência para $k = 1583, c = 4714$ $e\ N = p = 7919$

$$x^k = x^{1583} \equiv 4714\ (mod\ 7919)$$

onde o módulo p = 7919 é primo. Resolvendo a congruência através do algoritmo Euclidiano Extendido

$$1583\ d \equiv 1\ (mod\ 7918) \quad \Rightarrow \quad d \equiv 5277\ (mod\ 7918)$$

e segue do Lema 4.2 que $mdc\ (d, p-1) = 1$. Pela proposição 4.3 segue que

$$x \equiv c^d \equiv 4714^{5277} \equiv 6059\ (mod\ 7919)$$

é uma solução para $x^k = x^{1583} \equiv 4714\ (mod\ 7919)$. ■

A proposição 4.3 mostra que é fácil calcular a k-ésima raiz se o módulo é um primo p. A proposição seguinte explica com fazer isso se $N = pq$ é um produto de dois números primos

Proposição 4.4: Seja p e q primos distintos e seja $k \geq 1$ tal que

$$mdc\ (k, (p-1).(q-1)) = 1$$

Então a congruência

$$x^k \equiv c\ (mod\ pq)\ \text{tem a única solução}\ x \equiv c^d\ (mod\ pq)$$

Onde d é o inverso de k módulo $(p-1).(q-1)$.

Prova: Assuma que o $mdc\ (c, pq) = 1$. Como $mdc\ (k, (p-1).(q-1)) = 1$ segue do Lema 4.2 que k tem inverso módulo $(p-1).(q-1)$, isto é, existe $d \in \mathbb{Z}$ tal que

$$d.k \equiv 1\ (mod\ (p-1).(q-1)\ )$$

Isto significa que existe um inteiro r tal que

$$d.k = 1 + r(p-1).(q-1)$$

Agora iremos checar que $x = c^d$ é uma solução para $x^k \equiv c\ (mod\ pq)$

$(c^d)^k \equiv c^{dk}\ \ (mod\ \ pq)$

$\equiv c^{1+k(p-1)(q-1)}\ \ (mod\ pq)$ visto que $dk = 1 + r(p-1)(q-1)$

$\equiv c^1 . \left(c^{(p-1).(q-1)}\right)^k \ (mod\ pq)$

$\equiv c . 1^k \ (mod\ pq)$ pela Fórmula de Euler para pq

$\equiv c \quad (mod\ pq)$

Para mostar a unicidade, suponha que $x = u$ é uma solução da congruência $x^k \equiv c\ (mod\ pq)$. Então

$u \equiv u^{dk-r(p-1)(k-1)}\ (mod\ pq)$ visto que $dk = 1 + r(p-1).(q-1)$

$\equiv (u^k)^d . \left(u^{(p-1)(q-1)}\right)^{-r} (mod\ pq)$

$\equiv (u^k)^d . 1^{-r} \ (mod\ pq)$ usando a Fórmula de Euler para pq

$\equiv c^d \ (mod\ pq)$ visto que u é solução de $x^k \equiv c\ (mod\ pq)$.

Queremos mostrar que $c^{k.d} \equiv c \bmod n$ Por definição de d, temos que $k.d \equiv 1 \bmod (p-1).(q-1)$ $k.d = 1 + r.(p-1).(q-1)$ Queremos calcular separados $c^{kd} \bmod p$ caso 1 $c^{kd} \bmod q$ caso 2 <u>Fazendo o caso 1:</u> $c^{kd} \equiv c^1[b^{p-1}]^{r.(q-1)} \bmod p$ Se $p \nmid c \Rightarrow c^{p-1} \equiv 1 \bmod p$ (PTF) $\Rightarrow c^{kd} \equiv c.1^{r.(q-1)} \equiv b \bmod p$ Se $p \mid c \Rightarrow c^{kd} \equiv 0 \bmod p$ $\Rightarrow c \equiv 0 \bmod p$ $\Rightarrow c^{kd} \equiv c \bmod p$ $\Rightarrow y = 0 + k.p$ $\Rightarrow w = c + q\ .(k.p)$ $\Rightarrow w = c + k.(q.p)$ $\Rightarrow w \equiv c\ mod\ (p.q)$	Logo em qualquer caso $c^{kd} \equiv c \bmod p$ De maneira análoga provamos o caso 2 Sendo assim temos: $S=\begin{cases} c^{k.d} \equiv c \bmod p \\ c^{k.d} \equiv c \bmod q \end{cases}$ Observe que b é uma solução de $\begin{cases} w \equiv c \bmod p \quad (1) \\ w \equiv c \bmod q \quad (2) \end{cases}$ Segue de (2) $\Rightarrow w \equiv c\ mod\ p$ $\Rightarrow w - c = q.y$ $\Rightarrow w = c + q.y$ De (1) $\Rightarrow c + q.y \equiv c\ mod\ p$ $\Rightarrow q.y \equiv 0\ mod\ p$ $\Rightarrow \bar{q}.\bar{y} = \bar{0}$ solução geral Como $c^{k.d}$ também é solução de S Temos que $c^{k.d} = c + (p.q)r$ $\Rightarrow c^{k.d} \equiv c\ mod\ pq$ $\Rightarrow (c^d)^k \equiv c\ mod\ n.$

$\Rightarrow w \equiv c \, mod \, n$ $\Rightarrow$ w = c + t.(p.q) com t $\in \mathbb{Z}$ é a	$\Rightarrow x^k \equiv c \, mod \, n.$ ■

Exemplo 4.6: Vamos resolver a congruência

$$x^k = x^{17389} \equiv 43927 \, (mod \, 64349)$$

Onde o modulo $N = 64349 = 229.281$ é o produto de dois primos $p = 229$ e $q = 281$ e $k = 17389$. O primeiro passo é resolver a congruência

$$k \, d = 17389 \, d \equiv 1 \, mod \, 63840$$

Onde $(p-1).(q-1) = 228 \, . 280 = 63840$. Vemos que

$$d \equiv 53509 \, (mod \, 63840).$$

Então a proposição 4.4 nos diz que

$$x \equiv c^d = 43927^{53509} \equiv 14458 \, (mod \, 64349)$$

é solução para $x^k = x^{17389} \equiv 43927 \, (mod \, 64349)$.

Exemplo 4.7: Serginho desafia Joãozinho para resolver a congruência

$$x^k = x^{9843} \equiv 134872 \, (mod \, 30069476293)$$

O módulo $N = 30069476293$ é um produto de dois números primos, mas se Joãozinho não conhece sua fatoração, ele não pode usar a Proposição 4.4 para resolver o desafio do Serginho. Depois de aceitar a concessão da derrota de Joãozinho, Serginho informa a Joãozinho que $N = 30069476293 = 104729 \, . 287117 = p.q$. Com esta nova informação, o desafio de Serginho se torna muito mais fácil. Joãozinho calcula $(p-1).(q-1) = 104728 \, . 287116 = 3006908448$ e resolve a congruência

$$kd = 9843 \, d \equiv 1 \, (mod \, 30069084448)$$

Para encontrar $b \equiv 18472798299 \, (mod \, 30069084448)$ e calcular a solução

$$x = c^d \equiv 134872^{18472798299} \equiv 25470280263 \, (mod \, 30069476293).■$$

Serginho e Joãozinho sempre trocam informações confidenciais através de um canal de comunicação inseguro e temem que Mônica possa interceptar estas mensagens. Vimos no capítulo 3 várias maneiras em que Serginho e Joãozinho possam realizar essa tarefa, com base na dificuldade de resolver o Problema do Logaritmo Discreto, e na próxima seção iremos descrever o criptosistema de chave publica RSA.

4. 2 O Sistema de Criptografia RSA

Em 1976, Whitfield Diffie e Martin Hellman escreveram um documento chamado "As novas direções da criptografia" mostrando a ideia de usar criptografia de chaves publicas. Vários especialistas tentaram desenvolver um algoritmo que pudessem atender as especificações propostas por Diffie-Hellman.

O RSA foi desenvolvido em 1978 em resposta a essa necessidade no MIT, por Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman (daí a sigla RSA). O algoritmo do RSA foi o primeiro algoritmo de chaves publicas e vem sendo amplamente usado desde então.

O RSA é basicamente o resultado de dois cálculos matemáticos. Um para cifrar e outro para decifrar. O RSA usa duas chaves criptográficas, uma chave pública e uma privada. No caso da criptografia assimétrica tradicional, a chave pública é usada para codificar a mensagem e a chave privada é usada para decodificar a mensagem.

A segurança desse método se baseia na dificuldade da fatoração de números inteiros extensos. Em 1977, os criadores do RSA achavam que uma chave de 200 bits requereriam 1015 anos, porém chaves com 155 bits foram atacadas em menos de 8 meses. A saída é que na medida em que os algoritmos se tornem melhores e os computadores se tornem mais velozes, maiores serão as chaves. Atualmente chaves com 300 dígitos (1000 bits) nos dão uma tranquilidade por algum tempo. Em níveis críticos, chaves com 2000 bits começam a ser usadas.

O criptosistema de chave publica RSA é resumido na tabela abaixo entre Joãozinho e Serginho.

Joãozinho	Serginho
Criação da chave	
• Escolha dos primos secretos p e q • Escolha do expoente de criptografia k de modo que o $mdc\ (k, (p-1)(q-1)\ ) = 1$ • Chave Publica $(N = pq,\ k)$	
Codificando a Mensagem	
	• Escolhe a mensagem M • Usa a chave pública de Joãozinho para calcular $c \equiv M^k\ (mod\ N)$ • Enviar mensagem codificada c para Joãozinho.
Decodificando a Mensagem	
• Calcula d onde $kd \equiv 1\ (mod(p-1)(q-1))$ • Calcula $c^d \equiv \widetilde{M}\ (mod\ N)$ • Então $\widetilde{M}$ é igual a mensagem M	

Tabela RSA

A chave secreta do Joãozinho é um par de números primos grandes p e q. A sua chave pública é o par (N, k), que consiste do produto de $N = pq$ e um expoente de criptografia k que é relativamente primo com $(p-1)(q-1)$. Serginho escolhe a mensagem M e a converte através da chave de criptografia k em um inteiro c entre 1 e N com o seguinte cálculo

$$c \equiv M^k\ (mod\ N)$$

O inteiro c é a mensagem de Serginho codificada, que cascão envia para Joãozinho. Para decodificar a mensagem, Joãozinho resolve a congruência $x^k \equiv c\ (mod\ N)$ usando a Proposição 4.4, pois conhece a fatoração de $N = pq$. Mônica, por outro lado, pode interceptar a mensagem codificada c de Serginho, mas como não conhece os

fatores de N, ela terá muita dificuldade em resolver a congruência $x^k \equiv c\ (mod\ N)$ para decodificar a mensagem c em tempo hábil.

Exemplo 4.8: Ilustraremos o sistema de criptografia de chave pública RSA com um pequeno exemplo numérico. É claro que este exemplo não é seguro, já que para números pequenos, seria fácil para Mônica encontrar os fatores p e q de N. Implementações seguras de uso do criptosistema RSA módulo N utilizam centenas de dígitos.

Joãozinho	**Serginho**
Criação da chave	
Escolha dos primos secretos $p = 1223$ e $q = 1987$ e $N = p.q$ **Escolha** do expoente de criptografia $k = 948047$ de modo que o $mdc(k, (p-1), (q-1)) = 1$ Chave pública de Joãozinho $(N, k) = (2430101, 948047)$	
Codificando a Mensagem	
	Serginho converte sua mensagem simples em um inteiro $M = 1070777$ tal que $1 \leq M < N$ Serginho usa a chave publica de Joãozinho $(N, k) = (2430101, 948047)$ para calcular $c \equiv M^k\ (mod\ N)$, isto é $c \equiv 1070777^{948047} (mod\ 2430101)$ Resultando que $c \equiv 1473513\ (mod\ 2430101)$ Serginho envia a mensagem codificada $c = 1473513$ para Joãozinho
Decodificando a Mensagem	

Joãozinho conhece $(p-1)(q-1) = 2426892$ e calcula d onde $k\,d = 948047\; d \equiv 1\; mod\; 2426892$ e encontra que $d = 1051235$ Joãozinho decodifica c através do cálculo $c^d \equiv M\ (mod\ N)$ Isto é, $1473513^{1051235} \equiv 1070777\ mod\ N$ O valor encontrado por Joãozinho é a mensagem convertida de Serginho .	

Se p e q são grandes números primos, tendo, pelo menos 100 algarismos e escolhidos ao acaso, a fatoração de n, que tem pelo menos 200 algarismos não pode fazer-se em tempo razoável com os métodos hoje conhecidos. Uma pergunta natural, é como escolher bem os fatores primos do número $N = pq$ e a chave k, de modo que, seja pouco provável que o sistema possa ser violado.

É muito importante para a segurança da mensagem que não se possa fatorar a chave publica. Quantos algarismos devem ter essa chave para que a fatoração exija tempo demasiado para ser aplicável?

Para testar este ponto, várias chaves foram propostas aos matemáticos como um desafio. Assim foi o numero chamado RSA-768, que tem 768 bits de comprimento e 232 algarismos decimais

$RSA - 768 =$

1230 1866 8453 0117 7551 3049 4958 3849 6272 0772 8535 6959 53
3479 2197 3224 5215 1726 4005 0726 3657 5187 4520 2199 7864 69
3899 5647 4942 7740 6384 5925 1925 5732 6303 4537 3154 8268 50
7917 0261 2214 2913 4616 7042 9214 3116 0222 1240 4792 7473 77
9408 0665 3514 1959 7459 8556 6902 1434 13

Este número foi escolhido com muito cuidado em vista de ser uma chave possível para o RSA. O problema foi resolvido em dezembro de 2009 por um grupo internacional que conseguiu determinar os dois fatores primos, cada um com 116 algarismos.

p = 3347 8071 6989 5689 8786 0441 6984 8212 6908 1770 4794 9837 13
7685 6891 2431 3889 8288 3793 8780 0228 7614 7116 5253 1743 08
7737 8144 6799 9489

q = 3674 6043 6667 9959 0428 2446 3379 9627 9526 3227 9158 1643 43
0876 4267 6032 2838 1573 9666 5112 7923 3373 4171 4339 6810 27
0092 7987 3630 8917

O processo utilizado foi o crivo geral do corpo de números GNFS utilizando o software desenvolvido em grande parte na universidade de Bonn. O calculo que durou 20 meses, foi repartido por centenas de PC's; este trabalho exigiria 1.500 anos com um processador de 2,2 GHz.

Por causa da segurança, é necessária muita prudência na escolha de chaves para o processo RSA. Com o progresso dos métodos de fatoração e a codificação de equipes fortes, pode-se imaginar que em menos de uma década, módulos com 1024 bits, que no momento oferecem toda segurança, já poderiam ser fatorados pelo método GNFS. Por esta razão os cientistas recomendam que as chaves com 1024 bits não sejam mais utilizadas a partir das Olimpíadas em 2016.

Faremos agora um exemplo onde a mensagem M a ser transmitida será quebrada em blocos que devem ser números menores do que $N = pq$ pois após a decodificação, queremos obter a mensagem original e não blocos congruentes, e observamos que:

- A maneira de escolher os blocos não é única.
- Os blocos não precisam ter o mesmo tamanho.
- O bloco não pode começar com zero pois não teríamos como distinguir o bloco $0n_1n_2$ do bloco n_1n_2

Usaremos a seguinte notação:

- $b =$ bloco da mensagem M, isto é, um inteiro positivo menor do que $N = pq$.
- $C(b) =$ Codificação do bloco b, definido por $C(b) \equiv b^3 \ (mod\ N)$

- $a =$ bloco codificado, isto é, $a = C(b)$ para algum bloco b
- $D(a)$ = Decodificação do bloco a, definido por $D(a) \equiv a^d \ (mod\ N)$

Se b é um bloco da mensagem original, então só será legitimo chamar o processo de decodificação, se $D(\ C(b)\ ) = b$, e não é obvio que isto é verdade sem conhecer a Proposição 4.4. Primeiramente, mapearemos o alfabeto com números de dois algarismos e indicaremos o espaço por :

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	espaço
23	24	25	26	27	28	29	30	31	32	33	34	35	99

Desta forma a frase “COELHO NA FOGUEIRA” fica representada pelo número

$$M = 122414211724992310991524163014182710.$$

Joãozinho	**Serginho**
Passo 1: Cebolinha escolhe $p = 17$ e $q = 31$ primos secretos, e calcula $N = p.q = 527$ e como $(p-1)(q-1) = 16.30 = 480$ Cebolinha escolhe $k = 41$ onde $mdc\ (k, (p-1)(q-1)) = 1$ e sua chave publica é (N, k)	

	Passo 2: Serginho converte sua mensagem "coelho na fogueira" em um inteiro M e a divide em blocos b tal que $1 \leq b < N$ e não começando por zero, conforme abaixo $122 - 414 - 211 - 72 - 499$ $- 23 - 109 - 91 - 524 - 16$ $- 301 - 418 - 27 - 10$ Serginho usa a chave publica de Joãozinho $(N, k) = (527, 41)$ Para cada bloco b da mensagem M será efetuado o cálculo de codificação. $C(b) \equiv b^k \ (mod\ N)$
Joãozinho	**Serginho**
	$C(122) - C(414) - C(211) - C(72)$ $- C(499) - \mathbf{C(23)} - C(109) - C(91)$ $- C(524) - C(16) - C(301)$ $- C(418) - C(27) - C(10)$ Por exemplo: $C(23) = 23^{41} \ (mod\ 527)$ $23^2 = 529 \equiv 2 \ (mod\ 527) \Rightarrow$ $23^{20} = (23^2)^{10} \equiv -30 \ (mod\ 527) \Rightarrow$ $23^{40} = 900 \equiv 373 \ (mod\ 527) \Rightarrow$ $23^{41} \equiv 373 \,.\, 23 \equiv 147 \ (mod\ 527)$ Logo $C(23) = 147$, analogamente $184 - 334 - 129 - 174 - 385$ $-\mathbf{147} - 78 - 215 - 173 - 16$ $-449 - 58 - 143.$ Serginho envia M em blocos codificado.

Passo 3: Joãozinho malandro, calcula d

$$k\,d\ =\ 41\,d \equiv 1\ (mod\ 480)$$

e encontra que

$$d\ = 281$$

Para cada bloco da mensagem, Joãozinho decodifica $a = C(b)$ através do cálculo

$$D(a)\ \equiv a^d\ (mod\ N)$$

Decodificando $a = C(b)\ =\ 147$

usando o método de expansão binária

$$D(147) \equiv 147^{281}\ \ (mod\ 527)$$

Joãozinho	Serginho

De fato, usando o método de expansão binária do capítulo 3

$$281\ =\ 2^8\ +\ 2^4\ +\ 2^3\ +\ 1$$

$$147^{281}\ = 147^{2^8}.147^{2^4}.147^{2^3}.147^{1}$$

Segue que

i	0	1	2	3
$147^{2^i}\ (mod 527)$	147	2	4	16

i	5	6	7	8
$147^{2^i}\ (mod 527)$	188	35	171	256

Portanto

$$\boldsymbol{D(147)} \equiv\ 147^{281} = 256.256.16.147\ \equiv \mathbf{23}\ (mod\ 257)$$

Desta forma, Joãozinho recupera o inteiro M de Serginho

$$122 - 414 - 211 - 72 - 499 -\ 23 - 109 -$$

$$91 - 524\ - 16 -\ 301 - 418 - 27 - 10$$

Joãozinho finalmente converte a informação numérica M através do alfabeto obtendo:

"COELHO NA FOGUEIRA"

e abre um sorriso no rosto.

Faremos agora um caso particular do criptosistema RSA onde os parâmetros secretos p e q são primos distintos satisfazendo $p \equiv 5\,(mod\ 6)$ e $q \equiv 5\,(mod\ 6)$. A motivação desta escolha de p e q garante que 3 é inversível módulo $(p-1)(q-1)$ e a chave de codificação pública poderá ser $(N, 3)$.

Primeiro vamos determinar explicitamente o inverso de $3\ mod\ (p-1)(q-1)$ que será denotado por d. Como $p \equiv 5\,(mod\ 6)$, $q \equiv 5\,(mod\ 6)$ e $-1 \equiv -1\,(mod\ 6)$, segue que $(p-1) \equiv 4\,(mod\ 6)$ e $(q-1) \equiv 4\,(mod\ 6)$. Assim $(p-1)(q-1) \equiv -2\,(mod\ 6)$, e portanto $(p-1)(q-1) = 6k-2$. Como d é o inverso de $3\ mod\ (p-1)(q-1)$, temos que $3d \equiv 1\ \big(mod\ (p-1)(q-1)\big)$, logo $3d \equiv 1\ \big(mod\ (6k-2)\big)$ e assim, $3d = (6k-2)t + 1$ para algum t$\in \mathbb{Z}$. Já vimos que podemos calcular o inverso de um número módulo $(p-1)(q-1)$ através da extensão do algoritmo euclidiano, mas tomando $d = 4k-1$ segue que $3d = 3\,(4k-1) = 12k-3 = (6k-2).2 + 1$, onde $k = \frac{1}{6}\,[\,(p-1)(q-1)+2]$.

Joãozinho	**Serginho**
Passo 1: Joãozinho escolhe como primos $\equiv 5\,(mod\ 6)$ secretos $p = 17$ e $q = 23$. Logo $N = p.q = 391$ e toma como chave pública $(N, 3) = (391,3)$	
	Passo 2: Serginho converte sua mensagem "AMO A OBMEP" em um inteiro M $102224991099241122 1425$ e a divide em blocos b tal que $1 \leq b < N$ e não começando por zero, conforme abaixo $102 - 224 - 99 - 109 - 92 - 41 - 122 - 142 - 5$ Serginho usa a chave publica de Joãozinho $(N, 3) = (391, 3)$ Para cada bloco b da mensagem M será efetuado o cálculo de codificação. $C(b) \equiv b^3\ (mod\ N)$

Joãozinho	Serginho
	Como $C(b) \equiv b^3 \ (mod\ N)$ temos $34 - 129 - 228 - 37 - 207 -$ $105 - 44 - 386 - 125$ Serginho envia a mensagem codificada em blocos
Passo 3: Joãozinho usando sua malandragem de sempre sabe que $k = \frac{1}{6}[\,(p-1).(q-1)+2]$ $= \frac{1}{6}\,[16.22+2] = 59$ Portanto $d = 4k - 1 = 4.59 - 1 = 235$ Para cada bloco da mensagem, Joãozinho decodifica $a = C(b)$ através do cálculo $D(a) \equiv a^d \ (mod\ N)$ Decodificando, Joãozinho recupera o inteiro M de Serginho 1022249910992411221425 e converte esta informação numérica usando o alfabeto obtendo AMO A OBMEP	

4.3 A SEGURANÇA DO MÉTODO RSA

Note que determinar a chave privada de decodificação d não seria uma tarefa fácil sem conhecer o valor de $(p-1)(q-1)$. Por isso deve ser guardado de forma segura os valores dos primos p e q. Como já vimos, não existe um método eficiente para se fatorar números grandes, e um ponto muito importante, se refere à escolha dos primos p e q. É claro que se forem pequenos, o sistema será mais fácil de quebrar. Mas também não basta escolher p e q grandes com $|p-q|$ pequeno, devido ao **Algoritmo de Fermat** descrito a seguir. Contudo, precisamos ter certeza que os números $(p-1), (q-1)$, $(p+1)$ e $(q+1)$ não tem fatores primos pequenos, pois caso contrário, faria de $N = pq$ uma presa fácil para alguns algoritmos de fatoração conhecidos. Embora isso pareça muito simples em princípio, na prática é totalmente inviável. A razão é que não existem computadores rápidos o suficiente, nem algoritmos eficientes, que nos permitam fatorar um número inteiro muito grande que não tenha fatores relativamente pequenos.

Na verdade, não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente, não se sabe nem mesmo se é possível que esse algoritmo exista.

O Algoritmo de Fermat

Este exemplo está vinculado à necessidade de Fermat encontrar um processo para fatorar números relativamente grandes, para a época é claro, ou mostrar sua primalidade. Fermat desenvolveu dois algoritmos. Um para fatorar um número inteiro qualquer e outro específico para números de Mersenne. Estes resultados mostram o seu engenho na manipulação dos números. Segundo Coutinho (Coutinho, 2001 p. 40 e 157), o primeiro método consistia em fatorar um número utilizando um algoritmo mais ou menos como o descrito a seguir.

Para começar suporemos que N é ímpar, já que se N for par então 2 é um de seus fatores. A ideia do algoritmo é tentar achar números inteiros positivos x e y tais que N= $x^2 - y^2$. Supondo que encontramos estes números temos que

$$N = x^2 - y^2 = (x - y)(x + y)$$

Logo $(x - y)$ e $(x + y)$ são fatores de N.

Para poder aplicar o Algoritmo de Fermat, assumiremos que já temos em nosso computador um algoritmo para determinar a raiz quadrada de N. Na verdade é suficiente obter a parte inteira da raiz quadrada de N. Se r é um número real, denotaremos sua parte inteira por $[r]$. Por exemplo, $[\sqrt{125}] = 11$ e $[\pi] = 3$. É claro que se r é inteiro então $[r] = r$.

O caso mais fácil do algoritmo de Fermat ocorre quando N é um quadrado perfeito, isto é, quando existe algum inteiro r tal que $N = r^2$. Neste caso, temos que r é fator de N. Além disso, na notação acima, $x = r$ e $y = 0$. Observe que se $y > 0$ então

$$N = x^2 - y^2 \Rightarrow x = \sqrt{N + y^2} > \sqrt{N}$$

Isto sugere a seguinte estratégia para encontrar x e y

Algoritmo de Fermat

Entrada: inteiro positivo ímpar N

Saída: um fator de N ou uma mensagem indicando que N é primo

Etapa 1: Comece com $x = [\sqrt{N}]$, se $N = x^2$ então x é fator de N e paramos.

Etapa 2: Caso contrário, incremente x de uma unidade e calculamos

$$y = \sqrt{x^2 - N}$$

Etapa 3: Repita a Etapa 2 ate

- Encontrar um valor inteiro para y e assim $N = (x + y)(x - y)$
- Até que x seja igual $\frac{n+1}{2}$ e neste caso N é primo

O funcionamento do Algoritmo de Fermat ficará mais claro se fizermos um exemplo numérico. Seja $N = 1342127$ o número que queremos fatorar. A variável x inicializada com a parte inteira da raiz quadrada de N, que neste caso vale $x = 1158$. Mas

$$x^2 = 1158^2 = 1340964 < N = 1342127$$

Logo passamos a incrementar x de um em um. Fazemos isto até que

$$\sqrt{x^2 - N}$$

Seja inteiro, ou x seja igual a $(n + 1)/2$, que neste caso vale 671064. É mais fácil resumir isto em uma tabela

x	$y = \sqrt{x^2 - N}$
1159	33,97
1160	58,93
1161	76,11
1162	90,09
1163	102,18
1164	113

Obtivemos assim, um inteiro no sexto laço. Portanto $x = 1164$ e $y = 113$ são os valores desejados. Os fatores correspondentes são $x + y = 1277$ e $x - y = 1051$.

Prova do Algoritmo de Fermat:

Não é de modo algum claro porque o algoritmo de Fermat funciona, nem porque pára. Observe que é necessário considerar separadamente o que ocorre quando N é composto e quando N é primo.

No primeiro caso precisamos mostrar que existe um inteiro $x > [\sqrt{N}]$ tal que $y = \sqrt{x^2 - N}$é um inteiro menor que $\frac{N+1}{2}$. Isto significa que se N é composto então o algoritmo para antes de chegar a $\frac{N+1}{2}$. Se N é primo, então é necessário verificar que o único valor de x possível é $\frac{N+1}{2}$.

Suponhamos que N pode ser fatorado na forma $N = ab$ onde $a \leq b$. Queremos obter inteiros positivos x e y tais que $N = x^2 - y^2$. Em outras palavras

$$N = ab = (x-y)(x+y) = x^2 - y^2$$

Como $x - y \leq x + y$, isto sugere que tomemos $a = x - y$ e $b = x + y$. Resolvendo este sistema de duas equações em duas incógnitas obtemos

$$x = \frac{a+b}{2} \qquad e \qquad y = \frac{b-a}{2}$$

De fato, expandindo os produtos notáveis verificamos facilmente que

$$\left(\frac{b+a}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2 = ab = N \qquad (*)$$

Note que x e y tem que ser números inteiros, mas $(b+a)/2$ e $(b-a)/2$ estão escritos na forma de fração. Porém N é ímpar por hipótese, logo a e b, que são fatores de N tem que ser ímpares. Portanto $(b+a)$ e $(b-a)$ são pares e consequentemente $(b+a)/2$ e $(b-a)/2$ são inteiros. É por isso que precisamos sempre supor que a entrada do algoritmo é sempre um número ímpar.

Se N é primo então só podemos ter $a = 1$ e $b = N$. Com isto $x = (n+1)/2$ e este é o único valor possível para x se N é primo. Resta nos considerar o caso em que N é composto. Se $a = b$, o algoritmo já obtém a resposta desejada já na Etapa 1. Podemos então, supor que N é composto e não é um quadrado perfeito, isto é, $1 < a < b < N$. Vejamos que, neste caso, o algoritmo vai parar se forem satisfeitas as desigualdades

$$\left[\sqrt{N}\right] \leq \frac{a+b}{2} < \frac{n+1}{2} \qquad (**)$$

que provaremos a seguir.

A desigualdade da direita nos diz que $a + b < n + 1$. Substituindo $N = ab$ nesta ultima desigualdade e subtraindo $b + 1$ de ambos os membros obtemos $a - 1 < ab - b = (a-1)b$. Já que $a > 1$, podemos ainda cancelar $(a-1)$ de ambos os membros. Fazendo isso obtemos $1 < b$. Este argumento mostra que $1 < b$ é

equivalente a desigualdade original. Como $1 < a < b$ vale por hipótese provamos que $\frac{a+b}{2} < \frac{N+1}{2}$.

Consideremos agora a desigualdade da esquerda. Observemos primeiro que como $\lceil\sqrt{N}\rceil \leq \sqrt{N}$, basta verificar que $\sqrt{N} \leq \frac{(a+b)}{2}$. Esta desigualdade é verdadeira se e somente se $N \leq \frac{(a+b)^2}{4}$. Mas por $(*)$ segue que

$$\left(\frac{b+a}{2}\right)^2 - N = \left(\frac{b-a}{2}\right)^2$$

que é sempre um numero não negativo. Obtivemos assim que $\frac{(a+b)^2}{4} - N \geq 0$. O que é equivalente a desigualdade desejada.

Voltemos ao algoritmo de Fermat. Lembre que a variável x é inicializada com o valor $\lceil\sqrt{N}\rceil$ e que vai sendo incrementado de uma unidade a cada laço. Assim $(**)$ nos garante que , se N for composto, chegaremos a $(a+b)/2$ antes de chegar a $(n+1)/2$. Quando $x = (a+b)/2$

$$y^2 = \left(\frac{a+b}{2}\right)^2 - N = \left(\frac{b-a}{2}\right)^2$$

Pela identidade $(*)$. Atingindo este laço, o algoritmo pára, obtendo a e b como fatores. Portanto, se N é composto, o algoritmo sempre pára antes de chegar a $x = (n+1)/2$, tendo determinado fatores de N. ■

Este algoritmo nos diz uma coisa muito importante sobre o RSA. Lembre-se que a segurança do RSA depende da dificuldade de fatorar a chave publica N, que é igual ao produto de dois primos. A primeira impressão é que basta escolher os primos grandes, para que N é difícil de fatorar. Mas isto não é verdade. Por exemplo, se escolhermos primos grandes, mais próximos, então N é facilmente fatorável pelo algoritmo de Fermat.

CAPÍTULO 5

Nesse capítulo iremos propor atividades relativas aos conteúdos abordados

5.1 Atividades

1- Vamos criptografar a palavra MATEMATICA utilizando a palavra chave RSA

2- Com o auxilio de uma calculadora e utilizando o algoritmo de Fermat vamos decompor os números:

   a) 352717
   b) 799811
   c) 99400891
   d) 4087

3- Vamos criptografar a palavra COPA DO MUNDO dados n= 517 e $e = 3$

4- Vamos decodificar a mensagem encontrada na atividade um.

5- Tente decodificar a mensagem encontrada na atividade três.

5.2 Respostas das Tarefas

1)

M	A	T	E	M	A	T	I	C	A	ORIGINAL
12	26	19	4	12	26	19	8	2	26	
R	S	A	R	S	A	R	S	A	R	CHAVE
17	18	26	17	18	26	17	18	26	17	
29	34	45	21	30	52	36	26	28	43	SOMA
D	S	T	V	E	A	K	A	C	R	CODIFICADA

2) Fatores (x + y) e (x – y)

a) n = 352717

It	x	y = $\sqrt{x^2 - n}$
1	594	10.908712
2	595	36.166283
3	596	49.989999
4	597	60.761830
5	598	69.907081
6	599	78.000000

y = 78.000000 é inteiro, logo 352717 tem fatores 521 e 677.

b) n = 799811

It	x	y = $\sqrt{x^2 - n}$
1	895	34.842503
2	896	54.817880
3	897	69.267597
4	898	81.197291
5	899	91.596943
6	900	100.940577
7	901	109.498858
8	902	117.443603
9	903	124.891953
10	904	131.928011
11	905	138.614574
12	906	145.000000

y = 145.000000 é inteiro, logo 799811 tem fatores 761 e 1051.

c) n = 99400891

It	x	y = $\sqrt{x^2 - n}$
1	9970	3.000000

y = 3.000000 é inteiro, logo 99400891 tem fatores 9967 e 9973.

d) n = 4087

It	x	y = $\sqrt{x^2 - n}$
1	64	3.000000

y = 3.000000 é inteiro, logo 4087 tem fatores 61 e 67

3) Considerando os blocos

122-425-109-91-324-99-22-302-313-24

Ficarão codificados assim:

144-431-461-302-345-407-308-433-510-382

4) Temos que resolver a congruência da diferença mod 26

D	S	T	V	E	A	K	A	C	R	CODIFICADA
3	18	19	21	4	26	10	26	2	17	
R	S	A	R	S	A	R	S	A	R	CHAVE
17	18	26	17	18	26	17	18	26	17	
-14	0	-7	4	-14	0	-7	8	-24	0	DIFFERENÇA
M	A	T	E	M	A	T	I	C	A	ORIGINAL

5) Temos primeiro que encontrar "d" o inverso de 3 mod $\varphi(n)$

$d.e \equiv 1\ (mod\ 460)$

$\Rightarrow 3.d - 1 = 460k$

$\Rightarrow 3.d = 460k + 1$

$\Rightarrow 3.d = 459k + k + 1$

$\Rightarrow k + 1 = M(3) \Rightarrow k = 2$

$\Rightarrow d = 307$

Basta calcular $[c(b)]^d$ módulo n. Agora vamos decodificar o bloco 144, usando o método da expansão binária

Queremos encontrar o resto da divisão de 144^{307} por 517.

$307 = 2^8 + 2^5 + 2^4 + 2^1 + 2^0$

$144^{307} = 147^{2^8}.147^{2^5}.147^{2^4}.147^{2^1}.147^{2^0}$

i	0	1	2	3	4	5	6	7	8
$144^{2^i}(mod\ 517)$	144	56	34	122	408	507	100	177	309

$144^{307} \equiv 147^{2^8}.147^{2^5}.147^{2^4}.147^{2^1}.147^1 \equiv 144.56.408.507.309 \equiv 122\ mod\ 517$

Repetindo o mesmo processo para cada um dos blocos obteremos:

122-425-109-91-324-99-22-302-313-24

Apêndice 1

#	n	M_n	Dígitos em M_n	Data do descobrimento	Descobridor
1	2	3	1	*Antiguidade*	*Antiguidade*
2	3	7	1	*Antiguidade*	*Antiguidade*
3	5	31	2	*Antiguidade*	*Antiguidade*
4	7	127	3	*aAntiguidade*	*Antiguidade*
5	13	8.191	4	1456	*anônimo*
6	17	131.071	6	1588	Pietro Antonio Cataldi
7	19	524.287	6	1588	Pietro Antonio Cataldi
8	31	2.147.483.647	10	1772	Leonhard Paul Euler
9	61	2.305.843.009.213.693.951	19	1883	Ivan Mikheevich Pervushin
10	89	618970019…449.562.111	27	1911	R.E.Powers
11	107	162259276…010.288.127	33	1914	E. Fauquemberque
12	127	170141183…884.105.727	39	1876	Édouard Lucas
13	521	686479766…115.057.151	157	30 de janeiro de 1952	Raphael M. Robinson
14	607	531137992…031.728.127	183	30 de janeiro de 1952	Raphael M. Robinson
15	1.279	104079321…168.729.087	386	25 de junho de 1952	Raphael M. Robinson
16	2.203	147597991…697.771.007	664	7 de outubro de 1952	Raphael M. Robinson
17	2.281	446087557…132.836.351	687	9 de outubro de 1952	Raphael M. Robinson
18	3.217	259117086…909.315.071	969	8 de setembro de 1957	Hans Riesel
19	4.253	190797007…350.484.991	1.281	3 de novembro de 1961	Alexander Hurwitz
0	4.423	285542542…608.580.607	1.332	3 de novembro de 1961	Alexander Hurwitz
21	9.689	478220278…225.754.111	2.917	11 de maio de 1963	Donald B. Gillies
22	9.941	346088282…789.463.551	2.993	16 de maio de 1963	Donald B. Gillies
23	11.213	281411201…696.392.191	3.376	2 de junho de 1963	Donald B. Gillies
24	19.937	431542479…968.041.471	6.002	4 de março de 1971	Bryant Tuckerman
25	21.701	448679166…511.882.751	6.533	30 de outubro de 1978	Landon Curt Noll e Laura Nickel
26	23.209	402874115…779.264.511	6.987	9 de fevereiro de 1979	Landon Curt Noll
27	44.497	854509824…011.228.671	13.395	8 de abril de 1979	H. Nelson e David Slowinski

28	86.243	536927995…433.438.207	25.962	25 de setembro de 1982	David Slowinski
#	***n***	***M*$_n$**	**Dígitos em *M*$_n$**	**Data do descobrimento**	**Descobridor**
29	110.503	521928313…465.515.007	33.265	25 de setembro de 1988	Walt Colquitt e Luke Welsh
30	132.049	512740276…730.061.311	39.751	20 de setembro de 1983	David Slowinski
31	216.091	746093103…815.528.447	65.050	6 de setembro de 1985	David Slowinski
32	756.839	174135906…544.677.887	227.832	19 de setembro de 1992	David Slowinskii e Paul Gage
33	859.433	129498125…500.142.591	258.716	10 de janeiro de 1994	David Slowinski e Paul Gage
34	1.257.787	412245773…089.366.527	378.632	3 de setembro de 1996	David Slowinski e Paul Gage
35	1.398.269	814717564…451.315.711	420.921	13 de novembro de 1996	GIMPS / Joel Armengaud
36	2.976.221	623340076…729.201.151	895.932	24 de agosto de 1997	GIMPS / Gordon Spence
37	3.021.377	127411683…024.694.271	909.526	27 de janeiro de 1998	GIMPS / Roland Clarkson
38	6.972.593	437075744…924.193.791	2.098.960	1 de junho de 1999	GIMPS / Nayan Hajratwala
39	13.466.917	924947738…256.259.071	4.053.946	14 de novembro de 2001	GIMPS / Michael Cameron
40	20.996.011	125976895…855.682.047	6.320.430	17 de novembro de 2003	GIMPS / Michael Shafer
41	24.036.583	299410429…733.969.407	7.235.733	15 de maio de 2004	GIMPS / Josh Findley
42*	25.964.951	122164630…577.077.247	7.816.230	18 de fevereiro de 2005	GIMPS / Martin Nowak
43*	30.402.457	315416475…652.943.871	9.152.052	15 de dezembro de 2005	GIMPS / Curtis Cooper
44*	32.582.657	124575026…053.967.871	9.808.358	4 de setembro de 2006	GIMPS / Curtis Cooper
45*	37.156.667	202254406…308.220.927	11.185.272	6 de setembro de 2008	GIMPS / Hans-Michael Elvenich
46*	42.643.801	169873516…562.314.751	12.837.064	12 de abril de 2009	GIMPS / Odd M. Strindmo
47*	43.112.609	316470269…697.152.511	12.978.189	23 de agosto de 2008	GIMPS / Edson Smith
48*	57.885.161	581887266…724.285.951	17.425.170	25 de janeiro de 2013	GIMPS / Curtis Cooper

Conclusão

Esse trabalho teve como objetivo o estudo de alguns métodos de Criptografia, vimos que existem vários métodos de criptografia: Criptografia Simétrica (que usa apenas uma chave), a Criptografia Assimétrica (chaves-públicas e privadas) e a Criptografia via Curvas Elípticas.

Criptografia serve para vários propósitos, tais como a privacidade nas comunicações, transferências bancárias, informações diplomáticas secretas etc..

Vimos que é fácil criptografar uma mensagem via RSA, porém é muito difícil de decifrar, visto que não existem computadores rápidos o suficiente, nem algoritmos eficazes, que nos permitam fatorar um número inteiro muito grande que não tenha fatores relativamente pequenos.

Na verdade, não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente, não se sabe nem mesmo se é possível que esse algoritmo exista.

É preciso estimular o aprendizado por vários caminhos acessíveis e construir sólidos alicerces para o ensino e a pesquisa.

Se o processo de modernização do ensino se estende aos ramos de todas as disciplinas e há um grande esforço no sentido de melhorar seus aprendizados, no ensino da Álgebra o rompimento com os moldes tradicionais precisa ser definitivo. Desejamos que o ensino da álgebra suceda de maneira dinâmica e que ganhe vida com o uso dos instrumentos digitais disponíveis e a partir disso use o método dedutivo.

BIBLIOGRAFIA

[1] Ribenboim, P. Números primos-Velhos Mistérios e Novos Recordes, Coleção Matemética Universitária 1ª ed. Rio de Janeiro: IMPA, 2012;

[2] Coutinho, S. C. Números inteiros e Criptografia RSA, Coleção Matemática e Aplicações, Rio de Janeiro, IMPA, 2013;

[3] Jeffrey Hoffstein, Jill Pipher, J.H. Silverman. - An Introduction to Mathematical Cryptography 1ªEd, Springer, 2008

[4] Singh,Simon, O livro dos códigos tradução de Jorge Calife.- 6ª Ed.- Rio de Janeiro: Record, 2007

[5] Terada, Routo, Revista do professor de Matemática.- 12ª Ed

[6] Pimentel, Elaine, Álgebra A- Aula 10- Raízes primitivas.

[7] Salomão, Rodrigo, Um passeio pelo mundo secreto das curvas elípticas- Aulas 1, 2 e 3.

[8] Plínio de Oliveira Santos, José, Introdução a Teoria dos Números