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

Criptografia via curvas elípticas

Sergio dos Santos Correia Júnior

Rio de Janeiro
2013

Sergio dos Santos Correia Júnior

Criptografia via Curvas Elípticas

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

Correia Júnior, Sergio dos Santos

Criptografia via Curvas Elípticas / Sergio dos Santos Correia Júnior – 2013

87.p

1.Matemática 2. Álgebra. I. Título

CDU 536.21

Sergio dos Santos Correia Júnior

Criptografia via Curvas Elípticas

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

A meus pais, Maria Cristina e Sergio Correia, pelo incentivo e as minhas filhas, Gabriele e Alice, que foram o principal motivo para que eu concluísse esse estudo.

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 sobre curvas elípticas.

Esse trabalho foi desenvolvido em conjunto com o trabalho do professor João Gregório, cujo tema é o sistema de criptografia RSA. Em ambos há pré-requisitos comuns e o mesmo resumo histórico.

Esse trabalho tem como alvo principal estudantes 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.

Palavras-chaves: Criptografia, Curvas Elípticas, Problema do Logartimo Discreto

Agradecimentos

A todos os meus amigos pelo incentivo e ajuda durante todo o curso;

Ao meu amigo Sandro pelo carinho fraterno e pela ajuda com a apresentação;

Aos meus amigos Eduardo e Fábio pela preocupação e apoio;

Aos meus eternos mestres e amigos JJ e CATALDO, que, além de me ajudarem desde a graduação na UERJ, são verdadeiros exemplos de competência e amizade;

A todos os professores da UNIRIO, pela dedicação e companheirismo durante todo o curso;

Em especial ao professor SILAS, que, além de contribuir de forma decisiva para esse trabalho, com muita paciência e talento, foi um verdadeiro amigo durante todo esse período;

Aos meus pais e a meus irmãos, por quem tenho muita admiração e amor, pelo incentivo e carinho, dando-me condições de seguir até o fim com esse trabalho;

A minha querida e pioneira turma de mestrado que simplesmente foi maravilhosa.

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.

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.

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.

Os métodos de criptografia antigos necessitavam de uma comunicação prévia entre remetente e destinatário. Em virtude da proliferação dos meios de comunicação, do aparecimento dos computadores 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 de codificação de mensagens que não necessitassem dessa comunicação prévia ou que permitissem a troca de uma chave secreta por um meio de comunicação inseguro. Os métodos RSA e ECC (criptografia via curvas elípticas) são dois desses métodos.

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 chamado "Protocolo de Diffie e Hellman para Curvas Elípticas (PDHCE)," inicialmente proposto por Koblitz e Miller.

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 é 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 $\frac{5}{14} \cong 35\%$, 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**

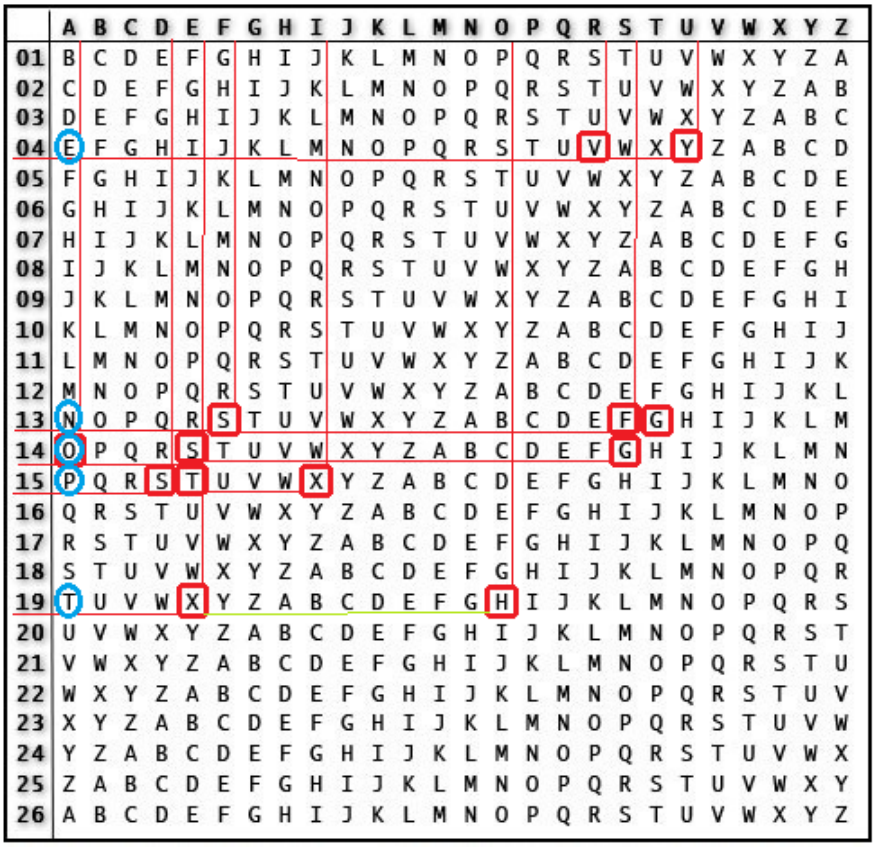
Desta forma, temos que:

- 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



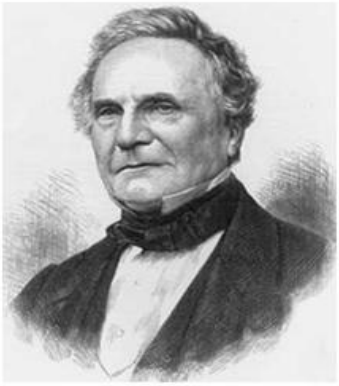
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	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**).



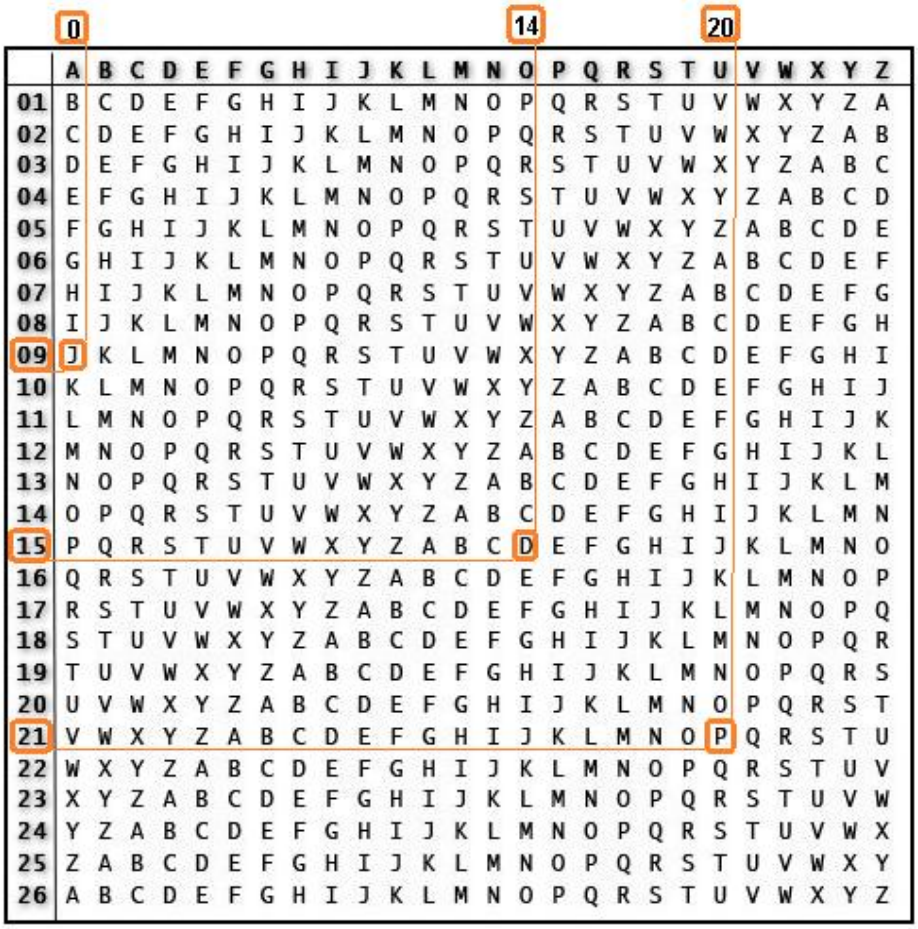
Mesmo conhecendo as técnicas desenvolvidas por Babbage e Kasisk pode-se levar bastante tempo tentando decifrar uma mensagem sem conhecer a palavra-chave. A palavra-chave usada na cifra da mensagem anterior é PAULINHO. Tente decifrar a mensagem. A resposta é um trecho da música "Solução de vida" de Paulinho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



	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.

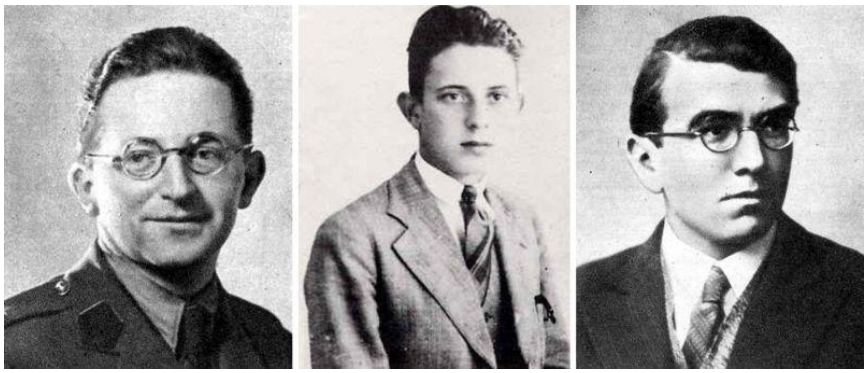
Em 1918 o inventor alemão **Arthur Scherbius (1878 -1925)** desenvolveu uma máquina criptográfica chamada ENIGMA, que ficou muito conhecida na 2ª guerra mundial.

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 elas 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:*



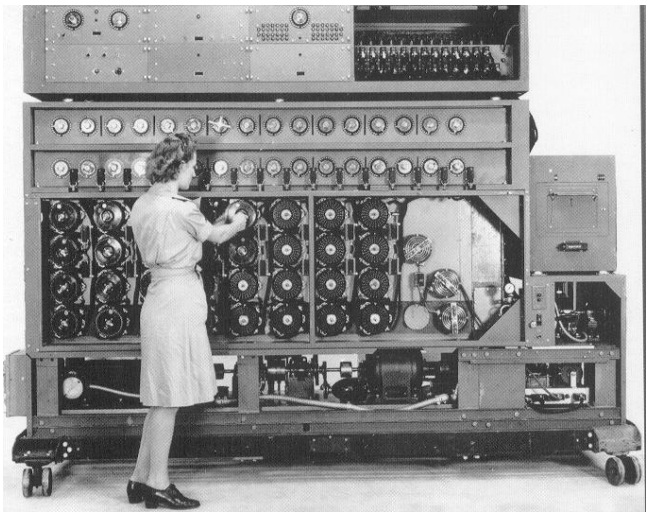
Marian Rejewski **Jerzy Różycki** **Henryk Zygalski**

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:

(⇒) $\bar{a} \in \mathbb{Z}_m$ 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 que $mdc\ (a,m) = 1$.

(⇐) 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 conseqüência 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 capitulo 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 que no 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:

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

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

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

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 sequencia 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

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

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

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

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

$$\ldots$$

$$a_r \equiv a_{r-1}^2 \equiv g^{2^r} \quad (mod\ N)$$

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} $(mod\ 1000)$	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 $(mod\ N)$ usando a formula

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

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

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

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:

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

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 $a^{p-1} \equiv 1\ (mod\ p)$ 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 duas 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 fosse primo então, pelo pequeno Teorema de Fermat, deveríamos ter obtido 1. Portanto, 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 que 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 inteiro tal que

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

O número x é chamado de 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

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

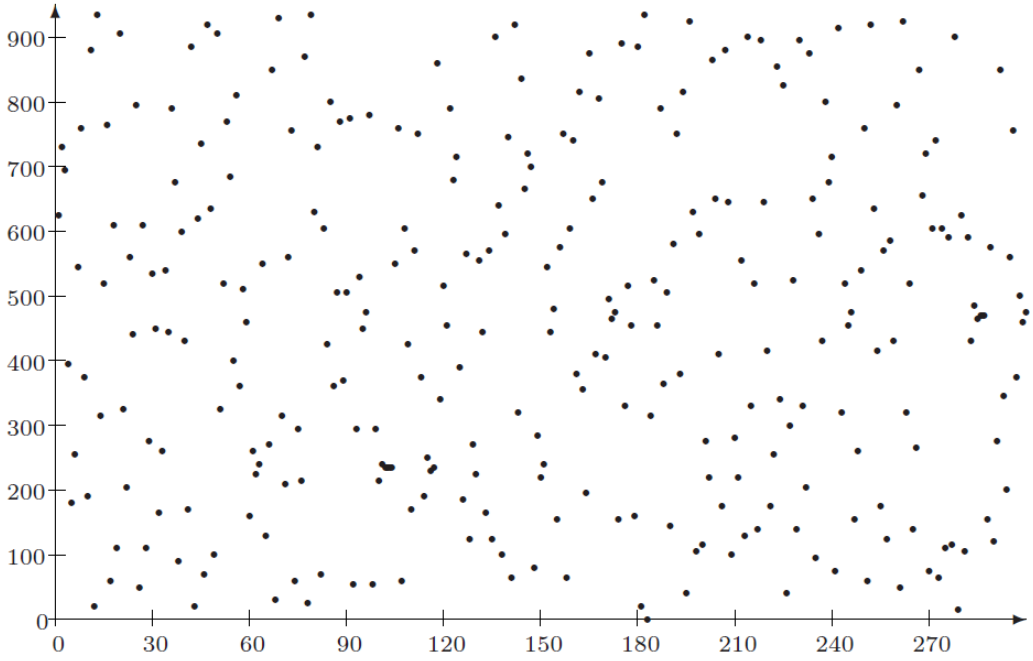
até encontrarmos alguma potência que seja côngruo a $b = 38679$ módulo $p = 56509$.

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. Joãozinho e Serginho 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 Joãozinho e Serginho compartilham, é observado pela Mônica.

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

No **primeiro passo**, Joãozinho e Serginho 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 Joãozinho e Serginho, são tornados de conhecimento público, permitindo que qualquer pessoa, inclusive Mônica, também conheça esses números.

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

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

No **terceiro passo**, Joãozinho envia o valor A para Serginho que, por sua vez, envia o valor B para Joãozinho. 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, Joãozinho e Serginho usam outra vez, seus inteiros secretos para calcular

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

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: Joãozinho e Serginhoconcordam em usar o primo $p = 941$ e a raiz primitiva $g = 627$.

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

Joãozinho envia para Serginho o número $A = 390$ e Serginho envia para Joãozinho 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, Joãozinho e Serginho 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 Joãozinho e Serginho. Para Mônica reconstituir as chaves secretas a e b de Joãozinho e Serginho, ela deverá resolver os seguintes problemas de congruência.

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

Assim ela conhecerá os expoentes secretos. Tanto quanto se sabe, este é o único caminho para Mônica encontrar o valor secreto compartilhado de Joãozinho e Serginho, 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, Joãozinho e Serginho 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 os dois é resolver o PLD, mas talvez isso não seja necessário. A segurança da chave compartilhada repousa sobre a dificuldade de resolver o seguinte problema, potencialmente mais fácil.

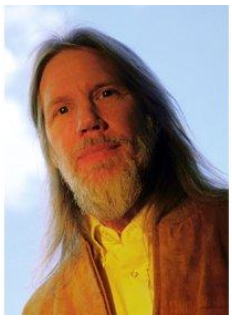
Definição: (Problema de Diffie - Hellman – *PDH*)

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 $B = g^b\ (mod\ p)$.

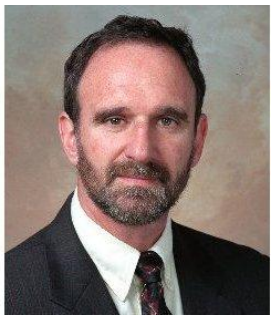
É claro que o *PDH* não é mais difícil do que o *PLD*. Se Mônica pode resolver o *PLD*, então ela pode calcular os expoentes secretos a e b de Joãozinho e Serginho que formam os valores interceptados $A = g^a$ e $B = g^b$, e então fica fácil Mônica calcular sua chave compartilhada, g^{ab} não transmitida 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 $x \equiv c_1^a \ (mod\ p)$

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

Passo 3: Calcula

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

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

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

$$A \equiv g^a \equiv 2^{153} \equiv 224\ \ (mod\ 467)$$

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:

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

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 $x \equiv c_1^a \equiv 87^{153} \equiv 367\ (mod\ 467)$

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

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

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.

Capítulo 4 - Criptografia via Curvas Elípticas

Curvas elípticas, apesar do nome, não estão associadas a elipses, apenas surgiram do problema da integral elíptica. Neste capítulo, apresentaremos a definição de curvas elípticas e uma operação de "soma" que define um grupo abeliano com os pontos da curva.

Em seguida, discutiremos as ideias do logaritmo discreto e da chave trocada de Diffie e Hellman adaptados para as curvas elípticas. Finalizaremos mostrando como enviar uma mensagem utilizando a criptografia sobre curvas elípticas (ECC), através do sistema de ElGamal.

A utilização de curvas elípticas em criptografia foi sugerida por Neal Koblitz e Victor S.Miller em 1985.

4.1. Preliminares

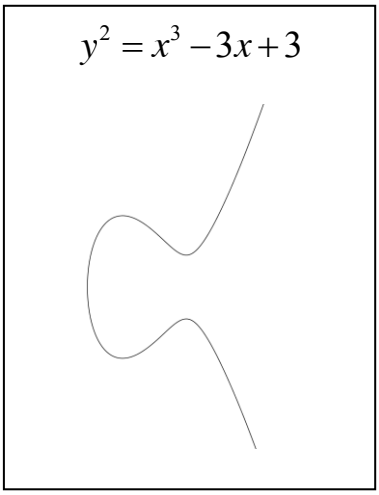
Uma curva elíptica C é o lugar geométrico dos pontos do plano cujas coordenadas cartesianas satisfazem a uma equação do tipo

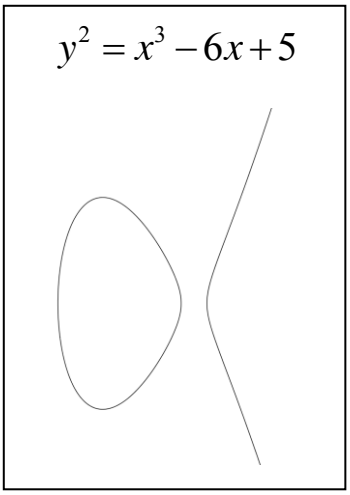
$$y^2 = x^3 + Ax + B$$

com A e B satisfazendo a condição $4A^3 + 27B^2 \neq 0$. Esta desigualdade é uma forma de garantir que a curva não tenha singularidades, o que possibilitará determinar a reta tangente em todos os pontos da curva, fato este, que será verificado no decorrer do texto.

Equações do tipo
$$y^2 = x^3 + Ax + B$$
são chamadas de equações de Weierstrass, em homenagem ao matemático alemão Karl Weierstrass (1815 – 1897).

Exemplos de curvas elípticas:



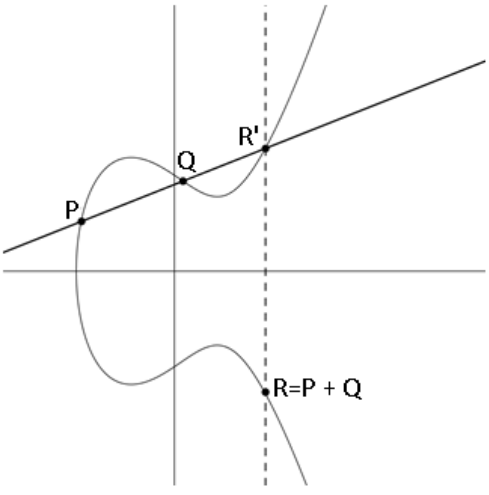


O que torna curvas elípticas particularmente interessantes do ponto de vista algébrico/aritmético é o fato de que toda curva elíptica é um *grupo abeliano*[*]. Isso quer dizer que podemos **"SOMAR"** dois pontos P e Q de uma curva elíptica E, obtendo um terceiro ponto $R = P + Q$ de E, e esta operação goza das propriedades: comutatividade, existência de elemento neutro, existência do elemento inverso e associatividade.

Esta lei de grupo possui a seguinte descrição geométrica, conhecida popularmente como **"lei da corda-tangente":**

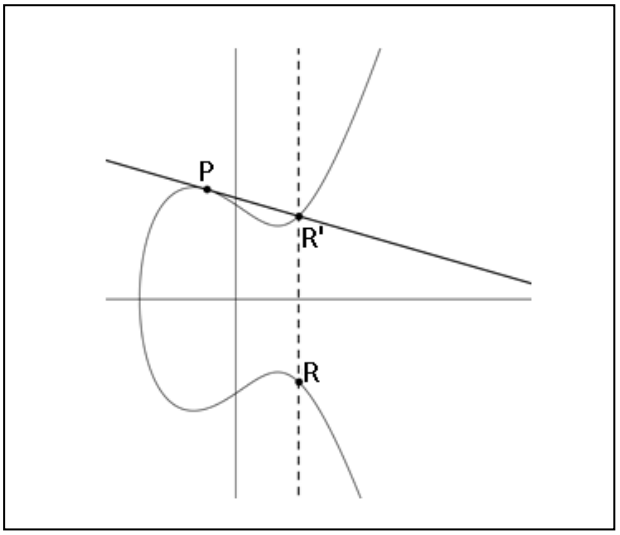
LEI DA CORDA-TANGENTE: A soma de dois pontos P e Q é a reflexão R, pelo eixo-x, do terceiro ponto de interseção R' da curva elíptica E com a reta que liga P e Q.

É mais fácil de entender fazendo uma figura da curva elíptica ao lado: $y^2 = x^3 - 3x + 3$.



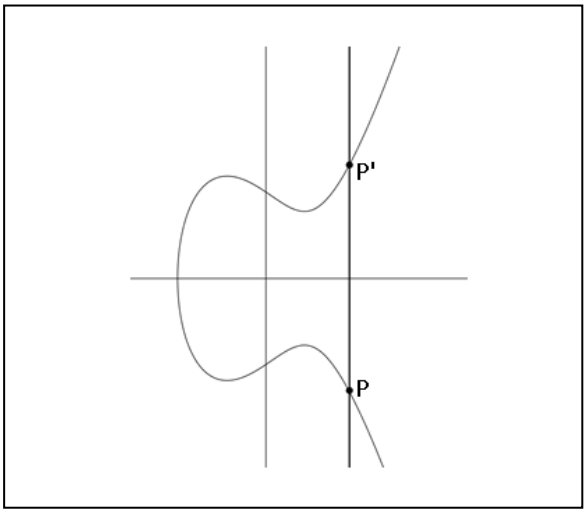
Para somarmos os pontos P e Q da curva, traçamos a reta PQ e marcamos o ponto R', outra interseção dessa reta com a curva. Pelo ponto R' traçamos uma reta perpendicular ao eixo horizontal. A interseção dessa reta com a curva E é o ponto $R = P + Q$. Observe que o ponto R é a reflexão do ponto R' em relação ao eixo horizontal.

Uma situação que também devemos analisar é a soma de $P + P$. Neste caso, desenhamos a reta tangente à curva E no ponto P e tomamos o ponto R', a outra interseção da curva E com essa reta. Observe a figura abaixo.

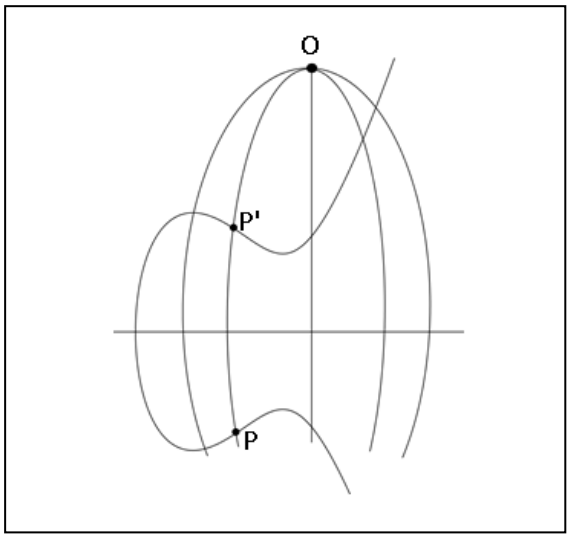


O ponto $R = P + P$ é a reflexão do ponto R' em relação ao eixo horizontal.

Outra situação a ser analisada, é quando somamos P ao seu simétrico P' em relação ao eixo-x.

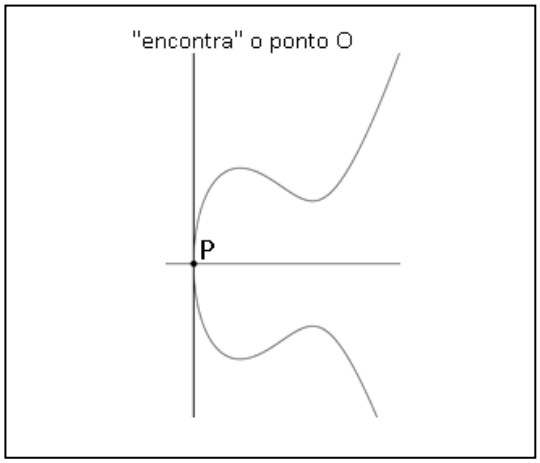


Neste caso a reta não intersecta novamente a curva. Para resolvermos esse problema, vamos criar um ponto O que esteja em toda a reta vertical do plano, que chamaremos de **"Ponto no infinito"**, observando que este ponto não pertence ao plano cartesiano $\mathbb{R}^2$, pois alem disso, queremos que ele esteja na interseção de toda reta vertical com a curva E. Esta propriedade se torna mais natural quando pensamos nas margens de uma estrada desaparecendo no horizonte.



Assim $P + P' = O$. Note que, a partir dessa ideia, também podemos definir $P + O = P$, pois a reta que passa pelos pontos P e O encontra o ponto P' da curva elíptica E cuja reflexão é o ponto P, portanto ***O* é o elemento neutro** para esta definição de soma, e consequentemente $O + O = O$. Observe também que P', o simétrico de P em relação ao eixo horizontal, é o único ponto que somado com P é igual a O. Então, o inverso de P é o ponto P', isto é, $P' = -P$.

Agora estamos pronto para definir a soma $P + P$ quando a reta tangente ao ponto P é perpendicular ao eixo horizontal. Neste caso, esta reta encontra o terceiro ponto da curva elíptica no ponto O, cuja reflexão é o próprio ponto O, assim, teremos $P + P = O$.



Desta forma o conjunto

$$E(\mathbb{R}^2) = \{(x,y) \in R^2; y^2 = x^3 + Ax + B\} \cup \{O\},$$

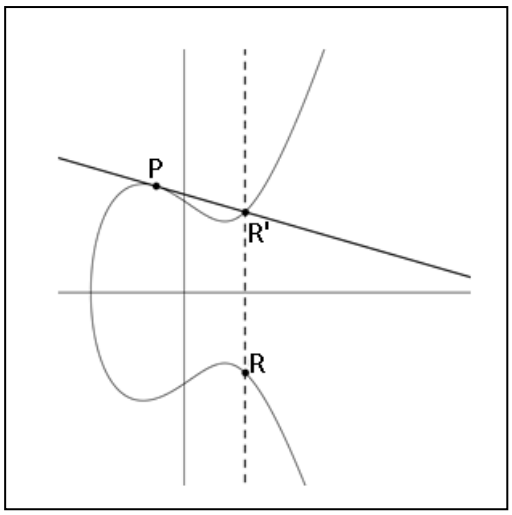
munido da operação de soma de pontos, goza das seguintes propriedades:

- $P + Q = Q + P$, pois a reta passando por P e Q é a mesma que passa por Q e P.
- $P + O = P$ para todo P, pois se $P \neq O$ a reta que liga P a O é a reta vertical que passa por P e portanto intercepta E novamente em $-P$, o simétrico P em relação ao eixo-x, logo refletindo novamente obtemos P de volta. O caso $P = O$ já foi considerado acima.
- $O + O = O$.
- $P + (-P) = O$, pois para $P = O$, a reta que liga os pontos P e $-P$ simétricos em relação ao eixo$-x$, é a reta vertical passando por P, observe que isto é válido mesmo no caso em que $P = -P$, ou seja, quando P está sobre o eixo x, pois neste caso a reta tangente em P é vertical.
- $P + (Q + S) = (P + Q) + S$ para todo $P, Q, S \in E$. A verificação da propriedade associativa está excluída do objetivo desse texto.

Assim, podemos dizer que $(E(\mathbb{R}^2), +)$ é um grupo comutativo.

A existência destas descrições geométricas para uma operação algébrica é surpreendente, pois abre a possibilidade de aliar a intuição geométrica juntamente com a precisão algébrica no estudo de curvas elípticas que podem ser definidas sobre corpos arbitrários.

Afirmação: O coeficiente angular da reta tangente a uma curva elíptica E:$y^2 = x^3 + Ax + B$ no ponto $P = (x_0, y_0)$ é dado por $m = \frac{3x_0^2 + A}{2y_0}$.



Prova: Sejam $r: y = mx + n$ a reta tangente a E no ponto $P = (x_0, y_0)$ e $R' = (x_1, y_1)$ o outro ponto de interseção da curva E com a reta tangente r.

Substituindo $y = mx + n$ em $y^2 = x^3 + Ax + B$, obtemos $(mx + n)^2 = x^3 + Ax + B \Rightarrow x^3 - m^2x^2 + x(A - 2mn) + B - n^2 = 0$. Como a reta r: $y = mx + n$ é tangente à curva E no ponto $P = (x_0, y_0)$, a raiz x_0 possui multiplicidade maior que ou igual a 2.

Assim, podemos representar as raízes da equação $x^3 - m^2x^2 + x(A - 2mn) + B - n^2 = 0$ por x_0, x_0 e x_1 Segue, das **Relações de Girard**, que:

$$\begin{cases} m^2 = x_0 + x_0 + x_1 \Rightarrow x_1 = m^2 - 2x_0 \\ A - 2mn = x_0\, x_1 + x_0\, x_1 + x_0 x_0 \end{cases} \Rightarrow A - 2mn = 2x_0(m^2 - 2x_0) + x_0^2$$

Como $P = (x_0, y_0)$ pertence à reta r, podemos escrever $n = y_0 - mx_0$,, assim:

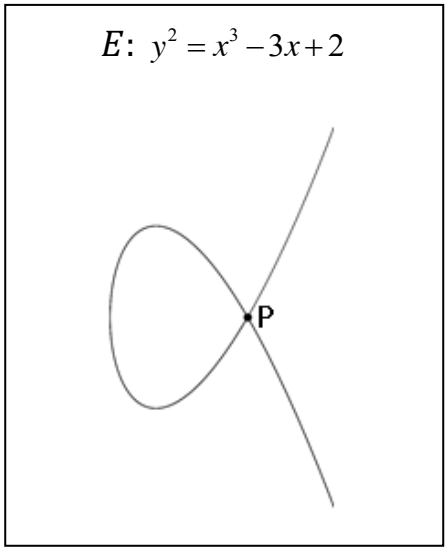
$$A - 2m(y_0 - mx_0) = 2x_0\,(m^2 - 2x_0) + x_0^2 \Rightarrow A - 2my_0 = -3x_0^2$$

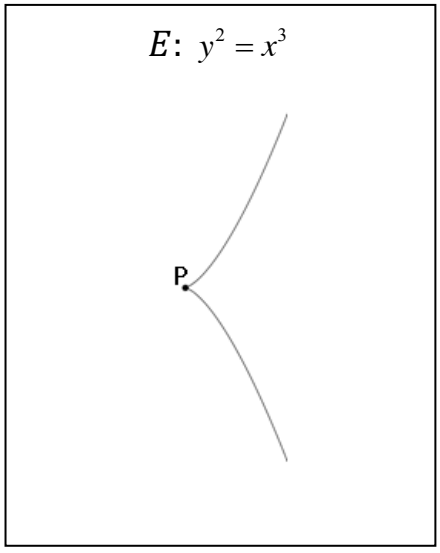
$$\Rightarrow m = \frac{3x_0^2 + A}{2y_0}.$$

NOTA: Esta fórmula pode ser obtida facilmente por derivada.

$$y^2 = x^3 + Ax + B \Rightarrow 2yy' = 3x^2 + A \Rightarrow y' = \frac{3x^2 + A}{2y}.$$

É óbvio que essa fórmula está bem definida para y_0 diferente de zero. Se $y_0$for igual a zero e $3x_0^2 + A$ for diferente de zero, a fórmula sugere que a reta tangente é perpendicular ao eixo horizontal. Esse caso será discutido mais à frente, antes precisamos resolver outro problema. Note que nas duas curvas elípticas a seguir não é possível determinar qual é a reta tangente no ponto P.





Além disso, não conseguimos definir a soma $P + P$ quando a curva apresenta alguma singularidade no ponto P, ou seja, quando o coeficiente da reta tangente no ponto P não está determinado. Já sabemos que o coeficiente angular da reta tangente em cada ponto (X, Y) é dado por $\frac{3X^2+A}{2Y}$. A indeterminação ocorre quando, no cálculo da inclinação da reta, aparece $\frac{0}{0}$. Então não podemos ter $3X^2 + A = 0$ e $2Y = 0$. Vamos determinar a relação entre A e B de modo que se $3X^2 + A = 0$, então $Y = 0$.

$$3X^2 + A = 0 \;\Rightarrow\; X^2 = -\frac{A}{3} \;\Rightarrow\; X = \pm\sqrt{-\frac{A}{3}}\,.$$

$$Y \neq 0 \;\Rightarrow\; X^3 + AX + B \neq 0$$

$$\Rightarrow\; X\,.\,(X^2 + A) + B \neq 0$$

$$\Rightarrow\; \left(\pm\sqrt{-\frac{A}{3}}\right) \cdot \left(-\frac{A}{3} + A\right) + B \neq 0$$

$$\Rightarrow\; B \neq \left(\mp\sqrt{-\frac{A}{3}}\right) \cdot \left(-\frac{2A}{3}\right)$$

$$\Rightarrow\; B^2 \neq \left(-\frac{A}{3}\right) . \left(\frac{4A^2}{9}\right) = \frac{-4A^3}{27}$$

$$\Rightarrow\; 4A^3 + 27B^2 \neq 0.$$

Portanto a relação $4A^3 + 27B^2 \neq 0$ é importante para que a soma $P + P$ esteja definida para qualquer ponto P na curva E.

É fácil verificar que os coeficientes das curvas da figura acima não obedecem a essa relação.

Na curva elíptica $Y^2 = X^3 - 3X + 2$, temos $A = -3$ e $B = 2$ e, consequentemente, $4A^3 + 27B^2 = 4 \cdot (-3)^3 + 27 \cdot 2^2 = 0$.

Na curva $Y^2 = X^3$ a verificação é ainda mais fácil, pois A e B são iguais a zero.

4.1.2. Algoritmo de Soma de Pontos na Curva Elíptica

Nosso próximo objetivo é encontrar fórmulas explícitas para sermos capazes de somarmos pontos em uma curva elíptica. Para obtermos estas fórmulas utilizaremos simplesmente geometria analítica elementar e pequenas manipulações algébricas conforme resultado abaixo.

Algoritmo de Soma de Pontos na Curva Elíptica: Sejam

$$E:\ y^2 = x^3 + Ax + B \quad com \quad 4A^3 + 27B^2 \neq 0$$

e P_1 *e* P_2 pontos da curva elíptica E.

1) $P_1 = O \Rightarrow P_1 + P_2 = P_2$
2) $P_2 = O \Rightarrow P_1 + P_2 = P_1$
3) Caso contrário, escreva $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$
4) Se $x_1 = x_2$ e $y_1 = -y_2 \Rightarrow P_1 + P_2 = O$
5) Caso contrário, defina λ por

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ se } P_1 \neq P_2 \quad \text{ou} \quad \lambda = \frac{3x_1^2 + A}{2y_1} \ se \ P_1 = P_2$$

Então $P_3 = P_1 + P_2 = (x_3, y_3)$ onde

$$x_3 = \lambda^2 - x_1 - x_2 \quad e \quad y_3 = \lambda(x_1 - x_3) - y_1$$

Portanto, se:

- $y = \lambda x + \mu$ é a reta P_1P_2 onde ($P_1 \neq P_2$ ou $P_1 = P_2$) e
- $P_3' = (x'_3; y'_3)$ é o outro ponto de interseção entre a reta e a curva E,

podemos escrever:

$$(\lambda x + \mu)^2 = x^3 + Ax + B \Rightarrow x^3 - \lambda^2 x^2 + (A - 2\lambda\mu)x + B - \mu^2 = 0.$$

Como x_1, x_2, x'_3 são as raízes dessa equação, temos que a soma das raízes

$$x_1 + x_2 + x'_3 = \lambda^2 \Rightarrow x'_3 = \lambda^2 - x_2 - x_1.$$

Acabamos de obter uma fórmula para a abscissa x'_3 do ponto P_3' que é a mesma abscissa x_3 do ponto $P_3 = P_1 + P_2$, logo $\boldsymbol{x'_3 = \lambda^2 - x_2 - x_1}$.

Agora vamos encontrar uma fórmula para a ordenada y'_3. Isso é fácil, basta substituir $x'_3 = x_3$ na equação da reta, mas antes vamos notar que $P_1 = (x_1, y_1)$ também pertence à reta $y = \lambda x + \mu$, logo

- $y_1 = \lambda x_1 + \mu \quad \Rightarrow \quad \mu = y_1 - \lambda x_1$.
- $y'_3 = \lambda x_3 + \mu = \lambda x_3 + (y_1 - \lambda x_1) = \lambda\,(x_3 - x_1) + y_1$

consequentemente

$$\boldsymbol{y_3 = -y'_3 = \lambda(x_1 - x_3) - y_1}$$

Se P e Q são pontos racionais de uma curva elíptica E sobre $\mathbb{Q}$ é fácil ver que a soma $P + Q$ também é um ponto racional de E. Em particular, dado um ponto racional P de E, a lei de grupo permite construir "NOVOS" pontos racionais, a saber, os múltiplos inteiros de P

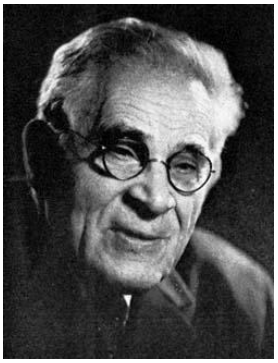
$$\ldots, -3P, -2P, -P, O, P, 2P, 3P, \ldots$$

Observe que os elementos desta lista, não precisam ser distintos. Por exemplo, se $P = O$ é o elemento neutro, então a lista acima só contem um elemento.

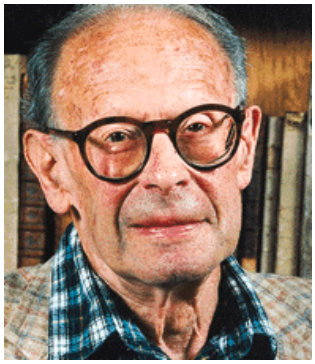
Desta forma, **é bastante natural perguntar se é possível encontrar** um "CONJUNTO DE GERADORES" $\{P_1, P_2, \ldots, P_r\}$ para os pontos racionais de E, de modo que qualquer ponto racional P de E se escreve como combinação $\mathbb{Z}$-linear de $P_1, \ldots, P_r$, isto é

$$P = n_1 P_1 + \cdots + n_r P_r \quad com\ (n_i \in \mathbb{Z})$$

Este é precisamente o conteúdo de um resultado clássico da literatura, conhecido como **Teorema de Mordell-Weil** que diz que dada uma curva elíptica $E: y^2 = x^3 + ax + b$ sobre $\mathbb{Q}$, ou seja, $a, b \in \mathbb{Q}$, mais um ponto no infinito, então o conjunto $E(\mathbb{Q})$ dos pontos racionais de E é um grupo finitamente gerado.

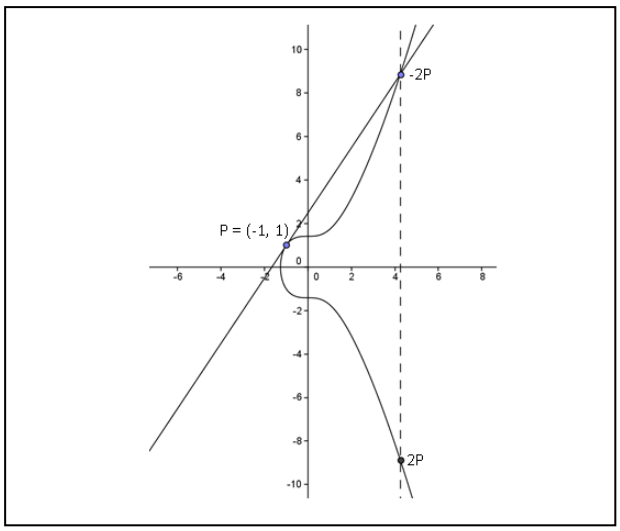


Louis J.Mordell (1888 – 1972)



André Weil (1906 – 1998)

Exemplo: Considere a curva elíptica $y^2 = x^3 + 2$ e o ponto $P = (-1,1)$ dessa curva. Vamos encontrar o ponto $2P = P + P$.



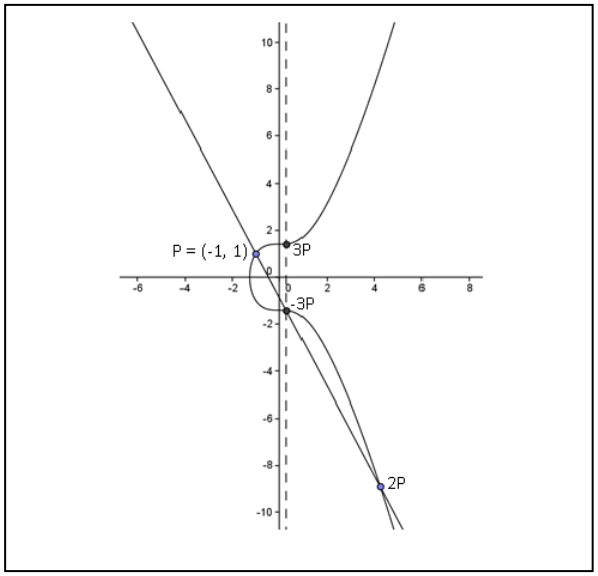
Como estamos somando dois pontos iguais,

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot (-1)^2 + 0}{2 \cdot 1} = \frac{3}{2}.$$

Agora vamos calcular as coordenadas x_3 *e* y_3 do ponto $2P = P + P$.

- $x_3 = \lambda^2 - x_1 - x_2 = \left(\frac{3}{2}\right)^2 - (-1) - (-1) = \frac{17}{4}$
- $y_3 = \lambda(x_1 - x_3) - y_1 = \frac{3}{2} \cdot \left(-1 - \frac{17}{4}\right) - 1 = -\frac{71}{8}$

Segue que $2P = (x_3, y_3) = \left(\frac{17}{4}, \frac{-71}{8}\right)$. Agora vamos somar o ponto P com o ponto $2P$ para obtermos o ponto $3P = P + 2P$.



Como os pontos P e $2P$ são distintos,

$$\lambda = \frac{y_3 - y_1}{x_3 - x_1} = \frac{\frac{-71}{8} - 1}{\frac{17}{4} - (-1)} = \frac{-79}{42}.$$

Agora vamos calcular as coordenadas x_4 *e* y_4 do ponto 3P = P + 2P.

- $x_4 = \lambda^2 - x_1 - x_3 = \left(\frac{-79}{42}\right)^2 - (-1) - \left(\frac{17}{4}\right) = \frac{127}{441}$
- $y_4 = \lambda(x_1 - x_4) - y_1 = \frac{-79}{42} \cdot \left(-1 - \frac{127}{441}\right) - 1 = \frac{13175}{9261}$

Segue que

$$3P = (x_4, y_4) = \left(\frac{127}{441}, \frac{13175}{9261}\right).$$

De modo análogo, calculamos $4P = P + 3P = (x_5, y_5)$ e encontramos

$$4P = \left(\frac{66113}{80656}, -\frac{36583777}{22906304}\right).$$

4.1.3. Curvas elípticas sobre $\mathbb{Z}_p$

Chegamos a uma etapa importante para a aplicação de curvas elípticas na criptografia. Agora vamos aplicar a definição que vimos para a soma de pontos de uma curva elíptica sobre o corpo finito $\mathbb{Z}_p$, onde p é um número primo. Para isso, definimos uma curva elíptica E sobre $\mathbb{Z}_p$ como uma equação do tipo

$$y^2 = x^3 + ax + b \quad com \quad a, b \in \mathbb{Z}_p \quad e \quad 4a^3 + 27b^2 \neq 0$$

e olhamos para os pontos de E com coordenadas em $\mathbb{Z}_p$. Denotaremos esses pontos por

$$E(\mathbb{Z}_p) = \{(x, y); x, y \in \mathbb{Z}_p ; \ y^2 = x^3 + ax + b\} \cup \{O\}$$

Claramente o conjunto de pontos $E(\mathbb{Z}_p)$ é um conjunto finito, visto que existe somente um número finito de possibilidades para as coordenadas x e y. Mais precisamente, existe p possibilidades para x e então para cada x, a equação $y^2 = x^3 + ax + b$ mostra que existe pelo menos duas possibilidades para y. Adicionando o ponto extra O, temos que $\#E(\mathbb{Z}_p) \leq 2p + 1$. No entanto, esta estimativa é consideravelmente maior do que a quantidade real de pontos de $E(\mathbb{Z}_p)$. Faremos um exemplo para ilustrar esta situação.

Exemplo: Considere a curva elíptica dada por $y^2 = x^3 - x$ sobre $\mathbb{Z}_5$. É fácil verificar que esta curva possui apenas **8 (oito)** pontos, dados a seguir:

$$E(\mathbb{Z}_5) = \{(0,0), (1,0), (2,1), (2,-1), (3,2), (3,-2), (4,0)\} \cup \{O\}.$$

Para um corpo finito com poucos elementos, é fácil verificar a quantidade de pontos de $E(\mathbb{Z}_p)$. Mas se a curva elíptica E estivesse sobre $\mathbb{Z}_{2017}$? onde 2017 é o próximo ano primo, que será logo após as olimpíadas do Rio de Janeiro; qual a quantidade de pontos de $E(\mathbb{Z}_{2017})$?

Um resultado famoso nesta direção, conhecido na literatura como **Teorema de Hasse-Weil**, diz que se E é uma curva elíptica sobre $\mathbb{Z}_p$ então

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{Z}_p) \leq p + 1 + 2\sqrt{p}$$

Assim, $\#E(\mathbb{Z}_{2017}) \leq 2017 + 1 + 2\sqrt{2017} \cong 2018 + 90 = 2108$ é uma estimativa melhor que $\#E(2017) \leq 2.2017 + 1 = 4035$. Faremos mais um exemplo para clarear as ideias.

Exemplo: Considere a curva elíptica dada pela equação

$$E: \quad y^2 = x^3 + 2x + 7 \ \ sobre \ \ \mathbb{Z}_{13}$$

Podemos encontrar os valores de $E(\mathbb{Z}_{13})$ substituindo cada $x \in \mathbb{Z}_{13}$ no polinômio $x^3 + 2x + 7$ e decidir se este valor é um quadrado ou não

y	y^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

x	$x^3 + 2x + 7$
0	7
1	10
2	6
3	1
4	1
5	12
6	1
7	0
8	2
9	0
10	0
11	8
12	4

(x, y)	y^2	$x^3 + 2x + 7$
(1,6), (1,7)	10	10
(3,1), (4,1), (6,1)	1	1
(3,12), (4,12), (6,12)	1	1
(5,5), (5,8)	12	12
(7,0), (9,0), (10,0)	0	0
(12,2), (12,11)	4	4

Segue da última tabela que $\#E(\mathbb{Z}_{13}) = 16$ onde

$$E(Z_{13}) = \{(1,6).(1,7), (3,1), (4,1), (6,1), (3,12), (4,12), (6,12)\}$$

$$\cup \{(5,5), (5,8), (7,0), (9,0), (10,0), (12,2), (12,11)\} \cup \{O\}$$

Agora, **Usando o Algoritmo de Soma de Pontos na Curva Elíptica**, podemos observar facilmente que:

Se $P_1 = (5,8)\ e\ P_2 = O$ então $P_1 + P_2 = (5,8)$

Se $P_1 = (3,1)\ e\ P_2 = (3,12)$ então $P_1 + P_2 = O$. **De fato**, $(3,1)$ e $(3,12)$ são simétricos em relação ao eixo horizontal, pois $12 \equiv -1(mod\ 12)$ e consequentemente $(3,12) = (3,-1)$.

Se $P_1 = (5,8)\ e\ P_2 = (12,11)$ então $\lambda = \frac{11-8}{12-5} = \frac{3}{7}$. Opa! Parece que temos um problema, pois estamos trabalhando módulo 13. **Neste momento surge uma pergunta muito natural**: Qual é o significado de $\lambda = \frac{3}{7}\ (mod\ 13)$? A resposta para isso é baseada no fato de que $\lambda = \frac{3}{7}$ é a solução da equação $7\lambda = 3$. Portanto, basta resolvermos a equação $7\lambda \equiv 3(mod 13)$. Não é difícil verificar que $\lambda = 6$ é a solução em Z_{13}. Agora podemos calcular explicitamente as coordenadas de $P_3 = P_1 + P_2 = (x_3, y_3) = (6,12)$, conforme verificação a seguir:

- $x_3 = \lambda^2 - x_2 - x_1 = 6^2 - 12 - 5 = 19 \equiv 6\ (mod\ 13)$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 6(5-6) - 8 = -14 \equiv 12\ (mod 13)$

Se $P_1 = P_2 = (1,6)$, então $\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 1^2 + 2}{2 \cdot 6} = \frac{5}{12}$. Resolvendo a equação $12\lambda \equiv 5\ (mod\ 13)$, encontramos $\lambda = 8$. Segue que $P_3 = (x_3, y_3) = (10,0)$ conforme contas a seguir:

- $x_3 = \lambda^2 - x_2 - x_1 = 8^2 - 1 - 1 = 62 \equiv 10\ mod\ 13$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 8(1-10) - 6 = -78 \equiv 0\ mod\ 13$.

4.2. Problema do Logaritmo Discreto para Curvas Elípticas *(PLDCE)*.

O Problema do Logaritmo Discreto (*PLD*) em $(Z_p)^*$, que vimos no capítulo 3, trata de encontrar um expoente x tal que $a^x \equiv b\ (mod\ p)$ e escrevemos $x = \log_a b$

Em outras palavras, o Problema do Logaritmo Discreto (*PLD*) consiste em determinar quantos fatores iguais a a são necessários para que o produto seja congruente a b módulo p, ou seja:

$$\underbrace{a.a.a \ldots a}_{x\ fatores} \equiv b\ \ (mod\ p)$$

De modo análogo, o Problema do Logaritmo Discreto em uma Curva Elíptica E (*PLDCE*) consiste em encontrar um inteiro m tal que

$$Q = \underbrace{P + P + P + \cdots + P}_{m\ parcelas} = mP$$

onde P e Q são dois pontos de $E(Z_p)$. Assim, o problema do logaritmo discreto (PLDCE) é o problema de encontrar um inteiro m tal que $Q = m\,P$. Por analogia com o problema do logaritmo discreto para $(\mathbb{Z}_p)^*$, denotamos o inteiro m por

$$m = \log_P(Q)$$

onde chamamos m o **Logaritmo Discreto Elíptico** de Q com respeito à P.

Lembre-se de que a lei de soma de pontos de uma curva elíptica é complicada, por isso determinar o logaritmo discreto em uma curva elíptica é até mais difícil do que em Z_p. Observando novamente a curva elíptica E: $y^2 = x^3 + 2x + 7$ sobre Z_{13}, onde temos que

$$E(Z_{13}) = \{(1,6).(1,7),(3,1),(4,1),(6,1),(3,12),(4,12),(6,12)\}$$

$$\cup\ \{(5,5),(5,8),(7,0),(9,0),(10,0),(12,2),(12,11)\}\ \cup \{O\}$$

Para o ponto $P = (3,1)$, usando o algoritmo, vemos que

- $2P = P + P = (6,1)$
- $3P = 2P + P = (6,1) + (3,1) = (4,12)$
- $4P = 3P + P = (4,12) + (3,1) = (10,0)$

Então, o Logaritmo Discreto Elíptico de

- $Q = (4,12)$ na base $P = (3,1)$ é igual a 3 pois $Q = 3P$.
- $Q = (10,0)$ na base $P = (3,1)$ é igual a 4 pois $Q = 4P$.

É importante enfatizar que a definição dada para Logaritmo Discreto Elíptico não é muito precisa. Há muitos pontos P e Q em $E(Z_p)$ tais que Q não é múltiplo de P e, consequentemente, para esses pontos o logaritmo não existe. Observando a lista de múltiplos de $P = (3,1)$ na curva elíptica dada:

$P = (3,1)$ $\quad 2P = (6,1)$ $\quad 3P = (4,12)$ $\quad 4P = (10,0)$

$5P = (4,1)$ $\quad 6P = (6,12)$ $\quad 7P = (3,12)$ $\quad 8P = O$

Perceba que esses são os únicos múltiplos de $P = (3,1)$, pois após $8P = O$ os valores se repetem:

$9P = P$ $\quad 10P = 2P$ $\quad 11P = 3P$ $\quad 12P = 4P$

e assim por diante. Assim vemos que todos os pontos de $E(Z_{13})$ que não estão nessa lista de múltiplos de P não possuem logaritmo na base $P = (3,1)$.

Claramente, temos para $Q = (5,8)$ que o $\log_P Q$ não existe, pois não existe m tal que $Q = mP$. Além disso, se existe um inteiro m satisfazendo $Q = mP$, então há infinitos inteiros que também satisfazem. Para ver isto, primeiro note que existe um inteiro s tal que $sP = O$. **De fato**, como $E(\mathbb{Z}_p)$ é finito, então a sequência infinita $(P, 2P, 3P, 4P, \ldots)$ possui elementos repetidos. Portanto, existem inteiros $k > j$ tais que $kP = jP$ e podemos tomar $s = (k - j)$. O menor desses elementos $s \geq 1$ é chamado de ordem de P.

Se s é a ordem de P e n é um inteiro qualquer tal que $Q = n\,P$ então as soluções para $Q = m\,P$ são os inteiros $m = n + r.s$ com $r \in \mathbb{Z}$. Isto significa que o valor de $\log_P(Q)$ é um elemento $\mathbb{Z}/s\mathbb{Z}$, isto é, $\log_P(Q)$ é um inteiro módulo s. onde s é a ordem de P. poderíamos dizer que $\log_P(Q) = n$, no entanto, a vantagem de se definir os valores para estarem em $\mathbb{Z}/s\mathbb{Z}$, é que o Logaritmo Discreto Elíptica satisfaz

$$\log_P(Q_1 + Q_2) = \log_P Q_1 + \log_p Q_2$$

De fato, fazendo $\log_P Q_1 = m \Rightarrow Q_1 = mP$ e $\log_P Q_2 = n \Rightarrow Q_2 = nP$ podemos escrever

$$Q_1 + Q_2 = mP + nP = (m + n)P \Rightarrow \log_P(Q_1 + Q_2) = m + n$$

o que ratifica a propriedade.

4.2.1. O algoritmo para calcular os múltiplos de um ponto de uma curva elíptica

Um problema que surge nesse momento é o de calcular $Q = mP$ para m grande. Podemos pensar de modo natural em calcular $2P = P + P, 3P = 2P + P, 4P = 3P + P$ e assim por diante, ate $\mathrm{m}P = (\mathrm{m} - 1)P + P$

Note que por esse processo, teremos que efetuar $(\mathrm{m} - 1)$ operações, o que não é muito prático mesmo que m não seja muito grande. No segundo capítulo, descrevemos um algoritmo para calcular $g^A \ (mod\ N)$ através da expansão binária, lembra?

Usaremos uma ideia análoga nas curvas elípticas. Para calcularmos, $Q = mP$ escreveremos mP como a soma de alguns termos da sequência $(P, 2P, 2^2P, 2^3P, \ldots)$, onde cada termo é obtido dobrando o seu antecessor. A grande vantagem deste algoritmo está no número de operações que precisam ser realizadas.

A maneira mais eficiente para calcular mP é muito similar ao método descrito no capítulo para calcular potências de $a^n \ mod \ N$, que necessitamos para a troca de chaves de Diffie-Hellmann.

Entretanto, visto que a operação em uma curva elíptica é escrita como uma adição no lugar de uma multiplicação, chamaremos as operações de dobra e soma, no lugar de quadrado e multiplicação. A ideia é similar à anterior. Primeiro escrevemos m na forma binária como

$$m = n_0 + n_1.2^1 + n_2.2^2 + \ n_3.2^3 + \cdots + n_r.2^r \quad \text{onde} \quad n_i \in \{0,1\}.$$

Podemos assumir que $n_r \ = \ 1$. O próximo passo é dobrar o passo anterior.

$Q_0 \ = \ P$	$Q_1 \ = \ 2Q_0$	$Q_2 \ = \ 2Q_1$	....	$Q_r \ = \ 2Q_{r-1}$

Note que Q_i é simplesmente duas vezes o antecessor Q_{i-1}. Assim

$$Q_i = 2^i \ P$$

Finalmente, computamos mP usando no máximo r somas

$$\text{m}P \ = \ n_0Q_0 \ + \ n_1Q_1 \ + \ n_2Q_2 \ + \cdots + \ n_rQ_r$$

Nos referimos à adição de dois pontos em $E(\mathbb{Z}_p)$ como uma ***operação de ponto***. Portanto o total de vezes para calcular mP é no máximo $2r$ operações de Ponto em $E(\mathbb{Z}_p)$. Note que $n \ \geq 2^r$. Por isso, não faremos mais do que 2 $log_2 \ (n)$ operações de pontos para calcular mP. Isto faz com que seja possível calcular mP, mesmo para valores muito grandes de m. Resumimos na tabela abaixo o algoritmo para calcular os múltiplos de um ponto de uma curva elíptica.

Entrada: Entre com o ponto $P \ \in \ E(\mathbb{Z}_p)$ e $n \geq 1$ inteiro

1. Seja $Q \ = \ P$ e $R \ = \ O$.
2. Enquanto $n \ > \ 0$ faça:
   - I. Se $n \ \equiv 1 \ mod \ 2$ então
   - II. Defina: $R \ = \ R \ + \ Q$
   - III. Defina: $Q \ = \ 2Q$
   - IV. Defina: $n \ = \left[\frac{n}{2}\right]$
   - V. Se $n \ > \ 0$ retorne ao passo 2
3. **Saída:** o ponto $R \ = \ nP$

Exemplo: Usaremos o algoritmo de dobrar e somar para calcular $R = nP$ em $E(\mathbb{Z}_p)$ para a curva elíptica $E: y^2 = x^3 + 14x + 19$ onde $n = 947$, $p = 3623$ onde o ponto $P = (6, 730) \in E(\mathbb{Z}_{3623})$. Escrevendo $n = 947$ na base 2, temos que:

$$n = 947 = \underbrace{\underbrace{1 + 2}_{3} + 2^4}_{19} + \underbrace{2^5}_{51} + \underbrace{2^7}_{179} + \underbrace{2^8}_{435} + \underbrace{2^9}_{947}$$

Fazendo os cálculos passo a passo, para obtermos $R = 947P$ efetuaremos 9 dobras com 6 somas, conforme a tabela a seguir:

Passo i	$n = \lceil n/2 \rceil$	$Q = 2^i P$	$R = R + Q$
0	947	$P = (6, 730)$	O
1	473	$(2521, 3601)$	$P = (6, 730)$
2	236 **(par)**	$(2277, 502)$	$3P = (2149, 196)$
3	118 **(par)**	$(3375, 535)$	$3P = (2149, 196)$
4	59	$(1610, 1851)$	$3P = (2149, 196)$
5	29	$(1753, 2436)$	$19P = (2838, 2175)$
6	14 **(par)**	$(2005, 1764)$	$51P = (600, 2449)$
7	7	$(2425, 1791)$	$51P = (600, 2449)$
8	3	$(3529, 2158)$	$179P = (3247, 2849)$
9	1	$(2742, 3254)$	$435P = (932, 1204)$
10	0	$(1814, 3480)$	$947P = (3492, 60)$

4.3. Criptografia via Curvas Elípticas

Chegamos ao momento mais esperado do nosso estudo de curvas elípticas. **Como usar as curvas elípticas na criptografia?** Começaremos apresentando a chave trocada Diffie-Hellman para curvas elípticas e depois mostraremos como funciona o sistema de criptografia com chave pública ElGamal em uma curva elíptica.

4.3.1. Chave Trocada DIFFIE-HELLMAN sobre uma curva Elíptica

Voltemos com nossos ilustres personagens, Joãozinho, Serginho e Mônica.
Primeiramente, Joãozinho e Serginho concordam em usar uma curva elíptica E sobre $\mathbb{Z}_p$ com ($p \gg 1$ primo) dada por uma equação do tipo

$$y^2 = x^3 + ax + b \quad com \quad a, b \in \mathbb{Z}_p \quad e \quad 4a^3 + 27b^2 \neq 0$$

e tomam $P \in E(\mathbb{Z}_p) = \{(x, y); x, y \in \mathbb{Z}_p ; \ y^2 = x^3 + ax + b\} \cup \{O\}$.

Esses dados são públicos, portanto qualquer um pode conhecê-los, onde descreveremos os passos na tabela abaixo:

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p \gg 1$ primo grande E uma curva elíptica sobre $\mathbb{Z}_p$ P um ponto de $E(\mathbb{Z}_p)$	
Passo 2: Escolhe $n_A \in \mathbb{Z}$ secreto.		**Passo 2:** Escolhe $n_B \in \mathbb{Z}$ secreto.
Passo 3: Calcula $Q_A = n_A P$		**Passo 3:** Calcula $Q_B = n_B P$
Passo 4: Envia Q_A para Serginho		**Passo 4:** Envia Q_B para Joãozinho. .
Recebe Q_B	Q_A e Q_B público	**Recebe Q_A**
Passo 5: Calcula $R = n_A Q_B$		**Passo 5:** Calcula $R = n_B Q_A$

Convém observar que

$$R = n_A\, Q_B = n_A\, n_B\, P = n_B\, Q_A$$

que Joãozinho e Serginho podem usar com uma chave para comunicar-se de forma privada através de uma cifra simétrica.

Exemplo: Joãozinho e Serginho decidem usar o método de Diffie-Hellman para curvas elípticas, para o seguinte caso, conforme a tabela abaixo:

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p = 3851 \gg 1$ primo grande $E\colon\ y^2 = x^3 + 324x + 1287$ uma curva elíptica sobre $\mathbb{Z}_p$ $P = (920,303) \in E(\mathbb{Z}_{3851})$	
Passo 2: Escolhe $n_A = 1194 \in \mathbb{Z}$ secreto.		**Passo 2:** Escolhe $n_B = 1759 \in \mathbb{Z}$ secreto.
Passo 3: Calcula $Q_A = n_A\, P = 1194\, P$ $= (2067, 2178)$		**Passo 3:** Calcula $Q_B = n_B\, P = 1759\, P$ $= (3684, 3125)$
Passo 4: Envia Q_A para Serginho		**Passo 4:** Envia Q_B para Joãozinho.
Recebe Q_B	Q_A e Q_B público	**Recebe Q_A**
Passo 5: Calcula $R = n_A Q_B$ $= 1194(3684,1242)$ $= (3347,1242)$		**Passo 5:** Calcula $R = n_B\, Q_A$ $= 1759(2067,2178)$ $= (3347,1242)$

Joãozinho e Serginho compartilharam o ponto secreto

$$R = (x_R,\ y_R) = (3347,\ 1242).$$

Com o objetivo de usar menos bits e tornar a comunicação menos pesada, eles podem descartar a coordenada y e enviar apenas o valor da primeira coordenada do ponto R, a saber: $x_R = 3347$, como sendo a chave secreta compartilhada.

Recebendo, um do outro, apenas a primeira coordenada, Joãozinho e Serginho devem calcular a coordenada y que falta. Neste momento se torna muito útil a seguinte proposição:

Proposição: Se p é um primo da forma $(4k - 1)$ e a equação $Y^2 \equiv a\ (mod\ p)$ admite solução, então $Y = a^{\frac{p+1}{4}}$ é uma solução dessa equação.

Prova: Se $a = 0$, não há o que mostrar.

Se $a \neq 0$ e g é uma raiz primitiva de $(\mathbb{Z}_p)^*$ então existe w tal que $Y \equiv g^w (mod\ p)$ e, consequentemente, $Y^2 \equiv g^{2w} \equiv a\ (mod\ p)$.

Note que $\frac{p+1}{4}$ é inteiro positivo, pois $p = 4k - 1$ para algum k inteiro positivo. Vamos mostrar que $Y = a^{\frac{p+1}{4}}$ satisfaz a nossa equação.

$$Y^2 = \left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} \equiv (g^{2w})^{\frac{p+1}{2}} (mod\ p)$$

$$\Rightarrow\ Y^2 = a^{\frac{p+1}{2}} \equiv g^{w(p+1)} (mod\ p)$$

$$\Rightarrow Y^2 = a^{\frac{p+1}{2}} \equiv g^{w(p-1)+2w} \equiv (g^w)^{p-1} \cdot g^{2w}\ (mod\ p)\ ,$$

Note que $(g^w)^{p-1} \equiv 1 (mod\ p)$ pelo P.T.F $g^{2w} \equiv a\ (mod\ p)$. Segue que

$$Y^2 = a^{\frac{p+1}{2}} \equiv a\ (mod\ p).$$

EXEMPLO: Vamos determinar uma solução para $Y^2 \equiv 6 (mod\ 19)$.. Note que 19 é um primo da forma 4k – 1, pois $4 \cdot 5 - 1 = 19$. Então, se existe solução para a nossa equação, $Y = 6^{\frac{19+1}{4}} = 6^5$ é solução. Podemos verificar que $Y = 6^5 \equiv 5 (mod\ 19) \Rightarrow Y^2 \equiv 25 \equiv 6 (mod\ 19)$.

Vamos fazer um exemplo com Joãozinho e Serginho enviando apenas a 1ª coordenada do ponto R.

Exemplo: Joãozinho e Serginho decidem usar o método de Diffie-Hellman para curvas elípticas, para o seguinte caso, conforme a tabela abaixo:

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p = 3851$ $E: \ y^2 = x^3 + 324x + 1287$ uma curva elíptica sobre $\mathbb{Z}_p$ $P = (920,303) \in E(\mathbb{Z}_{3851})$	
Passo 2: Escolhe $n_A = 2489 \in \mathbb{Z}$ secreto.		**Passo 2:** Escolhe $n_B = 2286 \in \mathbb{Z}$ secreto.
Passo 3: Calcula $Q_A = n_A P$ $= 2489 P$ $= (593, 719)$ $= (x_A, y_A)$		**Passo 3:** Calcula $Q_B = n_B P$ $= 2286 P$ $= (3681, 612)$ $= (x_B, y_B)$
Passo 4: Envia $x_A = 593$ para Serginho		**Passo 4:** Envia $x_B = 3681$ para Joãozinho.
Recebe $x_B = 3681$	x_A e x_B público	**Recebe $x_A = 593$**
Passo 5: Joãozinho Calcula $x_B = 3681$ Na equação de E $y_B^2 = x_B^3 + 324x_B$ $+1287$ $= 3681^3 + 324.3681$ $+1287$ $= 997 \in \mathbb{Z}_{3851}$		**Passo 5:** Serginho Calcula $x_A = 593$ Na equação de E $y_A^2 = x_A^3 + 324x_A$ $+1287$ $= 593^3 + 324.593$ $+1287$ $= 927 \in \mathbb{Z}_{3851}$

Como $b^{(p+1)/4}$ é uma raiz quadrada de b modulo p, segue que $y_B = 997^{(3851+1)/4}$ $= 997^{963}$ $\equiv 612\ mod\ 3851$		Como $b^{(p+1)/4}$ é uma raiz quadrada de b módulo p, segue que $y_B = 927^{(3851+1)/4}$ $= 927^{963}$ $\equiv 3132\ mod\ 3851$
Passo 6: Joãozinho encontra $\widetilde{Q_B} = (3681,612)$ que é o de Serginho. $Q_B = (3681,612)$		**Passo 6:** Serginho encontra $\widetilde{Q_A} = (593,3132)$ que não é o de Joãozinho. $Q_A = (593,719)$
Passo 7: Calcula $R_{AB} = n_A \widetilde{Q_B}$ $= 2489(3681,612)$ $= (509,1108)$		**Passo 7:** Calcula $R_{BA} = n_B\ \widetilde{Q_A}$ $= 2286\ (593,3132)$ $= (509,2743)$
Passo 8: Apesar de não ser o mesmo ponto, um é o simétrico do outro e a chave secreta compartilhada será a coordenada x que é a mesma para ambos os pontos $\boldsymbol{x = 509}$		**Passo 8:** Apesar de não ser o mesmo ponto, um é o simétrico do outro e a chave secreta compartilhada será a coordenada x que é a mesma para ambos os pontos $\boldsymbol{x = 509}$

4.3.2. SISTEMA DE CRIPTOGRAFIA COM CHAVE PÚBLICA ELGAMAL

É fácil construir um análogo ao ElGamal para o grupo das curvas elípticas sobre corpos finitos. Porém, teremos que supor que **a mensagem que Serginho deseja enviar para Joãozinho** é um ponto $M \in E(\mathbb{Z}_p)$ da curva elíptica onde o primo p e a curva elíptica E sobre $\mathbb{Z}_p$ são previamente fixados por um canal não seguro de comunicação.

Além disso, eles ainda compartilham um ponto $P \in E(\mathbb{Z}_p)$. Vamos descrever o método na tabela abaixo.

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p \gg 1$ primo grande E uma curva elíptica sobre $\mathbb{Z}_p$ P um ponto de $E(\mathbb{Z}_p)$	
Passo 2: Escolhe $n_A \in \mathbb{Z}$ secreto.		
Passo 3: Calcula $Q_A = n_A P$		
Passo 4: Envia Q_A para Serginho		
	Q_A público	**Recebe Q_A**

Serginho escolhe um inteiro k somente para codificar a mensagem e que será descartado após isto, conforme descrito na tabela a seguir:

Joãozinho	**Mônica**	**Serginho**
		Passo 5: Serginho escolhe $k \in \mathbb{Z}$ e calcula $R = kP$ $S = M + kQ_A$
		Passo 6: Envia para Joãozinho a seguinte mensagem (R, S)
Recebe (R, S)	(R, S) público	
Passo 7: Para decifrar a mensagem, Joãozinho calcula $S - n_A R$ $= (M + kQ_A) - n_A kP$ $= M + k(n_A P) - n_A kP$ $= M$		

Façamos outro exemplo, conforme tabela a seguir:

Joãozinho	**Mônica-(parâmetros Públicos)**	**Serginho**
	$p = 362, \quad P = (6, 730)$ $E: y^2 = x^3 + 14x + 19$	
Passo 2: Chave secreta: $n_A = 435$		
Passo 3: Joãozinho calcula $Q_A = n_A P = (932, 1204)$ e envia para Serginho		
	Q_A público	**Recebe Q_A**
		Passo 4: Serginho escolhe $k = 13$ e a mensagem $M = (2058, 3022)$ Calcula $R = kP = (1330{,}144)$ $S = M + kQ_A = (2940, 2636)$.
		Passo 5: Serginho envia para João a seguinte mensagem (R, S)
Recebe (R, S)	(R, S) público	
Passo 6: João calcula $S - n_A R =$ $= (M + kQ_A) - n_A kP$ $= M + k(n_A P) - n_A kP$ $= M = (2058{,}3022)$		

Como $R = (x_R, y_R)$ e $S = (x_S, y_S)$ são pontos de $E(\mathbb{Z}_p)$, Serginho pode enviar apenas as coordenadas (x_R, x_S) desses dois pontos e deixar que Joãozinho calcule as coordenadas y_R e y_S. No entanto, sabemos que Joãozinho pode obter com seus cálculos o simétrico do ponto R ou S, ou seja, $-R$ ou $-S$. É claro que se isso acontecer, ele não obtém a mensagem M. De fato, se Joãozinho encontrasse em seus cálculos $-R$ e S, **sua decodificação** seria:

$$S - n_A(-R) = (M + kQ_A) - n_A R = M + n_A\left(\underbrace{kP}_{R}\right) + n_A R = M + 2n_A R$$

Pergunta: Como Joãozinho e Serginho podem resolver esse problema?

Sabemos que

- $A = (x_A, y_A) \in E(\mathbb{Z}_p) \Rightarrow -A = (x_A, p - y_A)$

Deste modo, temos 2 possibilidades:

- Caso 1: $p - y_A < \frac{p}{2}$ e $y_A > \frac{p}{2}$
- Caso 2: $p - y_A > \frac{p}{2}$ e $y_A < \frac{p}{2}$

definindo δ_A como sendo um (bit extra) da seguinte forma:

- $\delta_A = 0 \ \ se \ \ 0 \leq y_A < \frac{p}{2}$
- $\delta_A = 1 \ \ se \ \ \frac{p}{2} < y_A < p$

Serginho pode resolver este problema enviando ($(x_R, \delta_R), (x_S, \delta_S)$),

possibilitando a Joãozinho determinar corretamente

$$R = (x_R, y_R) \quad \text{e} \quad S = (x_S, y_S)$$

e consequentemente descobrir a mensagem enviada por Serginho. Observe que para o funcionamento do método descrito no último exemplo, há a necessidade de que a mensagem M seja um ponto da curva elíptica E. **Isto nos leva a um questionamento natural:** Como associar mensagens de texto simples a pontos da curva elíptica? **Uma resposta possível seria a seguinte:** Associar aleatoriamente caracteres a pontos da curva.

Por outro lado, existe uma forma de fazer um análogo do ElGamal onde esse problema não aparece. Tal método foi sugerido por Menezes e Vanstone em um trabalho que reduzia o Problema do Logaritmo Discreto em Curvas Elípticas ($PLDCE$) para o problema em $\mathbb{Z}_p$.

No método de Menezes-Vanstone **não há a necessidade de que a mensagem seja um ponto da curva elíptica em questão**, porém a desvantagem desse sistema é

que as mensagens se tornam duas vezes maiores. A seguir, vamos apresentar a descrição desse método.

4.3.3. Variante de Menezes e Vanstone para ElGamal sobre Curvas elípticas

Iniciamos com uma curva elíptica E sobre $\mathbb{Z}_p$, um primo p grande, e um ponto $P \in E(\mathbb{Z}_p)$, que são previamente fixados por um canal não seguro de comunicação. Neste caso, a mensagem que Serginho enviará para Joãozinho será dada pelo par ordenado $M = (m_1; m_2)$, onde m_1 e $m_2 \in Z_p^*$ e M não é um ponto de $E(\mathbb{Z}_p)$.

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p \gg 1$ primo grande E uma curva elíptica sobre $\mathbb{Z}_p$ P um ponto de $E(\mathbb{Z}_p)$	
Passo 2: Escolhe $n_A \in \mathbb{Z}$ secreto.		
Passo 3: Calcula $Q_A = n_A P$		
Passo 4: Envia Q_A para Serginho		
	Q_A público	**Recebe Q_A**

Em seguida, Sergio codificará sua mensagem da seguinte maneira:

Joãozinho	**Mônica**	**Serginho**
		Passo 5: Escolhe $k \in \mathbb{Z}$ e calcula $R = kP$ $S = kQ_A = (x_S, y_S)$
		Passo 6: Calcula $C_1 \equiv x_S m_1 \mod p$ $C_2 = y_S m_2 \mod p$ A mensagem codificada enviada para João será a trinca a seguir (R, C_1, C_2)
Recebe (R, C_1, C_2)	(R, C_1, C_2) público	

Para decodificar a mensagem de Serginho, Joãozinho faz o seguinte:

Joãozinho	**Mônica** **(parâmetros Públicos)**	**Serginho**
Passo 7: Para decifrar a mensagem, João calcula $n_A R = n_A kP = kQ_A =$ $= S = (x_S, y_S)$ Em seguida, Joãozinho calcula $x_S^{-1} C_1 \equiv m_1 \ mod \ p$ $y_S^{-1} C_2 \equiv m_2 \ mod \ p$ obtendo a mensagem de Serginho: m_1 e m_2		

Exemplo: Serginho decide usar o método MV-ElGamal para enviar a Joãozinho a mensagem MCT, que para os dois significa Tomar o Caderno da Mônica. Tal mensagem será codificada na tabela ASCII (Código Padrão Americano para o Intercâmbio de Informação).

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

Por esta tabela, temos $M = 77, C = 67$ e $T = 84$. Como a mensagem deve ser enviada por um par ordenado, vamos escrever $M = (\mathrm{MC}, \mathrm{T}) = (m_1, m_2) = (7767,84)$.

Joãozinho	**Mônica - (parâmetros Públicos)**	**Serginho**
	$p = 2097421$ $P = (1355793,621792)$ $E: y^2 = x^3 + 67110x + 262147$	
Passo 2: Escolhe $n_A = 78771$ secreto.		
Passo 3: Calcula $Q_A = n_A P = (949594,812871)$		
Passo 4: Envia Q_A para Serginho.	Q_A público	**Recebe Q_A**
		Passo 5: Escolhe $k = 23358$ e calcula $R = kP = (1390038,1344654)$ $S = kQ_A = (x_S, y_S) = (647014,449701)$

Joãozinho	Mônica	Serginho
		Passo 6: Sergio calcula: $C_1 \equiv x_S m_1 = 647014 \cdot 7767 \equiv 2034443\ (mod\ 2097421)$ $C_2 \equiv y_S m_2 = 449701 \cdot 84 \equiv 21306\ mod\ 2097421$ A mensagem codificada e enviada para João será a trinca (R, C_1, C_2) onde $R = (1390038,1344654)$, $C_1 = 2034443$ $C_2 = 21306$
Recebe (R, C_1, C_2)	(R, C_1, C_2) público	
Passo 7: Para decifrar, Joãozinho calcula $n_A R = n_A kP = kQ_A = S = (x_S, y_S)$ Em seguida, calcula $x_S^{-1} C_1 \equiv m_1 = 7767\ (mod\ 2097421)$ $y_S^{-1} C_2 \equiv m_2 = 84\ (mod\ 2097421)$ Obtendo a mensagem $(7767,84)$.		

Como o grupo formado pelos pontos de uma curva elíptica tem uma estrutura diferente dos grupos normalmente utilizados em outros sistemas de criptografia, os ataques ao logaritmo discreto não funcionam tão bem sobre curvas elípticas. Isto acarreta uma diminuição do tamanho da chave usada sem perda de segurança, permitindo a utilização de um algoritmo mais rápido e mais leve.

Por essas razões, a criptografia sobre curvas elípticas está se tornando a principal candidata a substituir o sistema RSA, que atualmente é o sistema mais utilizado.

Na tabela a seguir podemos ver a quantidade de bits utilizada na chave com o mesmo grau de segurança.

ECC	RSA	Razão ECC:RSA
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

Tamanho das chaves em bits.

Atualmente a própria RSA Security está prosseguindo na validação da segurança da criptografia das curvas elípticas, o que indica que esta deve substituir o sistema RSA.

CAPÍTULO 5

Atividades relativas ao Capitulo 1

1) Nesta atividade, a turma deve ser dividida em três grupos: Grupo Remetente, Grupo Destinatário e Grupo Decifrador.

Grupo Remetente:

- Cria uma cifra, baseada no método de César, deslocando cada letra um certo número de casas para a direita.

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

- Codifica uma mensagem e a envia para o Grupo Destinatário.

Grupo Destinatário:

- Decodifica a mensagem com o conhecimento da cifra criada pelo Grupo Remetente.

Grupo Decifrador:

- Intercepta a mensagem codificada.
- Tenta decifrar a mensagem sem o conhecimento da cifra.

Depois os alunos podem mudar de grupos para executarem outras funções.

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

2) Codifique a frase “A Matemática e a criptografia são fascinantes”
3) Decodifique a frase “VGYZICQJQLFYKNQCALCVSZLYKILHVQYLIK”

4) Utilizando o método A cifra Indecifravel - decifre a frase "NUCAPIVAVSNICIEO" sabendo que a palavra-chave é JACOBI.

	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

5) Nesta atividade, a turma deve ser dividida em grupos. Um grupo será chamado de transmissor e os demais de receptores. O grupo transmissor divulgará uma palavra chave e, utilizando o método da cifra indecifrável, deverá codificar uma mensagem e enviá-la aos grupos receptores. O primeiro grupo receptor que decodificar a mensagem ganhará um ponto. A atividade continua trocando, a cada rodada, o grupo transmissor.

Atividades relativas ao Capítulo 2

1) Prove, usando o princípio de indução, que $1+2+3+...+n = \frac{n(n+1)}{2}$.
2) Determine o resto de 2^{30} por 17. Sugestão: note que $2^4 \equiv -1 \pmod{17}$.
3) Ache os elementos invertíveis de:
   a) $\mathbb{Z}_6$
   b) $\mathbb{Z}_7$

4) Mostre que $52^{280} \equiv 1 \pmod{29}$. Sugestão: Use o pequeno teorema de Fermat.
5) Verifique se o subconjunto M $=\{\bar{1}, \bar{5}\}$ de $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ é um grupo com relação à multiplicação.
6) Mostre que existem infinitos primos da forma $6k + 5$.

Atividades relativas ao Capitulo 3

1) Preencha a tabela a seguir para obter o cálculo de 3^{157} módulo 100.

i	$divisão$	$quociente\ Q_i$	$resto = A_i$	3^{2^i} módulo 100	R_i
0	$157 \div 2$		1		
1	78		0		
2	39		1		
3	19		1		
4	9		1		
5	4		0		
6	2		0		
7	1		1		

2) A observação da página 40 mostra um método para obter um inverso módulo p, baseado no pequeno teorema de Fermat: $a^{p-2} \equiv a^{-1}\ (mod\ p)$.
A partir desse método, utilize a calculadora do Windows para calcular o inverso de 2564 módulo131. OBS: Nesta calculadora há a função MOD que fornece o resto da divisão entre dois números.

3) Utilize a função MOD da calculadora do Windows para calcular o logaritmo de 395 na base 627 em Z_{941}.

Atividades relativas ao Capitulo 4

1) Considere a curva elíptica $y^2 = x^3 + 4x + 4$ em R e os pontos P=(1,3) e Q=(0,2) pertencentes à essa curva. Determine o ponto M = P + Q, usando a definição de soma de pontos de uma curva elíptica.

2) Considere a curva elíptica $y^2 = x^3 + 4x + 4$ em Z_7 e os pontos P=(1,3) e Q=(0,2) pertencentes à essa curva. Determine o ponto M = P + Q, usando a definição de soma de pontos de uma curva elíptica.

CONCLUSÃO

Esse trabalho apresenta resumidamente o desenvolvimento da Criptografia até os dias atuais, mostrando como a luta entre criadores e decifradores de códigos contribuiu para o desenvolvimento da Matemática e da tecnologia.

A criptografia, além de ser um assunto interessante e atual, exibe toda a criatividade e inteligência do homem para se comunicar de forma sigilosa. A teoria matemática apresentada nesse texto tem o propósito de explicar o funcionamento dessa área tão importante para as comunicações seguras, como transferências bancárias, informações diplomáticas etc.. Todos esses fatores servem como motivação para o estudo da Matemática e de áreas afins.

No último capítulo, foram propostas algumas atividades relacionadas aos assuntos abordados nesse texto. Algumas dessas atividades exigem um bom entendimento do conteúdo matemático explorado no decorrer do trabalho, sendo mais adequadas a alunos do ensino médio; enquanto outras são verdadeiras "brincadeiras" que estimulam a criatividade, o raciocínio e o trabalho em grupo, podendo ser realizadas inclusive por alunos do ensino fundamental.

BIBLIOGRAFIA

[1] Ribenboim, P. Números primos-Velhos Mistérios e Novos Recordes, Coleção Matemática 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