INSTITUTO TECNOLÓGICO DE AERONÁUTICA

Thiago Marques Esteves Póvoa

Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas

Trabalho de Graduação
2010

Civil-Aeronáutica

CDU 007:51

Thiago Marques Esteves Póvoa

Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas

Orientadora
Prof.ª Drª Tânia Nunes Rabello

Divisão de Engenharia Civil

SÃO JOSÉ DOS CAMPOS
INSTITUTO TECNOLÓGICO DE AERONÁUTICA

2010

Dados Internacionais de Catalogação-na-Publicação (CIP)
Divisão de Informação e Documentação

Póvoa, Thiago Marques Esteves
Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas / Thiago Marques Esteves Póvoa.
São José dos Campos, 2010.
86f

Trabalho de Graduação – Divisão de Engenharia Civil – Instituto Tecnológico de Aeronáutica, 2010. Orientadora: Prof.ª Drª Tânia Nunes Rabello.

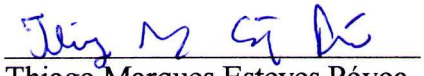
1. Criptografia de chave pública. 2. Algoritmos. 3. Curvas elípticas. I. Departamento de Ciência e Tecnologia Aeroespacial. Instituto Tecnológico de Aeronáutica. Divisão de Engenharia Civil. II. Título

REFERÊNCIA BIBLIOGRÁFICA

PÓVOA, Thiago Marques Esteves. **Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas**. 2010. 86f. Trabalho de Conclusão de Curso. (Graduação) – Instituto Tecnológico de Aeronáutica, São José dos Campos.

CESSÃO DE DIREITOS

NOME DO AUTOR: Thiago Marques Esteves Póvoa
TÍTULO DO TRABALHO: Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas.
TIPO DO TRABALHO/ANO: Graduação / 2010



Thiago Marques Esteves Póvoa
CND 04, Lote 03, Apt. 204, Taguatinga Norte
72120-025 – Distrito Federal – DF

ESTUDO DOS ALGORITMOS CRIPTOGRÁFICOS ASSIMÉTRICOS RSA E DE CURVAS ELÍPTICAS

Essa publicação foi aceita como Relatório Final de Trabalho de Graduação

Thiago Marques Esteves Póvoa, Asp. Of.
Autor

Profª. Drª Tânia Nunes Rabello - ITA
Orientadora

Prof. Dr Eliseu Lucena Neto
Coordenador do Curso de Engenharia Civil-Aeronáutica

São José dos Campos, 18 de novembro de 2010

Dedico este Trabalho aos Pet Shop Boys, por terem sido fiéis companheiros nas infinitas noites passadas em claro, absorto em pensamentos repletos de complexidade. Dedico também este Trabalho a Évariste Galois, por ter proporcionado à humanidade sua mais brilhante e criativa teoria matemática.

Agradecimentos

Agradeço a todos os seres que já passaram pela minha existência, animados e inanimados, visíveis e invisíveis, por contribuírem para a formação da singularíssima pessoa que me tornei nestes vinte e três anos de vida. Que todos possam ser felizes.

"Amar, ser verdadeiro, deve custar – deve ser árduo – deve esvaziar-nos do ego."

(Madre Tereza de Calcutá)

Resumo

Na sociedade moderna, com o advento da internet, há um fluxo intenso de informações dos mais variados tipos. Esse fluxo de comunicação se dá entre um número enorme de entidades diferentes, desde grandes corporações e órgãos governamentais até simples usuários de serviços de e-mail ou *internet banking*. Muitas vezes, as informações que se deseja transmitir são de caráter confidencial, sendo assim necessário que se apliquem algumas técnicas para tornar a mensagem secreta no processo de transmissão. Diante da crescente necessidade de protocolos criptográficos para a encriptação de mensagens dos mais variados tipos e tamanhos, surge em todo o mundo uma enorme corrente de pesquisas matemáticas e computacionais dedicada ao estudo dos algoritmos criptográficos já conhecidos e empenhada no desenvolvimento de novos modelos. Este Trabalho de Graduação pautou-se no estudo de dois algoritmos amplamente utilizados na atualidade em processos de criptografia assimétrica (também denominada criptografia de chave pública): O modelo RSA, e o modelo criptográfico baseado nas propriedades algébricas de Curvas Elípticas sobre corpos finitos. Ao longo do Trabalho, procurou-se tratar cada algoritmo de maneira específica, abordando sua metodologia de funcionamento, propriedades matemáticas relacionadas, tipos de aplicações, bem como sua presença nos protocolos criptográficos utilizados na atualidade. Por fim, procurou-se estabelecer um paralelo entre ambos, apontando assim algumas vantagens dos modelos criptográficos de Curvas Elípticas frente ao modelo RSA, tais como a possibilidade de uma escolha mais diversificada dos parâmetros necessários ao funcionamento do algoritmo (corpos finitos, Curvas Elípticas e pontos pertencentes à Curva) e também o caráter bastante reduzido do tamanho das chaves necessárias para que sejam mantidos níveis de segurança semelhantes aos alcançados quando se utiliza o modelo RSA. Vale ressaltar que este Trabalho preocupou-se com uma abordagem matemática dos algoritmos, de forma que seus aspectos computacionais não foram tratados de maneira específica.

Abstract

In modern society, with the advent of the Internet, there is a heavy flow of information of all kinds. This communication flow is between a huge number of different entities, from large corporations and governments to individual users of services of e-mail or internet banking. Often, information is being transmitted are confidential, therefore is necessary to apply some techniques to make the message secret in the transmission process. Given the growing need for cryptographic protocols for encryption of messages of all kinds and sizes, all over the world comes a huge stream of research devoted to mathematical and computational study of cryptographic algorithms known and committed to developing new models. This graduate work was supported by a study of two widely used algorithms currently in the process of asymmetric encryption (also called public key cryptography): The RSA model and the model based on cryptographic algebraic properties of Elliptic Curves over finite fields. Throughout the work, we tried to treat each algorithm in a specific manner, approaching its working methodology, mathematical properties related, types of applications, and their presence in cryptographic protocols in use today. Finally, we tried to draw parallels between them, pointing out some advantages like models of Elliptic Curve Cryptographic front of the RSA model, such as the possibility of a wider choice of parameters necessary for operation of the algorithm (finite fields, Elliptic Curves and points belonging to curve) and also the character greatly reduced of the sizes of the keys necessary to ensure that safety levels are kept similar to those achieved when using the RSA model. It is noteworthy that this work was concerned with a mathematical approach of the algorithms, so that its computational aspects have not been addressed specifically.

Lista de Figuras

Lista de Tabelas

Lista de Equações

Sumário

1 Introdução

1.1 Organização do Trabalho

Este trabalho abordará as metodologias de funcionamento dos algoritmos de criptografia assimétrica RSA e de Curvas Elípticas. Essa abordagem será feita em capítulos. No capítulo 1, será dada uma introdução a alguns temas criptográficos importantes, como criptografia simétrica, assimétrica e assinatura digital. No capítulo 2, será feito um estudo do algoritmo RSA, tratando das suas particularidades, sua metodologia de funcionamento e suas aplicações. O mesmo será feito para o algoritmo de Curvas Elípticas, no capítulo 3. Por fim, no capítulo 4 será feita uma pequena análise comparativa entre os dois modelos criptográficos, ressaltando-se as vantagens verificadas na utilização do algoritmo de Curvas Elípticas comparativamente ao modelo RSA.

1.2 Fundamentos de Criptografia

A criptografia, um ramo do conhecimento humano que vem se desenvolvendo desde a antiguidade clássica, passando pelas eras medievais e pela criação das primeiras máquinas de codificação e decodificação, culminando nos modernos processos de criptografia quântica estudados na atualidade, sempre se mostrou fundamental para a transmissão de informações das mais diversas naturezas. A enorme gama de atividade criptográfica existente na atualidade em bancos, em grandes corporações, em atividades diplomáticas e governamentais, juntamente com a crescente necessidade de uma maior segurança nos processos de transmissão de informação em organizações de pequeno porte, sejam empresas ou órgãos públicos, motiva um constante crescimento nas pesquisas realizadas acerca dos mais diversos algoritmos criptográficos e suas implementações computacionais. Devido aos avanços crescentes da computação, as técnicas criptográficas tornam-se frágeis num intervalo de tempo cada vez menor. Dessa forma, é sempre necessário que aspectos matemáticos relacionados principalmente à

segurança e à eficiência dos algoritmos sejam amplamente estudados (Póvoa, et al., 2008).

A palavra criptografia deriva do grego "*cryptos*", que significa oculto, secreto. Existem registros históricos acerca da utilização de algoritmos criptográficos desde a antiguidade clássica, porém os métodos utilizados nesse período eram bastante rudimentares se comparados aos modernos algoritmos existentes na atualidade. Tais métodos, na sua grande maioria, baseavam-se na "translação" das letras do alfabeto, de forma que as letras formadoras da palavra a ser criptografada fossem substituídas por outras letras do alfabeto (ou quaisquer outros símbolos), de uma maneira ordenada e previamente conhecida. Inclusive, o primeiro exemplo de código secreto de que se tem notícia foi o código utilizado por Júlio César, para se comunicar com seus generais em combates pela Europa, por volta do século I a.C. (Coutinho, 2000). Porém, tais códigos, baseados na substituição sistemática de uma letra por outra em seu lugar, são extremamente simples de serem quebrados mediante processos computacionais. Para a maioria desses códigos, uma simples contagem de frequência da ocorrência de cada uma das letras do alfabeto em um determinado idioma é suficiente para se estabelecer um "alfabeto posicional paralelo", em que cada letra está relacionada com sua correspondente no alfabeto convencional. Dessa forma, comparando-se as frequências das letras do alfabeto convencional com as frequências observadas na mensagem a ser decifrada (desde que o tamanho da mensagem seja grande o suficiente para que os valores de frequência observados possam ser considerados estatisticamente estabilizados), pode-se estabelecer a relação entre as posições das letras nos dois alfabetos. Esse processo foi utilizado pelo linguista francês Jean-François Champollion para decifrar o significado dos hieróglifos egípcios.

Ao longo dos anos, os processos criptográficos sofreram melhorias, tornando-se cada vez mais complexos e seguros. Na atualidade, a utilização da criptografia é bastante intensa, principalmente em segmentos que utilizam a internet para a troca de informações. Sempre que um usuário recebe ou envia ao banco alguma informação sobre sua conta bancária pela internet, é necessário que essa informação esteja protegida contra a leitura de pessoas indesejadas. Por isso, toda troca de informação bancária entre cliente e banco realizada pela internet é feita de maneira criptografada. Há também necessidade de verificação da autenticidade do emissor da informação, isto é, é necessário que se tenha certeza sobre a identidade do emissor da mensagem. Um método bastante intuitivo para que se possa caracterizar um emissor conhecido é a

utilização de uma “assinatura” na mensagem. Essa “assinatura” funciona como uma prova de que realmente se trata do emissor legítimo da mensagem, pois se supõe que nenhuma outra entidade estranha seja capaz de “falsificar” a assinatura do emissor autêntico. Como a troca de mensagens ocorre de uma maneira eletrônica, ao longo dos anos foi necessário se desenvolver um processo de “assinatura eletrônica”, também conhecida como “assinatura digital”. O desenvolvimento dos algoritmos de assinatura digital, bem como dos próprios algoritmos de criptografia de mensagens, são amplamente estudados na atualidade, principalmente seus aspectos matemáticos e computacionais. Este trabalho se propõe a esboçar aspectos, principalmente matemáticos, de dois conhecidos algoritmos da atualidade: o RSA e o algoritmo baseado em Curvas Elípticas.

De maneira geral, no campo da criptografia, há dois modelos básicos de algoritmo: os chamados modelos simétricos e os chamados modelos assimétricos. A criptografia simétrica é um tipo de processo criptográfico que se baseia na utilização de uma chave secreta comum entre emissor e receptor para a troca de mensagens. Dessa forma, toda a segurança do processo reside no caráter secreto da chave. Esse tipo de processo criptográfico é, de maneira geral, relativamente simples de ser implementado computacionalmente, não exigindo níveis muito altos de capacidade de processamento. Porém, esse tipo de abordagem criptográfica apresenta uma enorme fraqueza, pois uma vez que uma entidade estranha descubra a chave secreta e consiga interceptar a troca de mensagens, toda a segurança do algoritmo é perdida. Outra característica do modelo criptográfico simétrico é o fato de haver a necessidade de um compartilhamento de chaves secretas entre o emissor e o receptor da mensagem, torna-se imprescindível que, antes de se iniciar o processo de troca de mensagens criptografadas, haja comunicação entre emissor e receptor por meio de um canal seguro para que se estabeleça uma chave secreta comum entre ambos. Nem sempre é possível estabelecer essa comunicação de maneira segura, tornando assim o processo de transmissão das chaves relativamente comprometido. Este trabalho de graduação não abordará processos de criptografia simétrica. Para uma abordagem mais específica, podem ser consultados (Stinson, 2002), (Trappe, et al., 2002), (Tilborg, 2000) e (Póvoa, et al., 2008). A **Figura 1** ilustra o processo de troca de informação utilizando-se um algoritmo criptográfico simétrico.

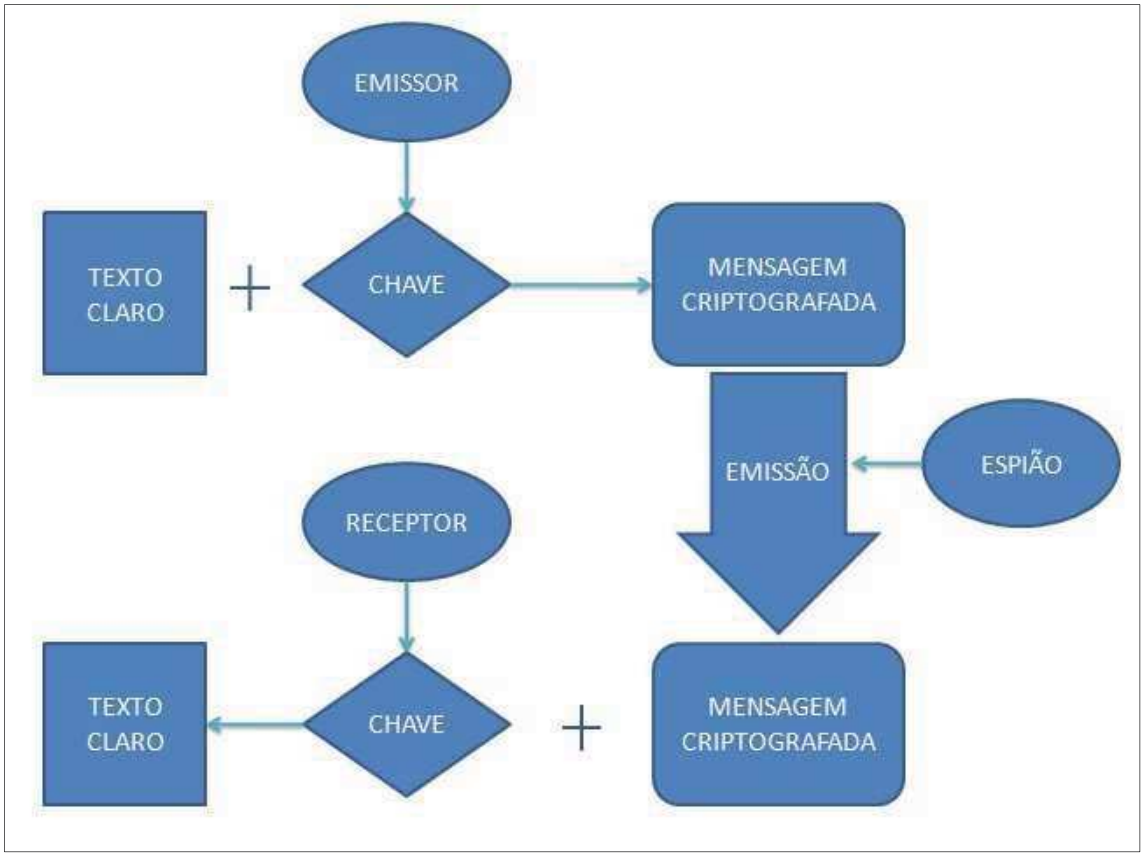


Figura 1 - Processo de Criptografia Simétrica

Em meio a esse universo de desconfiança na troca de informações por canais inseguros, surgiu a criptografia assimétrica, que consiste em um processo criptográfico em que não há a necessidade de compartilhamento de uma chave secreta entre emissor e receptor. No ano de 1976, W. Diffie e M.E. Hellman, da Universidade de Stanford, e, de maneira independente, R.C. Merkle, da Universidade da Califórnia, introduziram o conceito de criptografia assimétrica, também denominada criptografia de chave pública. Neste processo, não havia a necessidade de um compartilhamento prévio de chaves entre emissor e receptor. Por meio de um processo de exponenciação realizado em um corpo finito, era possível que, sem que houvesse qualquer comunicação secreta entre emissor e receptor, ambos obtivessem um mesmo número como resultado da exponenciação, e este número poderia ser então utilizado como chave secreta entre ambos. Esse método ficou conhecido como *The Diffie-Hellman Key Exchange System* (Tilborg, 2000). A partir daquele momento, não se necessitava mais de um canal seguro para se combinar a chave secreta entre emissor e receptor. Posteriormente, outros modelos de algoritmo criptográfico assimétrico foram desenvolvidos, utilizando-se a ideia de troca de mensagens criptografadas com segurança sem a

necessidade de comunicação direta entre as partes. Na seção 2.3, será introduzido o modelo criptográfico assimétrico RSA, que se baseia na intratabilidade computacional do problema da fatoração de inteiros grandes, e na seção 3.3.2, será apresentado o conceito de Problema do Logaritmo Discreto, no qual se baseia o funcionamento do algoritmo de Diffie e Hellman e também do algoritmo criptográfico baseado em Curvas Elípticas sobre corpos finitos.

O surgimento dos modelos criptográficos assimétricos revolucionou a utilização criptográfica conhecida até aquele momento, pois o conceito de segurança dos algoritmos de criptografia assimétrica é bastante diferente do conceito utilizado nos algoritmos de criptografia simétrica. Enquanto na criptografia simétrica a segurança do processo reside na chave secreta, a força dos algoritmos de criptografia assimétrica não está no caráter secreto da chave, e sim nas limitações computacionais para se realizar certos tipos de operações matemáticas em um tempo reduzido. Isto é, não se conhecem algoritmos de complexidade polinomial para o tratamento dos problemas matemáticos envolvidos nos processos de criptografia assimétrica (fatoração de inteiros, no caso do algoritmo RSA, e obtenção do logaritmo discreto, no caso do algoritmo de Curvas Elípticas). Os algoritmos criptográficos assimétricos utilizam, em conjunto, os conceitos de chave pública e chave privada. Cada uma das partes envolvidas no processo de troca de informação criptografada possui um par de chaves, uma pública e outra privada. Para criptografar uma mensagem, o emissor precisa conhecer somente a chave pública do receptor. Assim, o emissor criptografa a mensagem utilizando a chave pública do receptor e a envia. O receptor utiliza a sua chave privada para descriptografá-la. Dessa forma, caso a mensagem seja interceptada por uma entidade estranha, mesmo que a chave pública do receptor seja conhecida, somente é possível descriptografar a mensagem com a sua chave privada, que não foi compartilhada em momento algum do processo. Somente a chave privada do receptor pode descriptografar uma mensagem que foi criptografada utilizando-se a sua chave pública. Daí resulta toda a segurança do processo, pois não há a necessidade de qualquer troca de chaves por meio de canais inseguros. A **Figura 2** ilustra o processo de troca de informação utilizando-se um algoritmo criptográfico assimétrico.

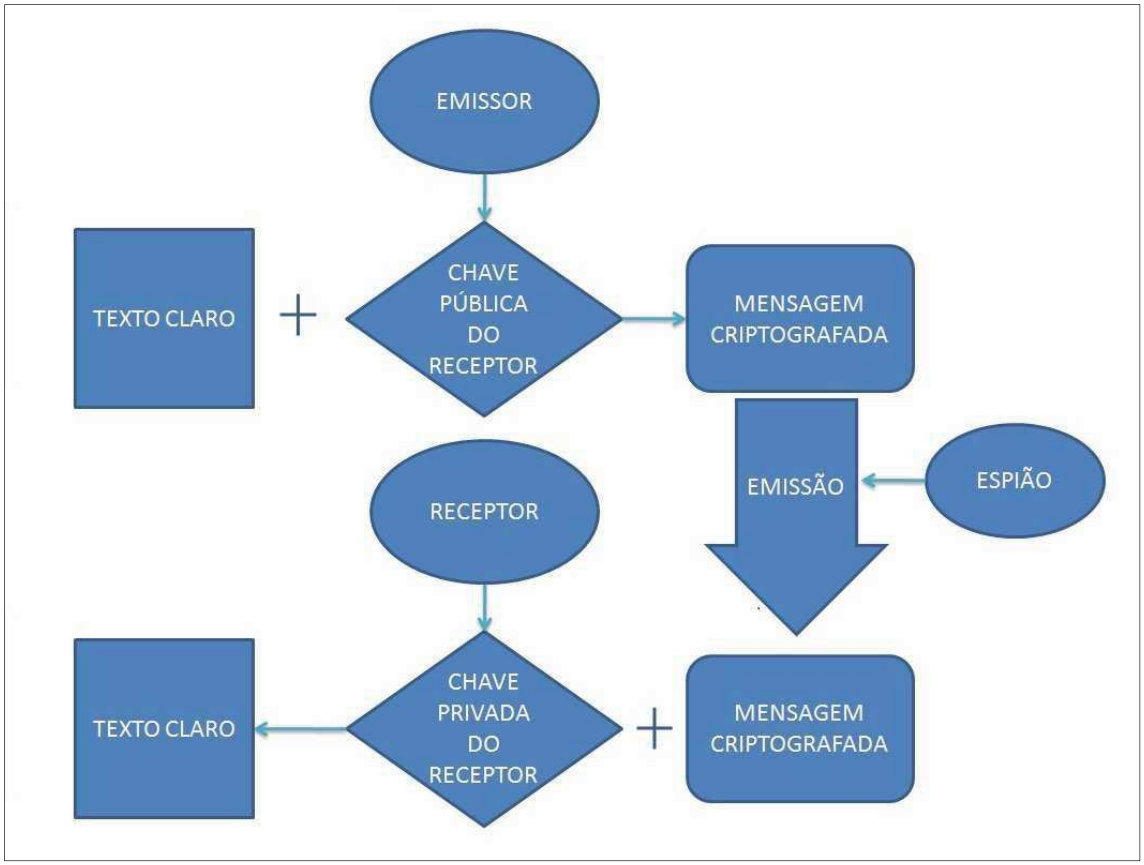


Figura 2 - Processo de Criptografia Assimétrica

Em uma abordagem mais rigorosa, pode-se observar que, de posse da chave pública do receptor, é matematicamente possível se obter a sua chave privada, pois ambas estão matematicamente relacionadas. Porém, os algoritmos criptográficos assimétricos utilizam metodologias específicas para que, com a capacidade computacional disponível atualmente, torna-se praticamente impossível obter uma chave privada a partir de uma chave pública. Os algoritmos criptográficos assimétricos utilizam algumas propriedades de funções matemáticas específicas, para que o conhecimento da chave pública não permita a dedução da chave privada por um possível interceptador da mensagem. Essas funções matemáticas são denominadas "funções de uma única via" (Aguiar, 2008), pois apresentam uma operação matemática relativamente simples de ser implementada, porém sua operação inversa mostra-se extremamente custosa computacionalmente. Mais detalhes acerca da segurança de algoritmos criptográficos assimétricos serão apresentados ao longo do texto.

1.3 Assinatura Digital

Quando uma análise mais criteriosa do modelo criptográfico assimétrico é realizada, surge, com bastante naturalidade, um questionamento sobre a autenticidade do emissor da mensagem. Isso ocorre pois, como o receptor deve divulgar sua chave pública por meio de um canal aberto, é possível que uma entidade estranha utilize essa chave para criptografar e enviar uma mensagem ao receptor, como se se tratasse do emissor real. Em outras palavras, uma entidade estranha qualquer pode "fingir" ser o emissor conhecido pelo receptor, e enviar mensagens em nome daquele. Há, porém, uma metodologia, denominada Assinatura Digital, utilizada nos processos criptográficos assimétricos, para se garantir a autenticidade do emissor da mensagem. Em linhas gerais, o processo consiste em o emissor "assinar" a mensagem utilizando para isso uma característica que só ele conheça. Ora, mas no processo de criptografia assimétrica há uma característica que só o emissor conhece, trata-se da sua própria chave privada, que não é divulgada em momento algum. Dessa forma, o emissor utiliza a sua chave privada para assinar a mensagem, de forma que somente o correspondente matemático daquela chave, isto é, a sua chave pública, poderá descriptografá-la. Porém, caso o emissor utilize a sua chave privada para assinar a própria mensagem, qualquer entidade com o conhecimento de sua chave pública poderia facilmente descriptografar a mensagem e ler seu conteúdo. Se a mensagem possui caráter secreto, isso não é desejável. Nesses casos, o emissor não deve assinar a própria mensagem secreta com a sua chave privada, mas sim algum outro tipo de mensagem, que possa ser obtida facilmente a partir da mensagem secreta original, e cujo conteúdo possa ser tornado público sem prejuízo ao caráter secreto da mensagem. Em outras palavras, é necessário que se assine uma espécie de "resumo" da mensagem original, que, caso interceptado por uma entidade estranha, não possa ser lido sem o conhecimento da mensagem original completa. Também é necessário que esse resumo possa ser facilmente gerado pelo receptor a partir da mensagem completa, para que este possa comparar o resumo gerado por ele com o resumo enviado assinado pelo emissor, verificando assim a autenticidade da mensagem. Esse tipo de resumo especial utilizado em processos de Assinatura Digital é denominado *Hash*, e há vários algoritmos conhecidos para a sua geração disponíveis no mercado. Além do caráter secreto do *Hash*, este tipo de resumo deve possuir também uma série de características relacionadas à segurança da mensagem, para que não seja possível obter a mensagem original a partir do seu *Hash*.

Este Trabalho não abordará a metodologia de funcionamento dos algoritmos geradores de *Hash*.

Devido às limitações de escopo da teoria criptográfica abordada, será apresentada, em caráter meramente ilustrativo do processo, uma hipotética troca de mensagens a partir de um modelo de Assinatura Digital sem a utilização de um *Hash*. Dessa forma, apenas a título de ilustração do processo, apresentar-se-á um protocolo em que o emissor assina a própria mensagem (e não o seu *Hash*), possibilitando assim que qualquer entidade que conheça a sua chave pública possa verificar a autenticidade da sua assinatura. Assim, faz-se a ressalva de que tal método nunca deve ser utilizado quando a mensagem possui caráter secreto, e o mesmo está sendo utilizado dessa maneira apenas como exemplo ilustrativo de um caso simples. Para uma abordagem da utilização de protocolos de Assinatura Digital utilizando-se algoritmos geradores de *Hash*, podem ser consultados (Stinson, 2002) e (Tilborg, 2000).

Portanto, em um processo de troca de mensagens utilizando-se um algoritmo criptográfico assimétrico, o emissor envia ao receptor duas mensagens criptografadas, uma utilizando a chave pública do receptor, e outra utilizando a sua própria chave privada. O receptor utiliza a sua chave privada para descriptografar a primeira mensagem e ler seu conteúdo. Porém, ainda resta dúvida a respeito da autenticidade do emissor. Então, o receptor utiliza a chave pública da entidade que ele supõe ser a emissora e descriptografa a segunda mensagem (na prática, descriptografa o seu *Hash*). Caso o emissor seja autêntico, a chave pública utilizada pelo receptor para descriptografar a segunda mensagem estará correta, e haverá uma coincidência entre as duas mensagens descriptografadas. Caso o emissor não seja autêntico, a chave pública utilizada pelo receptor para descriptografar a segunda mensagem não estará correta, e consequentemente as duas mensagens não serão iguais. Como se supõe que somente o emissor autêntico conhece sua chave privada, caso as duas mensagens descriptografadas não sejam idênticas, o receptor conclui que a mensagem não é autêntica. Dessa forma, garantem-se tanto a integridade da mensagem (pois caso ela tenha sido alterada por uma entidade estranha, essa entidade não poderá assiná-la como o emissor autêntico) quanto a autenticidade do emissor, pois só ele poderia assiná-la com sua chave privada. A **Figura 3** ilustra o processo de Assinatura Digital.

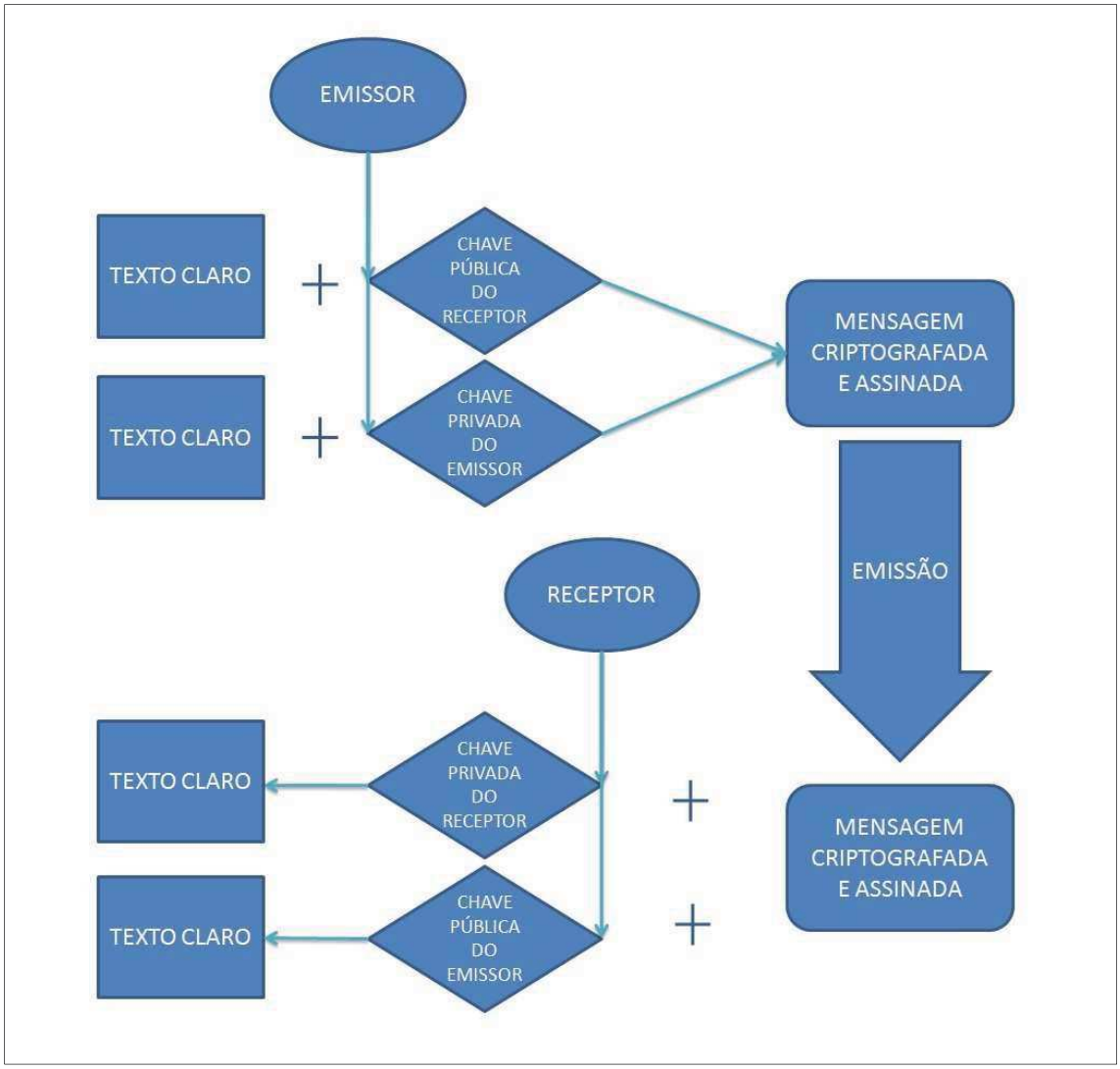


Figura 3 - Processo de Assinatura Digital

A metodologia de funcionamento dos algoritmos de Assinatura Digital será abordada com mais detalhes ao longo do texto, quando forem explicitados os processos de funcionamento dos algoritmos RSA e de Curvas Elípticas.

2 Algoritmo RSA

2.1 Histórico

No ano de 1976, Diffie e Hellman introduziram no universo criptográfico existente àquela época o conceito de criptografia de chave pública, também chamada de criptografia assimétrica. As ideias revolucionárias divulgadas pela dupla se espalharam por todo o mundo, e, em 1978, dois anos mais tarde, três pesquisadores do Massachussets Institute of Technology (M.I.T.) divulgaram um código, denominado RSA, cuja metodologia de funcionamento também se baseava no conceito de criptografia assimétrica. Esse algoritmo tornou-se mundialmente conhecido rapidamente, e começou a ser utilizado como padrão mundial para troca de informações por meio de canais inseguros, sendo amplamente utilizado principalmente em transações pela internet. Grande parte da troca de informações bancárias via internet na atualidade se dá por meio da utilização de protocolos que se baseiam no algoritmo RSA. A sigla RSA provém dos nomes dos autores do algoritmo: R. L. Rivest, A. Shamir e L. Adleman. O algoritmo RSA se baseia na dificuldade computacional para se fatorar números inteiros muito grandes, utilizando-se a capacidade de processamento atual. Não se conhecem algoritmos eficientes o suficiente para se fatorar esses números em um tempo reduzido, o que torna a quebra do RSA um tanto quanto improvável (mas não impossível).

2.2 Definições

Primeiramente, é necessário entender o processo de geração dos pares de chaves pública e privada, tanto da entidade emissora quanto da entidade receptora, de maneira totalmente independente. Cada uma das entidades escolhe secretamente dois números primos grandes p e q, e efetua a multiplicação $n = p.q$ dos mesmos. Em seguida, calcula-se o valor da função fi de Euler do número n:

$$\phi(n) = (p\text{-}1).(q\text{-}1)$$

Equação 1 - Função Fi de Euler para $n = p.q$

Conhecendo-se o valor de $\phi(n)$, escolhe-se um número e, de forma que $1 < e < \phi(n)$, e também MDC $(e, \phi(n)) = 1$. A necessidade de e e $\phi(n)$ serem primos entre si é decorrência imediata do próximo passo, que consiste em encontrar o inverso multiplicativo de e modulo $\phi(n)$. Por meio do Algoritmo de Euclides Estendido, encontra-se d, tal que $d.e \equiv 1 \ (mod\ \phi(n))$, isto é:

$$d = e^{-1} \text{ modulo } \phi(n)$$

Equação 2 - Inverso Multiplicativo de e modulo $\phi(n)$

A chave pública consiste no par de números (n,e), e a chave privada em (n,d). Publica-se a chave pública em qualquer tipo de canal, seja ele seguro ou não, e utiliza-se a chave privada para se decodificarem as mensagens enviadas por meio da chave pública.

2.3 Funcionamento do Algoritmo RSA

Para efeito de ilustração do método de funcionamento do Algoritmo RSA, supõe-se que uma entidade B deseja enviar uma mensagem criptografada para uma entidade A. É necessário, primeiramente, converter o texto a ser codificado em um bloco numérico m. Essa conversão é bastante simples, podendo ser utilizado, por exemplo, o padrão ASCII para a conversão. De posse de m, a entidade B adquire a chave pública (n,e) da entidade A, calcula $c \equiv m^e \ (mod\ n)$ e envia c para A. Para decodificá-la, A calcula $m \equiv c^d \ (mod\ n)$, obtendo assim a mensagem original enviada por B. Isso ocorre como consequência direta do Teorema de Euler:

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

Equação 3 - Teorema de Euler

Dessa forma, como $d.e \equiv 1 \ (mod\ \phi(n))$ e $c \equiv m^e \ (mod\ n)$, tem-se:

$c^d \equiv (m^e)^d \ (mod\ n)$

Mas:

$d.e \equiv 1 \ (mod\ \phi(n))$,

então existe um inteiro positivo k, tal que $d.e = k.\phi(n) + 1$. Assim:

$c^d \equiv m^{k.\phi(n)+1} \ (mod\ n) \ \Rightarrow$

$c^d \equiv (m^{\phi(n)})^k .m \ (mod\ n)$

Mas:

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

Portanto:

$c^d \equiv 1^k .m \ (mod\ n) \Rightarrow$

$c^d \equiv m \ (mod\ n)$, obtendo-se assim a mensagem original.

A força do algoritmo reside no fato de que, caso uma entidade estranha intercepte a mensagem e queira decodificá-la, é necessário que ela conheça a chave privada (n,d) de A. Porém, a única informação disponível para a entidade estranha é a chave pública de A (n,e), que foi divulgada por meio de um canal qualquer. Para se obter a chave privada (n,d) a partir da chave pública (n,e), é necessário calcular o valor de $\phi(n)$, conhecendo-se apenas o número composto n, sem que sejam conhecidos os seus fatores primos p e q. Portanto, seria necessário decompor n em fatores primos, o que é computacionalmente muito custoso para números muito grandes. Mesmo os melhores algoritmos de fatoração conhecidos na atualidade ainda se mostram ineficazes quando trabalham com inteiros suficientemente grandes. Para maiores detalhes sobre os tópicos matemáticos utilizados na metodologia do algoritmo, podem ser consultadas as referências (Coutinho, 2000), (Alencar, 1992) ou o APÊNDICE A.

2.4 Exemplo de Utilização do Algoritmo RSA

A seguir, será apresentado um exemplo ilustrativo da utilização do algoritmo RSA:

Duas entidades *A* e *B* desejam trocar mensagens criptografadas utilizando-se para isso o algoritmo RSA. Trabalhar-se-á com o caso em que a entidade *A* deseja enviar uma mensagem criptografada para a entidade *B*. O caso inverso é absolutamente análogo. Primeiramente, é necessário que *B* execute o processo de geração do seu par de chaves pública e privada. Para isso, *B* escolhe dois números primos grandes *p* e *q* e efetua a multiplicação $n = p.q$. Como exemplo, tomar-se-á:

p = 20.934.834.647 e
q = 2.593.843.747.457

Em seguida, calcula-se $n = p.q$

n = 20.934.834.647 x 2.593.843.747.457 = 54.301.689.953.167.121.742.679

Vale lembrar que o tamanho dos números primos utilizados em aplicações práticas do algoritmo RSA é extremamente grande, e que a utilização de números primos pequenos neste exemplo possui caráter meramente ilustrativo do método, em nada se assemelhando aos valores utilizados nas aplicações comerciais do algoritmo. A título de curiosidade, as chaves utilizadas atualmente nas aplicações práticas do algoritmo RSA possuem, no mínimo, 1024 bits. Para ilustrar essa magnitude, pode-se citar como exemplo o número:

n=135.066.410.865.995.223.349.603.216.278.805.969.938.881.475.605.667.027.524.485.143.851.526.510.604.859.533.833.940.287.150.571.909.441.798.207.282.164.471.551.373.680.419.703.964.191.743.046.496.589.274.256.239.341.020.864.383.202.110.372.958.725.762.358.509.643.110.564.073.501.508.187.510.676.594.629.205.563.685.529.475.213.500.852.879.416.377.328.533.906.109.750.544.334.999.811.150.056.977.236.890.927.563

Esse número é conhecido como RSA-1024, e foi proposto em 1991 pelo *RSA Laboratories*, em um concurso de fatoração de números compostos. Sabe-se que se trata de um número semiprimo, isto é, composto por dois números primos. Porém, até o presente ano, não se conhece ainda a sua fatoração.

Retomando o exemplo numérico da utilização do algoritmo RSA, tem-se o número n = 54.301.689.953.167.121.742.679. Em seguida, calcula-se o valor da função fi de Euler de n, obtendo-se:

$$\phi(n) = 20.934.834.646 \times 2.593.843.747.456 = 54.301.689.950.552.343.160.576$$

Em seguida, escolhe-se um número e, de forma que $1 < e < \phi(n)$, e também MDC $(e, \phi(n)) = 1$. Tomar-se-á e = 1009.

Então, calcula-se d, o inverso multiplicativo de e módulo $\phi(n)$. Em outras palavras, $d.e \equiv 1 \ (mod\ \phi(n))$

1009^{-1} modulo $\phi(n) = d$ = 4.251.569.381.658.706.748.945

Finalmente, B publica o par de números (n,e) como sua chave pública, e mantém secretamente o par de números (n,d) como sua chave privada.

Supondo-se que A deseja enviar a mensagem m = 29.384.737.849.576.728.375 para B. De posse da chave pública de B, A calcula:

m^e modulo $n = c$ = 20.636.340.188.476.258.131.729

Em seguida, A envia a mensagem c, criptografada, para B. Ao receber a mensagem, para que B possa descriptografá-la, basta utilizar sua chave privada para efetuar a exponenciação c^d modulo n, e obter a mensagem original m. Assim:

$m = 20.636.340.188.476.258.131.729^{4.251.569.381.658.706.748.945}$ modulo $n \Rightarrow$

m = 29.384.737.849.576.728.375

Dessa forma, *B* finalmente pode ler a mensagem criptografada por *A*. Todo o processo ocorreu sem que houvesse a necessidade de comunicação segura entre *A* e *B*, exemplificando assim a metodologia denominada criptografia assimétrica ou de chave pública.

2.5 Utilização do Algoritmo RSA em Assinatura Digital

O algoritmo RSA, além de possuir larga aplicação na criptografia de mensagens, também pode ser utilizado no processo de assinatura digital. A seguir, será apresentado um exemplo ilustrativo da utilização do algoritmo RSA em uma troca de mensagens na qual há a necessidade tanto de encriptação quanto de assinatura digital. Como se trata meramente de um exemplo ilustrativo, a assinatura será feita na própria mensagem, e não no seu *Hash*, como é normalmente realizado na prática.

Supondo que as mesmas duas entidades *A* e *B* do exemplo da seção 2.4 desejam trocar mensagens criptografadas e assinadas utilizando-se para isso o algoritmo RSA. Trabalhar-se-á com o caso em que a entidade *A* deseja enviar uma mensagem criptografada e assinada para a entidade *B*. O caso inverso é absolutamente análogo.

Inicialmente, é necessário que tanto *A* quanto *B* executem o processo de geração de seus pares de chaves pública e privada. Esse processo já foi ilustrado para a entidade *B* no exemplo da seção 2.4, e seu par de chaves é:

Chave Pública de *B*:
$(n , e) = (54.301.689.953.167.121.742.679 , 1009)$

Chave Privada de *B*:
$(n , d) = (54.301.689.953.167.121.742.679 , 4.251.569.381.658.706.748.945)$

Ilustremos agora o processo de geração do par de chaves da entidade *A*. Para isso, *A* escolhe dois números primos grandes *r* e *s* e efetua a multiplicação $k = r.s$. Como exemplo, tomar-se-á:

r = 23.764.850.281 e

s = 8.265.764.985.397

Em seguida, calcula-se $k = r.s$

k = 23.764.850.281 x 8.265.764.985.397 = 196.434.667.335.891.856.346.557

Novamente, vale lembrar que o tamanho dos números primos utilizados em aplicações práticas do algoritmo RSA, inclusive para assinatura digital, é muito maior que os números utilizados neste exemplo, que possui meramente função ilustrativa do processo.

De posse de k = 196.434.667.335.891.856.346.557, calcula-se o valor da função fi de Euler de k, obtendo-se:

$\phi(k)$ = 23.764.850.280 x 8.265.764.985.396 = 196.434.667.327.602.326.510.880

Em seguida, escolhe-se um número f, de forma que $1 < f < \phi(k)$, e também MDC $(f, \phi(k)) = 1$. Tomar-se-á f = 135.679.

Então, calcula-se g, o inverso multiplicativo de f módulo $\phi(k)$. Em outras palavras, $g.f \equiv 1 \ (mod\ \phi(k))$

135679^{-1} modulo $\phi(k) = g$ = 143.436.875.243.387.298.656.479

Têm-se então as chaves pública e privada de A:

Chave Pública de A:
(k , f) = (196.434.667.335.891.856.346.557 , 135.679)

Chave Privada de A:
(k , g) = (196.434.667.335.891.856.346.557 , 143.436.875.243.387.298.656.479)

Supõe-se que *A* deseja enviar a mensagem *m* = 29.384.737.849.576.728.375 criptografada e assinada para *B*. De posse da chave pública de *B*, *A* calcula:

$c = m^e$ modulo n = 20.636.340.188.476.258.131.729

Essa é a mensagem criptografada, análoga àquela obtida no exemplo numérico da seção 2.4. Em seguida, *A* deverá "assinar" a mensagem (na prática, *A* assina o *Hash* da mensagem) utilizando para isso a sua chave privada e enviar tanto a mensagem criptografada quanto a mensagem assinada para *B*, para que este possa comprovar a autenticidade do emissor. Então, *A* calcula:

$z = m^g$ modulo k = 138.327.885.332.253.107.547.257

Essa é a mensagem assinada por *A*.

Dessa forma, *A* envia a mensagem criptografada e a mensagem assinada (c , z) para *B*. Ao receber as mensagens, *B* utiliza sua chave privada para descriptografar a mensagem criptografada, efetuando a exponenciação c^d modulo *n*, e obtém a mensagem original *m*:

$m = 20.636.340.188.476.258.131.729^{4.251.569.381.658.706.748.945}$ modulo $n \Rightarrow$

m = 29.384.737.849.576.728.375

Porém, *B* ainda precisa confirmar a autenticidade da mensagem. Para comprovar a identidade do emissor, *B* utiliza a chave pública de *A* para descriptografar a mensagem assinada, efetuando a exponenciação z^f modulo *k*:

$m_z = 138.327.885.332.253.107.547.257^{135.679}$ modulo $k \Rightarrow$

$m_z = 29.384.737.849.576.728.375 = m$

Portanto, como *B* verificou a semelhança entre a mensagem criptografada e a mensagem assinada, depois de descriptografar ambas, está assegurada a autenticidade

da mensagem, isto é, a entidade emissora das mensagens é realmente a entidade *A*, como se supunha. Caso as mensagens criptografada e assinada apresentassem conteúdos diferentes após *B* descriptografá-las, então porder-se-ia afirmar que a entidade emissora das mensagens não se tratava da entidade *A*, pois a chave pública de *A* não se mostrou adequada na descriptação da mensagem assinada.

Na prática, conforme já apresentado, não se assina a própria mensagem, mas sim o seu *Hash*. O algoritmo utilizado para a geração do *Hash* deve ser conhecido tanto pelo emissor quanto pelo receptor da mensagem. Dessa forma, de maneira análoga ao exemplo numérico apresentado, o emissor envia dois pacotes de dados ao receptor: o *Hash* assinado com a sua própria chave privada (sua assinatura) e a mensagem original criptografada com a chave pública do receptor. Da mesma forma, o receptor utiliza a sua chave privada para descriptografar a mensagem e ler seu conteúdo. Para comprovar a autenticidade da mensagem, ele utiliza a chave pública do suposto emissor verdadeiro e descriptografa o *Hash*. Em seguida, ele aplica a função geradora do *Hash* à mensagem original descriptografada e compara o resultado com o *Hash* assinado, que já havia sido descriptografado. Se os dois resultados forem coincidentes, está assegurada a autenticidade da mensagem, pois somente um emissor autêntico poderia criptografar um *Hash* utilizando para isso a sua chave privada, de forma que a sua chave pública pudesse ser utilizada para descriptografá-lo.

Há vários motivos que justificam a utilização de um *Hash* no processo de assinatura digital, porém este Trabalho não irá abordar essa área específica da Teoria Criptográfica. Uma justificativa bastante simples para a necessidade de um *Hash* no processo de assinatura digital é o seguinte motivo: caso *A* enviasse a própria mensagem assinada (como foi feito no exemplo numérico) para *B*, qualquer entidade estranha (um espião, por exemplo) que pudesse interceptar a mensagem assinada poderia facilmente descobrir o seu conteúdo. Isso ocorre porque a mensagem foi assinada com a chave privada de *A*, sendo necessário apenas o conhecimento da sua chave pública para efetuar o processo inverso. Ora, mas a chave pública de *A* é amplamente conhecida, pois foi supostamente divulgada. Dessa forma, caso o processo de assinatura digital fosse aplicado diretamente à mensagem, haveria um sério comprometimento da segurança da troca de informações. Dessa forma, há a necessidade que não seja enviada a própria mensagem assinada, e sim alguma mensagem criptografada, que possa ser obtida a partir da mensagem original. Uma possível solução para esse problema é a utilização de

uma função geradora de *Hash*. Neste Trabalho, não serão abordadas as metodologias de funcionamento dos algoritmos geradores de *Hash*.

2.6 Aspectos Complementares do Algoritmo RSA

Ao se analisar com cuidado a metodologia do algoritmo RSA, surge com certa naturalidade a seguinte (e delicada) questão: *se os algoritmos de fatoração conhecidos atualmente não conseguem determinar os fatores primos de números muito grandes, como então é possível obter os números primos grandes necessários para se gerar o par de chaves pública e privada?*

Essa aparente contradição não procede pelo seguinte fato: Não se conhecem algoritmos eficientes o suficiente para se fatorar números compostos grandes em intervalos de tempo reduzidos, porém é possível determinar se um número é composto sem necessariamente fatorá-lo. Há uma variedade de testes probabilísticos, com tempo de processamento polinomial, que se podem aplicar em números grandes e verificar se são compostos ou provavelmente primos, sem que para isso seja necessário conhecer seus fatores. Inclusive, no ano de 2002, os pesquisadores indianos Manindra Agrawa, Neeraj Kayal e Nitin Saxena, do Indian Institute of Technology Kanpur, publicaram um artigo denominado "*PRIME is in P*", no qual apresentaram um algoritmo determinístico que determina, em tempo de processamento polinomial, se um número qualquer *n* é primo ou composto. Esse algoritmo ficou conhecido como *AKS Primality Test*, devido às iniciais dos sobrenomes de seus autores. O funcionamento do algoritmo se baseia em uma generalização polinomial do pequeno teorema de Fermat, e seus autores receberam diversos prêmios pelo seu desenvolvimento, entre eles o Prêmio Gödel, no ano de 2006. Para maiores detalhes acerca do funcionamento do algoritmo *AKS* e de outros testes de primalidade, consultar as referências (Agrawal, et al., 2004) e (Coutinho, 2000).

Outro aspecto importante acerca do RSA diz respeito à sua segurança, e torna-se absolutamente necessários que algumas ressalvas sejam também feitas sobre esse quesito. Haja vista todo o desenvolvimento do algoritmo RSA apresentado até aqui, fica claro que a utilização desse algoritmo possibilita a troca de informações de uma maneira segura, porém ainda passível de ser "quebrada", desde que novos algoritmos eficientes para a fatoração de inteiros sejam descobertos. Há inúmeros pesquisadores em todo o

mundo trabalhando no possível desenvolvimento de tais algoritmos. Além disso, outro conceito que vem surgindo ultimamente no universo da computação, e que está suscitando desde entusiasmo até temor entre os cientistas e usuários comerciais do algoritmo RSA, é o conceito de computação quântica. A construção dos denominados "computadores quânticos" se baseia na utilização de certas propriedades quânticas da matéria em seu funcionamento. Mesmo que os chamados "processadores quânticos" ainda não tenham sido desenvolvidos, já há uma enorme expectativa acerca dos impactos que seriam causados pelo seu surgimento. Por exemplo, em 1994, Peter Shor, do *AT&T Bell Laboratories*, mostrou que, se um computador quântico puder ser realmente construído, então poderá ser desenvolvido um algoritmo capaz de fatorar números inteiros enormes (e resolver o problema do logaritmo discreto) de maneira extremamente rápida! (Shor, 1997), (Coutinho, 2000). Peter Shor também foi ganhador do Prêmio Gödel, no ano de 1999, pela publicação do seu artigo sobre fatoração de números inteiros em tempo polinomial em computadores quânticos. Dessa forma, caso o computador quântico seja realmente viabilizado, toda a utilização atual do algoritmo RSA (que, diga-se de passagem, é enorme!) cairá por terra. Trata-se de um risco que se corre todos os dias. Cada usuário de serviços do tipo *internet banking* pode enfrentar vários problemas para utilizar tais serviços caso o RSA seja realmente quebrado, sem contar os investimentos milionários que seriam necessários para se adaptar grande parte da criptografia bancária existente na atualidade para outros sistemas criptográficos, muitos deles apresentando níveis de segurança significativamente menores que os proporcionados pelo algoritmo RSA. Portanto, o estudo sistemático das técnicas criptográficas atuais, bem como o possível desenvolvimento de novos algoritmos que possam ser utilizados para substituir os antigos, possui motivações bastante amplas, que vão desde as pesquisas ligadas meramente à área acadêmica até aquelas realizadas nos grandes centros de desenvolvimento tecnológico financiados pela iniciativa privada, para o desenvolvimento de tecnologia diretamente aplicável comercialmente. Todas as circunstâncias apresentadas, bem como o caráter inegavelmente atual da pesquisa criptográfica, motivaram a elaboração deste Trabalho de Graduação, principalmente a pesquisa sobre um algoritmo relativamente recente e ainda pouco explorado comercialmente, que é o algoritmo baseado na utilização de Curvas Elípticas sobre corpos finitos. No capítulo 3 serão apresentadas as nuances desse tipo de algoritmo.

3 Algoritmo Baseado em Curvas Elípticas

3.1 Histórico

O estudo das Curvas Elípticas e de suas propriedades teve início ainda no século XVIII, com trabalhos dos matemáticos Giulio Fagnano e Leonhard Euler, sobre integrais elípticas. Ao contrário do que possa parecer, as Curvas Elípticas não são elipses. Elas recebem esse nome devido à sua relação com algumas integrais elípticas que surgem no cálculo do comprimento do arco de elipses. Como exemplo de integrais elípticas, podem-se citar:

$$\int \frac{dx}{\sqrt{x^3+ax+b}} \qquad \text{e} \qquad \int \frac{xdx}{\sqrt{x^3+ax+b}}$$

As primeiras aplicações criptográficas de Curvas Elípticas foram propostas no ano de 1985, de maneira independente, pelos pesquisadores Neal Koblitz e Victor S. Miller. A abordagem criptográfica utilizando-se Curvas Elípticas (conhecida como ECC, devido à sigla em inglês para *Elliptic Curve Cryptography*) utiliza como fundamento os conceitos de criptografia assimétrica, ou de chave pública. Mais precisamente, os algoritmos criptográficos de Curvas Elípticas se utilizam da intratabilidade do problema do logaritmo discreto em corpos finitos (na verdade, um problema análogo, denominado problema do logaritmo discreto para Curvas Elípticas). Na seção 3.3.2 serão apresentados com detalhes os problemas do logaritmo discreto sobre corpos finitos e para Curvas Elípticas.

A **Figura 4** e a **Figura 5** ilustram duas representações gráficas de Curvas Elípticas definidas sobre o corpo dos reais.

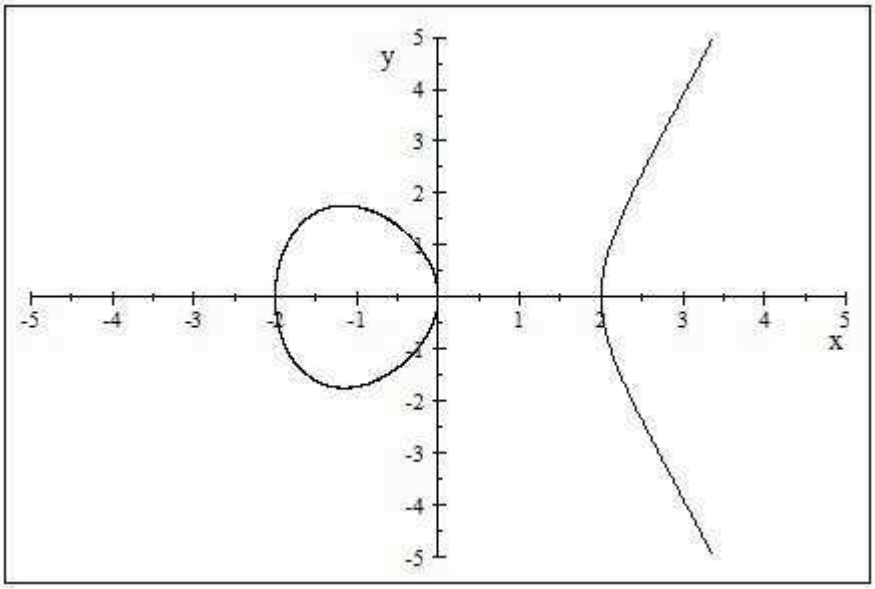


Figura 4 - Gráfico da Curva Elíptica $y^2 = x^3 - 4x$ definida sobre $\mathbb{R}$

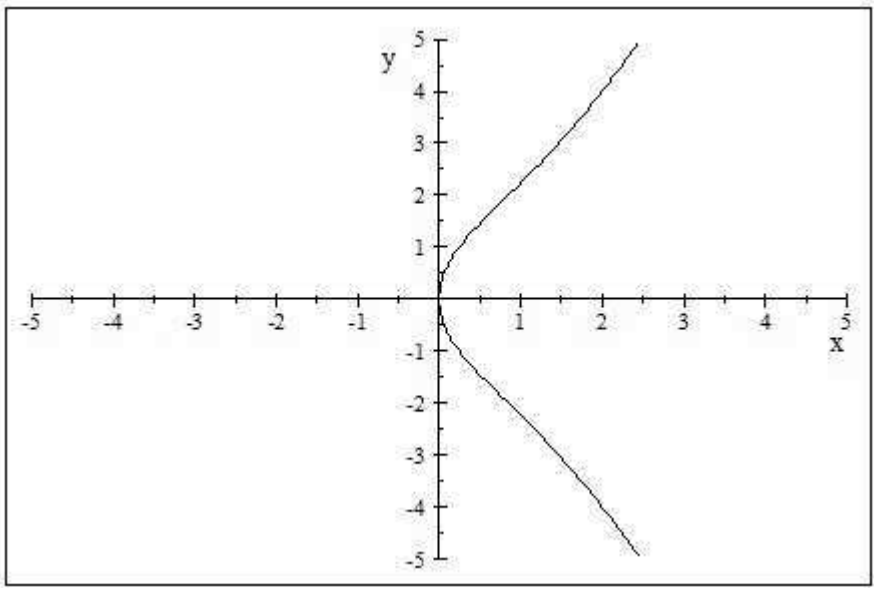


Figura 5 - Gráfico da Curva Elíptica $y^2 = x^3 + 4x$ definida sobre $\mathbb{R}$

A utilização atual das Curvas Elípticas não se restringe meramente ao campo da criptografia. A título de curiosidade, pode-se citar como exemplos de sua aplicação o algoritmo de fatoração de números inteiros baseado em Curvas Elípticas, proposto pelo pesquisador H. W. Lenstra Jr. em 1987, e também a sua utilização pelo pesquisador A. J. Wiles na demonstração do Último Teorema de Fermat, que teve sua versão final

publicada em 1995. Para maiores detalhes, pode-se consultar (Washington, 2008). Nas próximas seções, serão apresentados os detalhes matemáticos que permitem que Curvas Elípticas sejam utilizadas em aplicações criptográficas.

3.2 Definições

3.2.1 Curva Elíptica

Pode-se definir uma Curva Elíptica *E* sobre um corpo *K* como o conjunto de pares ordenados (*x*, *y*) que satisfazem à seguinte equação:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Equação 4 - Forma Generalizada de Weierstrass

com $x, y, a_1, \dots, a_6 \in K$ e $a_1, \dots, a_6$ constantes.

Essa equação é conhecida como Forma Generalizada de Weierstrass. Ela será particularmente útil quando forem abordadas as Curvas Elípticas sobre corpos de característica 2 ou 3. Caso o leitor não esteja familiarizado com as estruturas algébricas utilizadas nos processos criptográficos baseados em Curvas Elípticas, podem ser consultadas as referências (Nachbin, 1974), (Garcia, et al., 2002), (Lang, 1972) ou mesmo o APÊNDICE B, onde há um pequeno resumo dos principais tópicos de Álgebra utilizados ao longo deste trabalho.

Para a grande maioria dos casos que serão abordados neste texto, uma Curva Elíptica *E* sobre um corpo *K* terá uma equação da seguinte forma:

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

Equação 5 - Forma Reduzida de Weierstrass

com $x, y, A, B \in K$ e A, B constantes.

Essa equação é conhecida como Forma Reduzida de Weierstrass, ou simplesmente Equação de Weierstrass. Essa forma será largamente utilizada neste

trabalho, pois, quando a característica do corpo sobre o qual está definida uma Curva Elíptica *E* for diferente de 2 e 3, sempre se pode aplicar uma mudança de variáveis e transformar a Equação Generalizada da curva em uma Equação Reduzida. Para se realizar essa transformação, deve-se proceder da seguinte forma:

Tem-se a equação na sua forma generalizada

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Como a característica do corpo sobre o qual a curva está definida é diferente de 2, pode-se completar quadrados para os termos em y, obtendo-se assim:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{{a_1}^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{{a_3}^2}{4} + a_6\right)$$

Adotando-se a mudança de variável $y_1 = y + a_1x/2 + a_3/2$ e novas constantes, obtém-se:

$${y_1}^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

Como a característica do corpo sobre o qual a curva está definida também é diferente de 3, então pode-se adotar outra mudança de variável $x_1 = x + a_2'/3$, de forma que se obtém:

$$y_1^2 = x_1^3 + Ax_1 + B$$

com novas constantes *A* e B.

Para se utilizarem Curvas Elípticas em aplicações criptográficas, é necessário que a seguinte restrição seja respeitada:

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

Essa restrição é necessária para que se possa garantir a inexistência de raízes múltiplas na equação da Curva Elíptica, de forma que seja possível traçar uma reta

tangente passando por cada um dos pontos da curva. Essa necessidade ficará mais clara na seção 3.2.4, quando for abordada a Lei de Grupo.

3.2.2 Ponto no Infinito

Na seção 3.2.1, foi apresentada a definição de uma Curva Elíptica *E* sobre um corpo *K* como sendo o conjunto de pares ordenados $(x, y) \in K \times K$, que satisfazem à Equação Generalizada de Weierstrass daquela curva. Porém, para aplicações criptográficas computacionais de Curvas Elípticas, é necessário se adicionar à definição acima um ponto extra, denominado Ponto no Infinito de uma Curva Elíptica. À primeira vista, a definição do Ponto no Infinito pode parecer bastante estranha.

Na seção 3.2.4, quando for introduzida a Lei de Grupo, será apresentado um fato bastante elucidativo acerca da necessidade da definição do Ponto no Infinito. Para aplicações criptográficas, necessita-se de um "elemento neutro" da Lei de Grupo, para que as Curvas Elípticas apresentem uma estrutura análoga à de um grupo abeliano finito. Também, a definição do Ponto no Infinito torna-se bastante natural quando se utilizam coordenadas projetivas em um espaço projetivo bidimensional. O conceito de espaço projetivo bidimensional será abordado na seção 3.2.3.

3.2.3 Espaços Projetivos

Antes de se definir espaço projetivo, é necessário apresentar a definição de equivalência entre n-uplas de coordenadas. Sem perda de generalidade, será apresentada a definição de equivalência utilizando-se como exemplos triplas de coordenadas. Seja *K* um corpo. Duas triplas (x_1, y_1, z_1) e (x_2, y_2, z_2), com $x_i, y_i, z_i \in K$, $i = 1, 2$, são ditas equivalentes, e escreve-se $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, se existe $\lambda \in K$, tal que:

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$$

Define-se classe de equivalência de (x, y, z), e representa-se por $(x : y : z)$, o conjunto de todas as triplas equivalentes à tripla (x, y, z). Dessa forma, fica claro que a

classe de equivalência de uma tripla (x, y, z) depende apenas da proporção entre x, y e z. Uma maneira geométrica de se tentar visualizar a classe de equivalência ($x : y : z$), com ao menos umas das coordenadas não nula, para o caso em que K é o corpo $\mathbb{R}$ dos reais, é a sua visualização como uma reta no espaço Euclidiano tridimensional, passando por (x, y, z) e pela origem. Dessa forma, todas as triplas (x, y, z) equivalentes entre si seriam representadas por pontos pertencentes a uma mesma reta que passa pela origem do sistema.

Ainda, define-se o espaço projetivo bidimensional P_K^2 sobre o corpo K, também denominado plano projetivo P_K^2, como sendo o conjunto de todas as classes de equivalência de triplas (x, y, z), com x, y e $z \in K$ e ao menos uma das coordenadas não nula. Novamente, uma maneira geométrica de se tentar visualizar o plano projetivo P_K^2, para o caso em que K é o corpo $\mathbb{R}$ dos reais, é a sua visualização como o conjunto de todas as retas do espaço Euclidiano tridimensional que passam pela origem.

Tomando-se a classe de equivalência ($x : y : z$), com $z \neq 0$, pode-se simplificá-la para ($x/z : y/z : 1$). Os pontos (triplas) pertencentes a essa classe de equivalência são denominados pontos finitos em P_K^2. Quando se toma ($x : y : z$), com $z = 0$, as divisões x/z e y/z tendem ao infinito. Assim, os pontos pertencentes à classe de equivalência ($x : y : 0$) são denominados "pontos no infinito" em P_K^2. Pode-se, mais uma vez, recorrer a argumentos geométricos para se tentar visualizar os pontos finitos e os "pontos no infinito" em P_K^2. Traçando-se um plano paralelo ao plano xy no espaço Euclidiano tridimensional, por exemplo o plano $z = 1$, todas as retas que passam pela origem, com exceção daquelas contidas no plano xy, cruzam o plano $z = 1$ em um único ponto. Dessa forma, cada classe de equivalência ($x : y : z$), com $z \neq 0$, possui uma única tripla da forma (x, y, 1). Esses são os chamados pontos finitos no plano projetivo. Para se completar P_K^2, faltam ainda as classes de equivalência ($x : y : 0$) que possuem as triplas da forma (x, y, 0). Essas triplas são denominadas "pontos no infinito" exatamente porque as retas que passam por (x, y, 0) e pela origem estão contidas no plano xy, que é paralelo ao plano $z = 1$, e por isso não interceptam esse plano. Para se representar essas classes, pode-se traçar, no plano xy, uma reta paralela ao eixo x, por exemplo, a reta $y = 1$, de forma que cada classe de equivalência das triplas (x, y, 0), com $y \neq 0$, possui uma única tripla da forma (x, 1, 0), isto é, todas as retas do plano xy que passam pela origem, com exceção da reta coincidente ao eixo x, cruzam a reta $y = 1$ em um único ponto. Dessa forma, cada classe de equivalência ($x : y : 0$), com $y \neq 0$, possui uma única tripla

da forma (x, 1, 0). Por fim, falta a classe de equivalência (x : 0 : 0). Essa classe de equivalência pode ser representada por uma reta coincidente ao eixo x. Dessa forma, fica representado geometricamente o plano projetivo P_K^2.

Pode-se mostrar que existe apenas um "ponto no infinito" em qualquer Curva Elíptica, isto é, existe uma única classe de equivalência pertencente a P_K^2 que satisfaz a equação da Curva Elíptica, para as triplas da forma (x, y, 0). Antes de fazer essa demonstração, é necessário apresentar algumas definições importantes.

Primeiramente, define-se o plano A_K^2, denominado "plano afim sobre K", como sendo o conjunto $A_K^2 = \{(x, y) \in K \times K\}$. Pode-se estabelecer uma inclusão de A_K^2 em P_K^2 dada por:

$$(x, y) \longmapsto (x : y : 1)$$

Dessa forma, observa-se que há uma identificação entre o plano afim A_K^2 e os pontos finitos em P_K^2. Uma Curva Elíptica E sobre um corpo K pode ser representada como sendo o conjunto de pares ordenados (x, y) que anulam o valor de um polinômio $f(x, y)$ da forma $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Isto é, os pares ordenados (x, y) que constituem a curva são as soluções da equação $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$. Percebe-se facilmente que esses pares ordenados pertencem ao plano afim A_K^2. Da mesma forma que se estabeleceu uma relação entre A_K^2 e P_K^2, pode-se estabelecer uma relação entre os polinômios da forma $f(x, y)$ e os polinômios homogêneos da forma $F(x, y, z)$. Para que as características da Curva Elíptica sejam preservadas ao se realizar a correspondência entre $f(x, y)$ e $F(x, y, z)$, é necessário que a inclusão da coordenada z não interfira nos valores que anulam o polinômio original, quando $z = 1$. Em outras palavras, deve-se construir o polinômio $F(x, y, z)$, tal que:

$$F(x, y, 1) = f(x, y)$$

Equação 6 – Relação entre Polinômio Homogêneo em $\boldsymbol{P_K^2}$ e $f(x, y)$

Para se construir o polinômio homogêneo $F(x, y, z)$, é necessário que antes sejam definidos alguns conceitos complementares. Um polinômio de grau n é dito homogêneo, se ele é formado apenas por termos da forma $ax^iy^jz^k$, com $a \in K$ e também $i + j + k = n$. Se um polinômio $F(x, y, z)$ é homogêneo, então se pode mostrar

que $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$, para todo $\lambda \in K$. Dessa forma, se (x_1, y_1, z_1) é raiz de um polinômio homogêneo $F(x, y, z)$ em P_K^2, então todas as triplas pertencentes à mesma classe de equivalência $(x_1 : y_1 : z_1)$ também o são. Esse fato torna irrelevante a busca por cada uma das triplas que "zeram" o polinômio homogêneo, pois basta que se encontrem as classes de equivalência que representam essas triplas para que se tenha um mapeamento completo das suas raízes e, consequentemente, dos pontos pertencentes à Curva Elíptica. Portanto, para se analisar os pontos (pares ordenados) de uma Curva Elíptica em coordenadas projetivas, é interessante transformar o polinômio $f(x, y)$, em um polinômio homogêneo $F(x, y, z)$, de forma que $F(x, y, 1) = f(x, y)$.

Seja E uma Curva Elíptica, definida sobre um corpo K, dada pela equação $y^2 = x^3 + Ax + B$. Sua forma homogênea é dada por:

$$zy^2 - x^3 - Axz^2 - Bz^3 = 0$$

Equação 7 – Equação da Curva Elíptica Homogeneizada para $n = 3$

De acordo com a **Equação 6**, deve-se ter $F(x, y, 1) = f(x, y)$. Portanto, todos os pares ordenados que se mostrem solução da equação $f(x, y) = y^2 - x^3 - Ax - B = 0$ também serão solução da equação $F(x, y, z) = zy^2 - x^3 - Axz^2 - Bz^3 = 0$, para $z = 1$. Dessa forma, todos os pares ordenados (x, y) pertencentes à Curva Elíptica E original irão corresponder aos pontos pertencentes às classes de equivalência $(x : y : 1)$ em P_K^2. Esses são os pontos finitos de E em P_K^2. Para se encontrarem os "pontos no infinito" da curva E, basta fazer $z = 0$. Dessa forma, a **Equação 7** se transforma em:

$$-x^3 = 0 \quad \Rightarrow \quad x = 0$$

Portanto, como $x = z = 0$, então obrigatoriamente $y \neq 0$ pela própria definição de espaço projetivo bidimensional. Conclui-se, então, que há apenas uma classe de equivalência de E com "pontos no infinito" em P_K^2, a saber, a classe $(0 : y : 0) = (0 : 1 : 0)$. Essa classe de equivalência corresponde ao Ponto no Infinito, citado anteriormente na seção 3.2.2. Na próxima seção, será introduzida a Lei de Grupo, que utilizará o conceito de Ponto no Infinito como seu elemento neutro.

3.2.4 Lei de Grupo

Para que seja possível a aplicação criptográfica da teoria de Curvas Elípticas, é necessário que as curvas assumam o comportamento algébrico de um grupo. Dessa forma, é necessário que seja estabelecida uma operação "soma" entre elementos desse conjunto (pontos da curva), e essa operação deve satisfazer algumas propriedades algébricas específicas dos grupos.

A operação "soma" estabelecida entre dois pontos (distintos ou não) de uma Curva Elíptica produz um terceiro ponto, também pertencente à Curva Elíptica. A seguir, será ilustrado o processo de soma para curvas definidas sobre o corpo dos reais. Devido ao seu apelo geométrico, será apresentada essa abordagem, pois dessa forma é possível uma tentativa de "visualização" do processo, algo que se mostra extremamente complexo quando se define tal operação "soma" para curvas sobre outros corpos. As fórmulas obtidas, mesmo que por meio de argumentos geométricos sobre $\mathbb{R}$, podem ser estendida para curvas sobre quaisquer outros corpos, desde que sua característica seja diferente de 2 e 3. A definição da Lei de Grupo para curvas definidas sobre esses corpos será feita na seção 3.2.6. Para as curvas definidas sobre os demais corpos, tem-se:

Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos pertencentes à Curva Elíptica E, dada pela equação $y^2 = x^3 + Ax + B$, com $P_1, P_2 \neq \infty$. O ponto $P_3 = (x_3, y_3) = P_1 + P_2$, denominado "soma" de P_1 com P_2, é definido como sendo a reflexão, através do eixo *x*, do ponto de intersecção entre a reta que contém P_1 e P_2 e a Curva Elíptica E. É importante salientar que a definição acima somente assume tal caráter geométrico quando a Curva Elíptica E está definida sobre o corpo K dos reais, e foi apresentada dessa forma com o intuito de ilustrar geometricamente as fórmulas seguintes, que valem para qualquer corpo K de característica diferente de 2 e 3. A **Figura 6** ilustra geometricamente o processo de adição de pontos em uma Curva Elíptica.

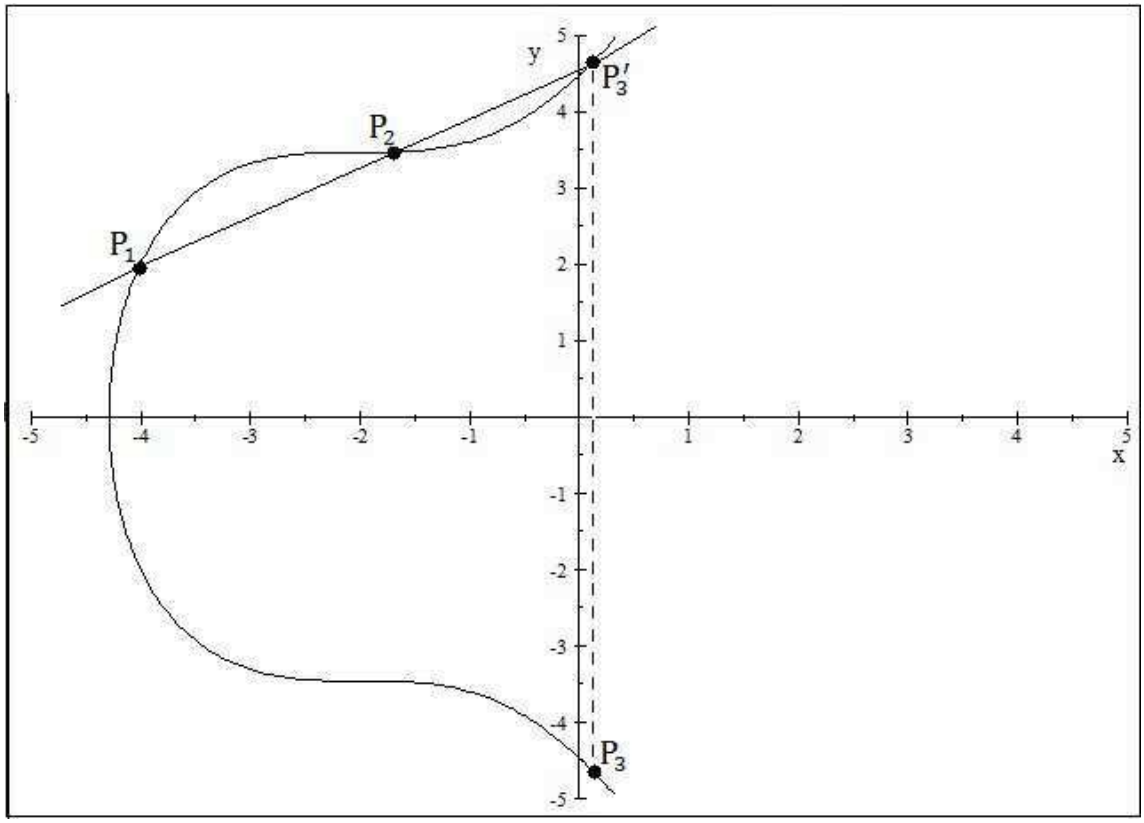


Figura 6 - Soma de Pontos na Curva Elíptica $y^2 = x^3 + 6x^2 + 12x + 20$

Porém, o processo acima não contempla os casos em que algum dos pontos a serem somados, ou mesmo ambos, sejam o Ponto no Infinito. Para este caso, são necessárias algumas definições extras, que serão apresentadas a seguir.

Com o intuito de tornar mais claro o processo de "soma" de pontos em uma Curva Elíptica, far-se-á uma abordagem detalhada de cada caso possível de combinação dos pontos P_1 e P_2:

Caso 1 - $P_1 \neq P_2$ e ambos $\neq \infty$

Se $x_1 = x_2$, para que os pontos P_1 e P_2 pertençam à Curva Elíptica e sejam pontos distintos, é necessário que $y_1 = -y_2$, pois se tem:

$$x_1^3 + Ax_1 + B = x_2^3 + Ax_2 + B \quad \Rightarrow \quad y_1^2 = y_2^2 \quad \Rightarrow \quad y_1 = \pm y_2$$

Como não se pode ter $y_1 = y_2$, pois $P_1 \neq P_2$, então $y_1 = -y_2$

Dessa forma, a reta que passa por P_1 e P_2 é vertical. Quando se utilizam coordenadas projetivas para se representar P_1 e P_2, a reta que passa por esses pontos intercepta a Curva Elíptica somente nos pontos pertencentes à classe de equivalência

(0 : 1 : 0), que foi definida anteriormente como o Ponto no Infinito. Refletindo o Ponto no Infinito no eixo *x*, obtém-se o próprio Ponto no Infinito, pois (0 : *y* : 0) = (0 : $-y$: 0) = (0 : 1 : 0). Portanto, a inversão desse ponto leva a ele próprio (trata-se do elemento neutro da Lei de Grupo). Então, $P_1 + P_2 = \infty$. Nesse caso, denota-se $P_2 = -P_1$.

Se $x_1 \neq x_2$, calcula-se a equação da reta que passa por P_1 e P_2:

$(y - y_1) = m(x - x_1)$, com $m = \frac{y_2 - y_1}{x_2 - x_1}$

É necessário determinar o ponto em que a reta interceptará a Curva Elíptica $y^2 = x^3 + Ax + B$. Fazendo-se *y* da reta coincidente com *y* da curva, obtém-se uma equação cúbica em *x*, dada por:

$$x^3 - m^2x^2 + (A - 2my_1 + 2m^2x_1)x + (B - m^2x_1^2 + 2mx_1y_1) = 0$$

As três raízes da equação acima fornecem as abscissas dos três pontos de intersecção entre a reta que passa por P_1 e P_2 e a própria Curva Elíptica. Porém, as abscissas de dois dos três pontos de intersecção já são conhecidas, pois P_1 e P_2 são pontos da curva. Portanto, é possível determinar a terceira abscissa utilizando-se a relação da soma das raízes da equação:

$m^2 = x_1 + x_2 + x_3' \Rightarrow$

$x_3' = m^2 - x_1 - x_2$ e $y_3' = m(x_3' - x_1) + y_1$

Por fim, realiza-se a reflexão do ponto (x_3', y_3') no eixo *x*, e obtém-se o ponto:

$x_3 = x_3' = m^2 - x_1 - x_2$ e $y_3 = -y_3' = m(x_1 - x_3) - y_1$

Caso 2 - $P_1 = P_2 \neq \infty$

Nesse caso, como $P_1 = P_2$, não é possível encontrar uma reta que passe pelos dois pontos, pois eles são coincidentes. Porém, ao se construírem retas passando por dois pontos distintos de uma curva, quanto mais os pontos se aproximam um do outro, mais próxima essa reta se torna da reta tangente à curva naquele ponto. Portanto, no caso em que $P_1 = P_2$, basta que se tome a reta tangente à Curva Elíptica naquele ponto:

Se $y_1 = 0$, a reta é vertical, e o caso é análogo ao caso anterior ($P_1 \neq P_2$ e $x_1 = x_2$), resultando em $P_1 + P_2 = \infty$. Tem-se, portanto, $P_2 = -P_1$.

Se $y_1 \neq 0$, pode-se encontrar o coeficiente angular dessa reta por meio de derivação implícita:

$2y\frac{dy}{dx} = 3x^3 + A \Rightarrow$

$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$

Então, obtém-se a equação da reta tangente:

$(y - y_1) = m(x - x_1)$

Fazendo-se *y* da reta coincidente com *y* da curva, obtém-se uma nova equação cúbica em *x*, dada por:

$x^3 - m^2x^2 + (A - 2my_1 + 2m^2x_1)x + (B - m^2x_1^2 + 2mx_1y_1) = 0$

Essa equação possui raiz dupla (x_1), portanto:

$x_3' = m^2 - 2x_1$ e $y_3' = m(x_3' - x_1) + y_1 \Rightarrow$

$x_3 = m^2 - 2x_1$ e $y_3 = m(x_1 - x_3) - y_1$

Caso 3 - $P_1 \neq \infty$ e $P_2 = \infty$

Como $P_2 = \infty$, a reta que contém P_1 e P_2 é vertical, para qualquer P_1 da Curva Elíptica considerada. Dessa forma, a reta irá interceptar a curva em um ponto $P_3' = (-P_1)$, que é a reflexão do ponto P_1 sob eixo *x*. Por fim, procedendo-se a reflexão do ponto P_3' pelo eixo *x*, obtém-se o ponto P_1. Portanto, $P_1 + \infty = P_1$.

Caso 4 - $P_1 = P_2 = \infty$

Este caso é análogo ao anterior. Como $P_1 + \infty = P_1$ para todo ponto P_1 pertencente à curva, basta fazer $P_1 = \infty$, e obtém-se: $\infty + \infty = \infty$.

A partir da análise das possibilidades de "soma" de pontos de uma Curva Elíptica utilizando-se a Lei de Grupo, percebe-se que o ponto ∞ funciona como elemento neutro do processo de adição definido. Vale salientar também que o processo de adição de pontos descrito acima não equivale a uma simples adição das coordenadas desses pontos e, portanto, não se deve confundir a operação "soma" de pontos de uma Curva Elíptica com a operação de soma de pontos usual do $\mathbb{R}^2$.

A seguir, serão apresentadas algumas características importantes do processo de adição de pontos em uma Curva Elíptica, de forma que será possível tratar a Curva Elíptica como uma estrutura algébrica com propriedades bem definidas, a saber, propriedades de um grupo abeliano aditivo finito. As propriedades seguintes serão enunciadas sem demonstração. Para uma elucidação mais rigorosa, pode-se consultar (Washington, 2008).

1. A adição de pontos de uma Curva Elíptica E sobre um corpo K é fechada em E;
2. $P_1 + P_2 = P_2 + P_1$, para todo P_1 e $P_2 \in E$;
3. $P_1 + \infty = P_1$, para todo $P_1 \in E$;
4. Dado um ponto $P_1 \in E$, existe um ponto $P_2 \in E$, tal que $P_1 + P_2 = \infty$;
5. $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$, para todo P_1, P_2 e $P_3 \in E$.

As propriedades 1, 2, 3, 4 e 5 são denominadas, respectivamente, fechamento, comutatividade, existência de elemento neutro, existência de elemento inverso e associatividade. O elemento inverso definido como P_2 na proposição 4 é comumente denotado ($-P_1$). Vale salientar que se $P = (x, y)$, então $(-P) = (x, -y)$, como já visto no Caso 1 da definição da Lei de Grupo. Essa relação é válida para Curvas Elípticas com equação na forma reduzida de Weierstrass. A relação de elemento inverso para curvas com equação na forma generalizada de Weierstrass será apresentada na seção 3.2.6, quando serão apresentados aspectos de Curvas Elípticas definidas sobre corpos de característica 2 e 3.

Para aplicações criptográficas, há também a necessidade de que $4A^3 + 27B^2 \neq 0$, para que se possa garantir a existência de reta tangente em todos os pontos da curva, de forma que, dado um ponto P pertencente à curva, sempre seja possível se calcular $P + P = 2P$. Em outras palavras, para se garantir que a adição de dois pontos da curva sempre exista, é necessário que a curva seja não-singular (também denominada suave). As seguintes definições estabelecem as condições para que uma Curva Elíptica seja denominada não-singular:

Primeiramente, conforme apresentado na seção 3.2.3, define-se o plano A_K^2, denominado "plano afim sobre K", como sendo o conjunto $A_K^2 = \{(x, y) \in K \times K\}$. Define-se curva plana afim sobre K como o conjunto de zeros de um polinômio irredutível $C \in K[X, Y]$ em A_K^2. Em outras palavras, define-se curva plana afim sobre K como o seguinte conjunto $C = \{(x, y) \in A_K^2$, tais que $C(x, y) = 0\}$.

Seja C uma curva plana afim sobre K, e $P = (x, y)$ um ponto de C. Então, P é denominado "singular" se $\frac{\partial C}{\partial X}(x, y) = \frac{\partial C}{\partial Y}(x, y) = 0$. Uma curva é denominada não-singular (ou suave) se ela não possui pontos singulares (Enge, 1999).

Portanto, para se garantir que a Curva Elíptica possua reta tangente em todos os seus pontos, basta que as derivadas parciais $\frac{\partial C}{\partial X}(x, y)$ e $\frac{\partial C}{\partial Y}(x, y)$ não sejam nulas

simultaneamente. Então, para a Curva Elíptica E definida pelo conjunto de pontos (x, y), tais que $C(x, y) = y^2 - x^3 - Ax - B = 0$, deve-se evitar a seguinte situação:

$$\frac{\partial C}{\partial X}(x, y) = -3x^2 - A = 0$$

$$\frac{\partial C}{\partial Y}(x, y) = 2y = 0$$

Portanto, não se deve permitir que ocorra simultaneamente $3x^2 + A = 0$ e $y = 0$. Porém, se $y = 0$, então $x^3 + Ax + B = 0$. Logo, deve-se evitar a seguinte situação:

$$x^3 + Ax + B = 0$$
$$3x^2 + A = 0$$

Ora, mas para que as igualdades acima nunca sejam verdadeiras simultaneamente, basta que o polinômio $x^3 + Ax + B$ não possua raízes múltiplas, pois dessa forma a sua primeira derivada $(3x^2 + A)$ nunca se anula. Sabe-se que o discriminante de um polinômio cúbico cujas raízes são x_1, x_2 e x_3 é dado pela seguinte expressão:

$$((x_1 - x_2)\,(x_1 - x_3)\,(x_2 - x_3))^2 = -(4A^3 + 27B^2)$$

Dessa forma, garantindo-se que $4A^3 + 27B^2 \neq 0$, garante-se também a inexistência de raízes múltiplas no polinômio $x^3 + Ax + B$, garantindo-se assim também a não-singularidade da Curva Elíptica representada pela equação $y^2 = x^3 + Ax + B$. Portanto, para que a adição de dois pontos da curva sempre exista (o que é fundamental na utilização criptográfica das Curvas Elípticas), basta que se tenha $4A^3 + 27B^2 \neq 0$.

A título de ilustração do método apresentado, serão feitos dois exemplos numéricos de “soma” de pontos de uma Curva Elíptica.

Exemplo 1: Seja a Curva Elíptica *E* definida sobre o corpo dos reais $\mathbb{R}$ pela equação $y^2 = x^3 + 73$. Têm-se P_1 = (2, 9) e P_2 = (3, 10) pontos (pares ordenados) pertencentes à Curva Elíptica. Deseja-se obter o ponto $P_3 = P_1 + P_2$. Procede-se da seguinte maneira:

Inicialmente, é necessário encontrar a equação da reta que passa pelos pontos P_1 e P_2, que é $y = x + 7$. Essa equação é facilmente obtida conforme descrito no *Caso 1* acima. Fazendo-se *y* da equação coincidente com *y* da Curva Elíptica, obtém-se:

$(x + 7)^2 = x^3 + 73 \quad \Rightarrow$

$x^3 - x^2 - 14x + 24 = 0$

Como já se conhecem duas das raízes dessa equação ($x_1 = 2$ e $x_2 = 3$), obtém-se facilmente a terceira raiz $x_3' = -4$. Substituindo-se na equação da reta (ou da Curva Elíptica), obtém-se $y_3' = 3$. Procedendo-se a inversão do ponto (x_3', y_3'), obtém-se o ponto $P_3 = (-4, -3)$.

Para se calcular P_3 de uma maneira mais simples, pode-se utilizar as fórmulas já determinadas no *Caso 1*:

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

Dessa forma, ter-se-ia:

$$x_3 = 1^2 - 2 - 3 = -4$$
$$y_3 = 1(2 - (-4)) - 9 = -3$$

Obtendo-se, de maneira análoga, o ponto $P_3 = (-4, -3)$.

Exemplo 2: Seja a Curva Elíptica *E* definida sobre o corpo $\mathbb{Z}_{11}$ pela equação $y^2 = x^3 + x + 6$. Como 11 é um número primo, pode-se mostrar que $\mathbb{Z}_{11}$ é, de fato, um corpo. Tem-se P_1 = (2, 7) pertencente à Curva Elíptica. Deseja-se obter o ponto $2P_1 = P_1 + P_1$. Procede-se da seguinte maneira:

Utilizando-se as fórmulas já determinadas no *Caso 2*, têm-se:

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

$x_3 = m^2 - 2x_1$ e $y_3 = m(x_1 - x_3) - y_1$

Portanto:

$$m = \frac{3 \times 2^2 + 1}{2 \times 7} \; mod\ 11 \quad \Rightarrow$$

$$m = \frac{13}{14} \; mod\ 11 \quad \Rightarrow$$

$$m = 2 \times 3^{-1} \; mod\ 11 \quad \Rightarrow$$

$$m = 2 \times 4 \; mod\ 11 \quad \Rightarrow$$

$$m = 8 \; mod\ 11$$

Então:

$$x_3 = 8^2 - 2 \times 2 \; mod\ 11 \quad \Rightarrow$$

$$x_3 = 60 \; mod\ 11 \quad \Rightarrow$$

$$x_3 = 5 \; mod\ 11$$

$$y_3 = 8 \times (2 - 5) - 7 \; mod\ 11 \quad \Rightarrow$$

$$y_3 = -31 \; mod\ 11 \quad \Rightarrow$$

$$y_3 = -9 \; mod\ 11 \quad \Rightarrow$$

$$y_3 = 2 \; mod\ 11$$

Assim, obtém-se o ponto $2P_1 = P_1 + P_1 = (5, 2)$

3.2.5 Discriminante e j-invariante de uma Curva Elíptica

Nessa seção, serão definidos os conceitos de discriminante e j-invariante de uma Curva Elíptica. Para tal, utilizar-se-ão as equações da Curva Elíptica na sua Forma Generalizada de Weierstrass, pois, procedendo-se dessa forma, podem ser obtidos resultados mais gerais, aplicáveis também às Curvas Elípticas definidas sobre corpos de característica 2 e 3.

Seja a Curva Elíptica *E* definida sobre o corpo *K*, representada pela equação:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

com $x, y, a_1, \dots, a_6 \in K$ e $a_1, \dots, a_6$ constantes.

Definem-se os seguintes parâmetros:

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$
$$c_4 = b_2^2 - 24b_4$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$
$$j(E) = \frac{c_4^3}{\Delta} \quad \text{para } \Delta \neq 0$$

O parâmetro Δ é denominado discriminante da Curva Elíptica, e o parâmetro *j*(*E*) é denominado seu *j*–invariante. Pode-se demonstrar que uma Curva Elíptica é não-singular (suave) se, e somente se, seu discriminante é diferente de zero. Para uma prova desta afirmação, pode-se consultar (Enge, 1999). Porém, na seção 3.2.4, foi mostrado que uma Curva Elíptica, representada na sua Forma Reduzida de Weierstrass $y^2 = x^3 + Ax + B$, é denominada não-singular se $4A^3 + 27B^2 \neq 0$. Ora, não é muito difícil perceber que se trata de um caso particular contido no caso geral de $\Delta \neq 0$. Para a Forma Reduzida de Weierstrass, têm-se:

$$a_1 = a_2 = a_3 = 0$$

Portanto,

$b_2 = 0$
$b_4 = 2A$
$b_6 = 4B$
$b_8 = -A^2 \qquad \Rightarrow$
$\Delta = -8(2A)^3 - 27(4B)^2 = -16(4A^3 + 27B^2)$

Assim, quando se faz $\Delta \neq 0$, recai-se na condição anteriormente estabelecida $4A^3 + 27B^2 \neq 0$.

A verificação da não-singularidade de uma Curva Elíptica a partir de seu discriminante é bastante útil, haja vista a impossibilidade de se trabalhar de maneira geral com a Forma Reduzida de Weierstrass sobre corpos de característica 2 e 3. Quando a Curva Elíptica está definida sobre um corpo de característica diferente de 2 e 3, sempre é possível transformar sua equação da Forma Generalizada de Weierstrass para a Forma Reduzida (veja a seção 3.2.1).

O *j*-invariante de uma Curva Elíptica recebe esse nome porque, dadas duas Curvas Elípticas distintas E_1 e E_2, existe uma mudança de variáveis que transforma E_1 em E_2 se, e somente se, $j(E_1) = j(E_2)$. Nesse caso, as curvas E_1 e E_2 são denominadas isomorfas. Diz-se também, nesse caso, que a curva E_1 é o *twist* da curva E_2, e vice-versa (Washington, 2008). Para uma demonstração do resultado enunciado acima, pode-se consultar (Silverman, 1992). Pode-se mostrar também que todas as possíveis mudanças de variáveis que preservam a Forma Generalizada de Weierstrass de uma Curva Elíptica são da forma:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} u^2x + r \\ u^3y + u^2sx + t \end{pmatrix}$$

com $u \in K^\times$, $r, s, t \in K$.

Quando se aplica sobre uma Curva Elíptica a mudança de variáveis definida acima, com $u = -1$, $r = 0$, $s = -a_1$ e $t = -a_3$, obtém-se a seguinte transformação:

$$\binom{x}{y} \mapsto \binom{x}{-y - a_1 x - a_3}$$

Essa mudança de variáveis é denominada involução, pois, no grupo abeliano finito formado pelos pontos de uma Curva Elíptica, ela transforma um elemento (x, y) no seu inverso − (x, y) (para a Lei de Grupo definida na seção 3.2.4). Quando se trabalha com Curvas definidas sobre corpos de característica diferente de 2 e 3, sempre é possível transformar sua equação da Forma Generalizada de Weierstrass para a Forma Reduzida. Por isso, quando foi apresentado o conceito de elemento inverso na definição de Lei de Grupo na seção 3.2.4, este elemento foi denotado da seguinte forma: − (x, y) = (x, −y), que é um caso particular da definição acima, para as Curvas Elípticas representadas na sua Forma Reduzida de Weierstrass ($a_1 = a_3 = 0$). Na próxima seção, quando for definida a Lei de Grupo para Curvas Elípticas sobre corpos de característica 2 e 3, não será possível utilizar a definição particular de elemento inverso para Curvas representadas na Forma Reduzida, de forma que a definição para o caso geral será de suma importância.

3.2.6 Curvas Elípticas sobre Corpos de Característica 2 e 3

Quando se trabalha com Curvas Elípticas sobre corpos de característica 2 ou 3, não é possível representá-las de uma maneira geral por meio da Forma Reduzida de Weierstrass. Portanto, é necessário que se defina a Lei de Grupo para esse caso específico, apresentando uma formulação das suas equações baseada na Forma Generalizada de Weierstrass. A saber, a utilização de Curvas Elípticas sobre corpos de característica 2 (ou corpos finitos GF (2^n), com $n \in \mathbb{N}$) é bastante frequente nas aplicações computacionais de Curvas Elípticas, pois a aritmética dos processadores de computador é binária, de forma que a utilização de igualdades modulo 2 simplifica sobremaneira alguns processos de cálculo específicos. Porém, a utilização de Curvas Elípticas sobre corpos de característica 2 e 3 não apresenta uma abordagem muito intuitiva na prática, de forma que é necessária uma formulação bastante rigorosa das particularidades envolvidas na sua utilização. Por exemplo, ao se realizar o processo de

derivação da expressão y^2 em um corpo de característica 2, obtém-se a expressão $2yy' = 0$, pois nesse corpo todas as igualdades são modulo 2. O mesmo ocorre quando se realiza, por exemplo, a derivação da expressão y^3 em um corpo de característica 3. Dessa forma, torna-se evidente a necessidade de uma formulação algébrica mais generalista dos processos envolvendo Curvas Elípticas definidas sobre esses tipos de corpos.

Em todo o restante da seção, as Curvas Elípticas serão representadas por meio da sua Forma Generalizada de Weiesrtrass, haja vista a impossibilidade de sempre representá-las em sua Forma Reduzida.

Seja a Curva Elíptica *E* definida sobre um corpo *K*, de característica 2 ou 3, representada pela equação:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Procedendo-se de maneira análoga à seção 3.2.3, em coordenadas projetivas, obtém-se como único ponto no infinito da Curva o ponto (0 : 1 : 0). A seguir, será apresentada a definição da Lei de Grupo, bem como suas respectivas expressões, para o caso geral de Curvas representadas por equações na Forma Generalizada de Weierstrass.

Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos pertencentes à Curva Elíptica *E*, dada pela equação $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, com $\Delta \neq 0$. O ponto $P_3 = (x_3, y_3) = P_1 + P_2$, denominado "soma" de P_1 com P_2, é definido da seguinte forma:

Se $P_1 = P_2 = \infty$, então $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 = \infty$, então $P_3 = P_1 + P_2 = P_1 + \infty = P_1$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 = x_2 = x$, então para que os pontos P_1 e P_2 pertençam à Curva Elíptica e sejam distintos, é necessário que $y_2 = -y_1 - a_1x - a_3$, pois se tem:

$$x_1^3 + a_2x_1^2 + a_4x_1 + a_6 = x_2^3 + a_2x_2^2 + a_4x_2 + a_6 \quad \Rightarrow$$

$$y_1^2 + a_1xy_1 + a_3y_1 = y_2^2 + a_1xy_2 + a_3y_2 \quad \Rightarrow$$

$$y_2 = y_1 \quad \text{ou} \quad y_2 = -y_1 - a_1 x - a_3$$

Como não se pode ter $y_1 = y_2$, pois $P_1 \neq P_2$, então $y_2 = -y_1 - a_1 x - a_3$. Nesse caso, denota-se $P_2 = -P_1$, e tem-se $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 \neq x_2$, então

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2$$

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 - (a_1 x_3 + a_3)$$

Se $P_1 = P_2 = (x, y) \neq \infty$, então:

$$x_3 = \left(\frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}\right)^2 + a_1\left(\frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}\right) - a_2 - 2x$$

$$y_3 = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}(x - x_3) - y - (a_1 x_3 + a_3)$$

Como $\Delta \neq 0$, as expressões para x_3 e y_3 sempre estão definidas.

Essas são as fórmulas gerais para a soma de pontos de uma Curva Elíptica *E* qualquer não-singular, definida sobre um corpo *K* qualquer. É possível realizar várias simplificações nessas fórmulas, desde que seja conhecida a característica do corpo *K*. Por exemplo, as fórmulas apresentadas na seção 3.2.4, são simplificações realizadas para o caso em que a característica de *K* é diferente de 2 e 3.

Para o caso específico de Curvas Elípticas definidas sobre corpos de característica 2, seguem as fórmulas simplificadas:

Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos pertencentes à Curva Elíptica *E*, dada pela equação $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, com $\Delta \neq 0$, definida

sobre um corpo *K*, de característica 2. O ponto $P_3 = (x_3, y_3) = P_1 + P_2$, denominado "soma" de P_1 com P_2, é definido da seguinte forma:

Caso 1 - Se $j(E) \neq 0$, então $a_1 \neq 0$, pois $j(E) = \frac{{a_1}^{12}}{\Delta}$. Portanto, é possível realizar a seguinte mudança de variáveis:

$$(x, y) \longmapsto \left(a_1^2 x + \frac{a_3}{a_1},\ a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$

Dessa forma, a equação da Curva Elíptica assume a forma:

$$y^2 + xy = x^3 + \bar{a}_2 x^2 + \bar{a}_6$$

Então:

Se $P_1 = P_2 = \infty$, então $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 = \infty$, então $P_3 = P_1 + P_2 = P_1 + \infty = P_1$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 = x_2 = x$, então para que os pontos P_1 e P_2 pertençam à Curva Elíptica e sejam distintos, é necessário que $y_2 = -y_1 - x$, pois se tem:

$x_1^3 + \bar{a}_2 x_1^2 + \bar{a}_6 = x_2^3 + \bar{a}_2 x_2^2 + \bar{a}_6 \quad \Rightarrow$

$y_1^2 + x y_1 = y_2^2 + x y_2 \quad \Rightarrow$

$y_2 = y_1 \quad \text{ou} \quad y_2 = -y_1 - x$

Como não se pode ter $y_1 = y_2$, pois $P_1 \neq P_2$, então $y_2 = -y_1 - x$. Nesse caso, denota-se $P_2 = -P_1$, e tem-se $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 \neq x_2$, então

$$x_3 = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + \left(\frac{y_2 + y_1}{x_2 + x_1}\right) + \bar{a}_2 + x_1 + x_2$$

$$y_3 = \frac{y_2 + y_1}{x_2 + x_1}(x_1 + x_3) + y_1 + x_3$$

Se $P_1 = P_2 = (x, y) \neq \infty$, então:

$$x_3 = x^2 + \frac{\bar{a}_6}{x^2}$$

$$y_3 = \frac{x^2 + y}{x} x_3 + x^2 + x_3$$

Caso 2 - Se $j(E) = 0$, realiza-se a seguinte mudança de variáveis:

$$(x, y) \longmapsto (x + a_2, y)$$

Dessa forma, a equação da Curva Elíptica assume a forma:

$$y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6$$

Então:

Se $P_1 = P_2 = \infty$, então $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 = \infty$, então $P_3 = P_1 + P_2 = P_1 + \infty = P_1$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 = x_2 = x$, então para que os pontos P_1 e P_2 pertençam à Curva Elíptica e sejam distintos, é necessário que $y_2 = -y_1 - \bar{a}_3$, pois se tem:

$$x_1^3 + \bar{a}_4 x_1 + \bar{a}_6 = x_2^3 + \bar{a}_4 x_2 + \bar{a}_6 \quad \Rightarrow$$

$$y_1^2 + \bar{a}_3 y_1 = y_2^2 + \bar{a}_3 y_2 \quad \Rightarrow$$

$$y_2 = y_1 \quad \text{ou} \quad y_2 = -y_1 - \bar{a}_3$$

Como não se pode ter $y_1 = y_2$, pois $P_1 \neq P_2$, então $y_2 = -y_1 - \bar{a}_3$. Nesse caso, denota-se $P_2 = -P_1$, e tem-se $P_3 = P_1 + P_2 = \infty$

Se $P_1 \neq P_2 \neq \infty$, e $x_1 \neq x_2$, então

$$x_3 = \left(\frac{y_2+y_1}{x_2+x_1}\right)^2 + x_1 + x_2$$

$$y_3 = \frac{y_2 + y_1}{x_2 + x_1}(x_1 + x_3) + y_1 + \bar{a}_3$$

Se $P_1 = P_2 = (x, y) \neq \infty$, então:

$$x_3 = \left(\frac{x^2 + \bar{a}_4}{\bar{a}_3}\right)^2$$

$$y_3 = \frac{x^2 + \bar{a}_4}{\bar{a}_3}(x + x_3) + y + \bar{a}_3$$

3.2.7 Multiplicação por um Escalar

Seja *P* um ponto pertencente a uma Curva Elíptica *E* definida sobre um corpo *K*, e seja *k* um inteiro não nulo. Define-se o produto *kP* como a soma *P* + *P* + ... + *P*, com *k* elementos, para *k > 0*. Se *k* < 0, então *kP = (-k).(-P) = (-P)* + *(-P)* + ... + *(-P)*. Uma estratégia interessante para se proceder à multiplicação *kP* é realizar sucessivas duplicações de *P*, até uma certa potência *n* de 2, tal que $2^n < k < 2^{n+1}$. A partir dos valores de *P, 2P, 4P, 8P, ... ,* 2^nP é possível obter-se o produto *kP* efetuando-se poucas adições. Em aplicações criptográficas de Curvas Elípticas, costuma-se trabalhar com valores bastante elevados de *k*, o que justifica a adoção da estratégia das sucessivas duplicações. Porém, à primeira vista, pode parecer que a adoção da estratégia das duplicações sucessivas possui um grave inconveniente, pois a necessidade de se armazenarem os valores de *P, 2P, 4P...* demandaria uma parcela considerável de memória, ao passo que a soma sucessiva dos valores de *P* não demandaria o

armazenamento de qualquer valor além da soma anterior efetuada. Essa aparente desvantagem do processo de duplicações sucessivas não se perpetua na prática, pois nas aplicações criptográficas utilizam-se Curvas Elípticas definidas sobre corpos finitos. Dessa forma, à medida que os valores de *P, 2P, 4P...* vão crescendo e, consequentemente, requisitando mais memória para se armazená-los, pode-se proceder uma redução modulo *p* (supondo, sem perda de generalidade, que o corpo finito sob o qual está definida a curva possui *p* elementos) de cada um dos valores duplicados, reduzindo-se assim substancialmente a necessidade de memória extra para armazená-los. Vale salientar que esse procedimento só pode ser aplicado devido à propriedade associativa da soma de pontos em uma Curva Elíptica.

3.2.8 Ordem de uma Curva Elíptica e o Teorema de Hasse

Define-se ordem de uma Curva Elíptica *E* sobre um corpo *K*, e denota-se por #*E*, a quantidade de pares ordenados (*x*, *y*) pertencentes à Curva, mais o Ponto no Infinito.

Por exemplo, seja a Curva Elíptica *E* definida sobre o corpo $\mathbb{Z}_{11}$, dada pela equação $y^2 = x^3 + x + 6$ (essa curva já foi utilizada no Exemplo 2, da seção 3.2.4). Uma maneira possível de se encontrar a ordem da Curva é determinar todos os seus pontos. Isso pode ser feito por tentativas sucessivas, por exemplo, fazendo *x* = 0, 1, 2, ...,10 e verificando quais os valores de *y* correspondentes satisfazem à equação da Curva modulo 11. Dessa forma, podem-se encontrar os seguintes pontos: (2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2) e (10, 9). Além desses pontos (finitos), há ainda o Ponto no Infinito, que pertence à Curva pela sua própria definição. Portanto, como a Curva possui 13 pontos, sua ordem #*E* = 13.

Pode-se mostrar também que, como uma Curva Elíptica *E* definida sobre um corpo finito apresenta a estrutura de um grupo abeliano aditivo finito, se a ordem #*E* dessa Curva é um número primo, o grupo formado por seus pontos é cíclico. Denotando-se #*E* = *n*, pode-se mostrar que o grupo formado pelos pontos da Curva Elíptica *E* é isomorfo à $\mathbb{Z}_n$ (Washington, 2008), e cada ponto da Curva (com exceção do Ponto no Infinito) é uma raiz primitiva desse grupo (consequência direta do Teorema de Lagrange, pois a ordem de cada um dos elementos deve ser um divisor da ordem do grupo. Como a ordem do grupo é prima, seus únicos divisores são 1 e *n*). Dessa forma, a

ordem $\#E$ da Curva pode ser definida como o menor $n \in \mathbb{N}$, tal que nP = Ponto no Infinito.

Para aplicações criptográficas de Curvas Elípticas, é fundamental que se conheça a ordem da Curva sobre um corpo finito K, pois o número de pontos pertencentes à Curva nesse corpo é um dos principais parâmetros a serem escolhidos quando se estabelece um protocolo de criptografia com base em Curvas Elípticas. Porém, quando se utilizam corpos de ordem elevada, torna-se impraticável determinar a ordem da Curva Elíptica encontrando-se todos os seus pontos e os contando. Portanto, é fundamental que se conheça a ordem da Curva sem que seja necessário determinar todos os seus pontos. O teorema seguinte fornece uma boa ideia da ordem de uma Curva Elíptica, sem que seja necessário se encontrar todos os seus pontos.

Teorema de Hasse:

Seja uma Curva Elíptica E definida sobre um corpo finito K com q elementos. Então, a ordem de E satisfaz a seguinte relação:

$$-2\sqrt{q} \leq q + 1 - \#E \leq 2\sqrt{q}$$

Realizando-se algumas manipulações nas desigualdades, obtém-se o seguinte intervalo de valores para a ordem da Curva Elíptica E:

$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$$

Portanto, utilizando-se o Teorema de Hasse, pode-se estabelecer um intervalo de valores possíveis para a ordem da Curva E. Em aplicações práticas, pode-se utilizar o Teorema de Hasse juntamente com o Teorema de Lagrange, que estabelece que para todo grupo finito G, a ordem de qualquer subgrupo H de G divide a ordem de G. Dessa forma, quando se conhece a ordem de algum subgrupo de G, sabe-se que se trata de um divisor da ordem do grupo G. Para uma aplicação no contexto das Curvas Elípticas definida sobre corpos finitos, quando se conhece a ordem de algum de seus pontos, sabe-se que se trata de um divisor da ordem da própria Curva. Essa informação, juntamente com o intervalo fornecido pelo Teorema de Hasse, muitas vezes é suficiente para se estabelecer a ordem da Curva Elíptica. Para o caso particular de se conhecer a

ordem de uma raiz primitiva (mesmo que não se saiba previamente que tal ponto seja uma raiz primitiva) da Curva Elíptica *E*, a união das duas informações (ordem do ponto e Teorema de Hasse) sempre possibilita a determinação exata da ordem de *E*.

Muitas vezes, conhece-se a ordem de uma Curva Elíptica definida sobre um corpo finito pequeno *K* com q elementos, e deseja-se conhecer a ordem dessa mesma Curva definida sobre um corpo finito *K* com q^n elementos, para algum $n \in \mathbb{N}$. Nesses casos, pode-se recorrer ao seguinte teorema:

Seja a ordem de uma Curva Elíptica *E* definida sobre um corpo finito *K*, com q elementos, dada por $\#E = q + 1 - a$, para algum inteiro a. Então, a ordem de *E* definida sobre um outro corpo finito *K'*, com q^n, é dada por $q^n + 1 - (\gamma^n + \beta^n)$, sendo γ e β determinados pela equação $x^2 - ax + q = (x - \gamma)(x - \beta)$.

Esse teorema é bastante útil, pois possibilita que se conheça a ordem de uma Curva Elíptica definida sobre um corpo finito com uma quantidade grande de elementos, conhecendo-se apenas a ordem da Curva definida sobre um corpo finito com um número bem menor de elementos, desde que a quantidade de elementos do primeiro corpo seja uma potência da quantidade de elementos do segundo corpo.

Como exemplo de aplicação prática dos teoremas definidos acima, juntamente com o Teorema de Lagrange, a seguir serão apresentados alguns exemplos numéricos.

Exemplo 1 - Seja uma Curva Elíptica *E* definida sobre um corpo finito *K* com 79 elementos, descrita pela seguinte equação:

$$y^2 = x^3 + 10x + 5$$

De acordo com o Teorema de Hasse, como $q = 79$, tem-se:

$$63 \leq \#E \leq 97$$

Seja o ponto $P = (30, 45)$, pertencente a *E*. Pode-se mostrar (utilizando-se, de acordo com (Washington, 2008), o método *Baby Step, Giant Step*) que sua ordem é 85. Isto é, o menor $n \in \mathbb{N}$, tal que nP = Ponto no Infinito, ocorre quando $n = 85$. Portanto, a ordem da Curva *E* é um múltiplo de 85. Como o único múltiplo de 85 pertencente ao

intervalo acima é o próprio 85, conclui-se que a ordem da Curva é exatamente 85. Em outras palavras, $\#E = 85$.

Exemplo 2 - Seja uma Curva Elíptica *E* definida sobre um corpo finito *K* com 103 elementos, descrita pela seguinte equação:

$$y^2 = x^3 + 7x + 12$$

De acordo com o Teorema de Hasse, como $q = 103$, tem-se:

$$84 \leq \#E \leq 124$$

Sejam os pontos $P = (19, 0)$ e $Q = (102, 2)$, pertencentes a *E*. Pode-se mostrar que a ordem de *P* é 2, e a ordem de *Q* é 13. Portanto, a ordem da Curva Elíptica *E* é um múltiplo de $13 \times 2 = 26$. Como 104 é o único múltiplo de 26 pertencente ao intervalo acima, conclui-se que a ordem da Curva é 104. Isto é, $\#E = 104$.

Exemplo 3 - Seja uma Curva Elíptica *E* definida sobre um corpo finito *K* com 13 elementos, descrita pela seguinte equação:

$$y^2 = x^3 + 10x + 5$$

Sabe-se que a ordem de *E* definida sobre *K* é 10. Sabe-se também que:

$$\#E = q + 1 - a$$

Portanto:

$$10 = 13 + 1 - a \quad \Rightarrow$$

$$a = -4$$

Como:

$$x^2 - ax + q = (x - \gamma)(x - \beta)$$

Obtém-se então a seguinte equação:

$$x^2 + 4x + 13 = (x - \gamma)(x - \beta) \quad \Rightarrow$$

$$\gamma = -2 + 3i \quad \beta = -2 - 3i$$

Para se determinar a ordem da Curva *E* definida sobre um outro corpo finito *K'*, com, por exemplo, $13^5 = 371293$ elementos, basta calcular:

$$\#E \text{ sobre } K' = q^n + 1 - (\gamma^n + \beta^n) \quad \Rightarrow$$

$$\#E \text{ sobre } K' = 13^5 + 1 - ((-2 + 3i)^5 + (-2 - 3i)^5) \quad \Rightarrow$$

$$\#E \text{ sobre } K' = 371293 + 1 + 244 = 371538$$

A demonstração do Teorema de Hasse pode ser encontrada em (Washington, 2008), e a do Teorema de Lagrange em (Garcia, et al., 2002).

3.3 Funcionamento do Algoritmo de Curvas Elípticas

3.3.1 Introdução

Nas seções 3.2.4 e 3.2.7, foi apresentada a metodologia utilizada para se calcular o produto *kP*, dado um ponto *P* pertencente a uma Curva Elíptica *E*, e um inteiro não nulo *k*. A partir da descrição das técnicas utilizadas para se realizar o cálculo do produto, torna-se evidente que se trata de um processo computacionalmente simples, isto é, dado o ponto *P* e o inteiro *k*, é computacionalmente simples se obter o ponto *kP*. Porém, o processo inverso é computacionalmente bastante complexo. A partir dos valores de *P* e *kP,* é consideravelmente complicado obter-se o valor de *k*. Esse tipo de problema é denominado Problema do Logaritmo Discreto para Curvas Elípticas. Trata-se de um tipo de "função de uma única via" (Aguiar, 2008), e o processo criptográfico

baseado em Curvas Elípticas utilizará exatamente essa característica como suporte para o seu funcionamento.

3.3.2 Problema do Logaritmo Discreto sobre Corpos Finitos

Seja p um número primo, e sejam a e b inteiros não nulos modulo p. Supondo-se que exista um inteiro k, tal que:

$$a^k \equiv b \pmod{p}$$

Então, o problema que consiste em se determinar k, dados os valores de a, b e p, é denominado Problema do Logaritmo Discreto. Vale salientar que o valor de k, tal que $a^k \equiv b \pmod{p}$, não é único, haja vista que qualquer $k' = k + n(p-1)$, $n \in \mathbb{N}$, também é solução da equação modular. Para que não seja necessário se trabalhar com múltiplas soluções para a equação, costuma-se representar a sua solução por k mod (p – 1), eliminando-se assim a necessidade de tratamento de múltiplas raízes.

Pode-se definir o Problema do Logaritmo Discreto de maneira mais abrangente. De maneira análoga à definição acima, apresentada para o caso de a, b pertencentes ao grupo multiplicativo dos inteiros, pode-se definir o Problema do Logaritmo Discreto para qualquer grupo multiplicativo G, tal que $a, b \in G$, e deseja-se determinar k, tal que $a^k = b$. Para o contexto criptográfico da aplicação de Curvas Elípticas, define-se como Problema do Logaritmo Discreto para Curvas Elípticas o seguinte problema:

Sejam P e Q pontos pertencentes a uma Curva Elíptica E, definida sobre um corpo K. Então, sabendo-se que $kP = Q$, para algum inteiro k, e conhecendo-se os parâmetros E, K, P e Q, deseja-se encontrar k. Esse problema é denominado Problema do Logaritmo Discreto para Curvas Elípticas.

Toda a aplicação criptográfica de Curvas Elípticas se baseia em algumas propriedades desse problema. A principal delas consiste em, dados E, K, P e k, é computacionalmente simples se determinar Q. Porém, dados E, K, P e Q, é computacionalmente complexo o processo para se determinar k. Dessa forma, desde que sejam respeitadas algumas restrições acerca da escolha da Curva E e do corpo K, toda a

segurança do processo criptográfico baseado em Curvas Elípticas depende da dificuldade de se resolver o Problema do Logaritmo Discreto para Curvas Elípticas em tempo reduzido (polinomial).

3.4 Exemplo de Utilização do Algoritmo de Curvas Elípticas

Nesta seção, serão descritas as metodologias de funcionamento de algumas aplicações criptográficas de Curvas Elípticas. Por bem da simplicidade, será adotada a sigla ECC (*Elliptic Curve Cryptography*) quando necessário, para se designar aplicações criptográficas de Curvas Elípticas.

3.4.1 Representação de Mensagens como Pontos de Curvas Elípticas

Conforme apresentado na seção 3.3.2, os algoritmos de ECC se baseiam no seguinte problema: dados dois pontos P e Q pertencentes a uma Curva Elíptica E, definida sobre um corpo K, sabendo-se que $kP = Q$, para algum inteiro k, e conhecendo-se os parâmetros E, K, P e Q, deseja-se encontrar k. Porém, inicialmente, é necessário se atribuir uma correspondência entre a mensagem a ser criptografada em um valor numérico, para que as operações matemáticas pertinentes possam ser realizadas. Na maioria dos sistemas criptográficos, isso pode ser executado de maneira bastante simples, por exemplo, utilizando-se para tal o padrão ASCII. Porém, quando se utilizam algoritmos de ECC, é necessário que se atribua uma relação entre a mensagem a ser criptografada e um ponto pertencente à Curva Elíptica utilizada no processo, para que as operações matemáticas relacionadas à ECC possam ser executadas. Dessa forma, a mensagem a ser criptografada é inicialmente transformada em um ponto da Curva Elíptica e, após a realização das operações matemáticas pertinentes, obtém-se um novo ponto também pertencente à Curva Elíptica. Esse novo ponto constitui a própria mensagem criptografada, a ser enviada para o destinatário.

Portanto, é necessário utilizar-se um método de conversão entre uma mensagem m a ser criptografada e um ponto pertencente à Curva Elíptica utilizada no processo. Há vários métodos conhecidos para tal, e nesta seção será apresentado um método desenvolvido por Neal Koblitz. Trata-se de um método probabilístico, que estabelece uma relação entre a mensagem m (já previamente convertida em um valor numérico, por exemplo, utilizando-se o padrão ASCII) e um ponto da Curva Elíptica utilizada, com

uma probabilidade de sucesso de $1 - \frac{1}{2^T}$. Dessa forma, controlando-se o valor do parâmetro *T*, pode-se limitar em valores bem pequenos a probabilidade de fracasso do método. Segue uma descrição detalhada do método:

Seja uma Curva Elíptica *E* definida sobre um corpo *K* com característica *p*, dada pela equação $y^2 = x^3 + Ax + B$. Seja m a mensagem que se quer criptografar, já previamente convertida em um valor numérico. Estabelece-se o valor do parâmetro $T \in \mathbb{N}^*$, tal que $\frac{1}{2^T}$ seja o máximo valor aceitável para a probabilidade de o método falhar. Deve-se ter $0 \leq m < \frac{p}{T}$. Caso $m \geq \frac{p}{T}$, deve-se quebrar a mensagem *m* em duas outras mensagens menores, e criptografá-las separadamente.

Seja $x_j = Tm + j$, para $0 \leq j < T$. Para cada um dos valores de x_j, deve-se calcular $s_j = x_j^3 + Ax_j + B$.

Se $s_j^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, então s_j é um quadrado modulo *p*, e a equação da Curva Elíptica está satisfeita para o ponto $(x_j, \sqrt{s_j})$. Para se recuperar a mensagem *m* a partir do ponto $(x_j, \sqrt{s_j})$, basta se calcular:

$$m = \left[\frac{x_j}{T} \right]$$

em que $\left[\frac{x_j}{T} \right]$ representa o maior inteiro menor ou igual a $\frac{x_j}{T}$.

Dessa forma, procedendo-se por tentativas, calcula-se s_j até que se encontre um quadrado modulo *p*, ou até que se tenha $j = T$ e nenhum quadrado modulo *p* tenha sido encontrado. Nesse caso, o método falhou. Porém, desde que se escolha um valor adequado para *T*, a probabilidade de falha do método pode ser limitada em valores bastante pequenos. Como cada um dos s_j é, em tese, um elemento aleatório de *K*, a probabilidade de s_j ser um quadrado modulo *p* é de aproximadamente $\frac{1}{2}$. Como faz-se *j* variar de 0 a $(T - 1)$, então a probabilidade de nenhum dos pontos s_j corresponder a um quadrado modulo *p* é de aproximadamente $\frac{1}{2^T}$. A seguir, será apresentado um exemplo numérico a título de ilustração.

Seja a Curva Elíptica $y^2 = x^3 + 2x + 7$, definida sobre o corpo $\mathbb{Z}_{179}$. Admitindo-se uma probabilidade de falha do método de aproximadamente $\frac{1}{2^{20}} = 0{,}00000095$,

toma-se $T = 20$. Seja $m = 5$ a mensagem que se quer criptografar. Então, faz-se $x_j = 100 + j$, para $0 \leq j < 20$. Para $j = 4$, tem-se $104^3 + 2 \times 104 + 7 \equiv 64 \pmod{179}$. Como $64 \equiv 8^2 \pmod{179}$, então a mensagem $m = 5$ pode ser representada pelo ponto $P_m = (104, 8)$. Para se recuperar a mensagem m a partir do ponto P_m, basta fazer-se $m = \left[\frac{104}{20}\right] = 5$, que de fato é o valor que se esperava encontrar.

3.4.2 Sistemas Criptográficos baseados em Curvas Elípticas

Existem vários sistemas criptográficos que utilizam algoritmos baseados em Curvas Elípticas, em particular, algoritmos envolvendo o Problema do Logaritmo Discreto. Como exemplos, podem ser citados os modelos de troca de chaves de Diffie-Hellman, o modelo de encriptação de Massey-Omura, o modelo Menezes-Vanstone e vários outros. Nesta seção, será abordado o modelo ElGamal de encriptação baseado em Curvas Elípticas, e na seção 3.5 o modelo ElGamal para Assinatura Digital. Para uma descrição mais detalhada de outros sistemas criptográficos baseados em Curvas Elípticas, podem ser consultadas as referências (Washington, 2008) e (Aguiar, 2008).

Inicialmente, será apresentado o modelo criptográfico ElGamal na sua versão original e, em seguida, será apresentada a sua versão para Curvas Elípticas.

Modelo Criptográfico ElGamal

Duas entidades *A* e *B* desejam trocar mensagens criptografadas utilizando-se para isso o sistema Criptográfico ElGamal. Trabalhar-se-á com o caso em que a entidade *A* deseja enviar uma mensagem *m*, criptografada, para a entidade *B*. O caso inverso é absolutamente análogo. Primeiramente, é necessário que *B* escolha a sua chave privada, e divulgue a chave pública associada à chave privada escolhida. Então, *B* escolhe um número primo grande *p*, um número inteiro γ modulo *p* e um outro número inteiro *a*. Em seguida, *B* calcula $\beta \equiv \gamma^a \pmod{p}$, divulga *p*, γ e β como sua chave pública e mantém *a* secreto, como sua chave privada. A entidade *A*, que deseja enviar a mensagem *m* para a entidade *B*, escolhe então aleatoriamente um número inteiro *k* e calcula os seguintes valores:

$$y_1 \equiv \gamma^k \pmod{p}$$
$$y_2 \equiv m\beta^k \pmod{p}$$

A entidade *A* envia então (y_1, y_2) para a entidade *B*. Essa é a mensagem criptografada. Para descriptografá-la, *B* calcula:

$$m \equiv y_2 y_1^{-a} \pmod{p}$$

obtendo assim a mensagem original.

Esse procedimento funciona, pois:

$$y_2 y_1^{-a} \equiv m\beta^k (\gamma^k)^{-a} \pmod{p} \quad \Rightarrow$$
$$y_2 y_1^{-a} \equiv m(\gamma^a)^k (\gamma^k)^{-a} \pmod{p} \quad \Rightarrow$$
$$y_2 y_1^{-a} \equiv m(\gamma^k)^a (\gamma^k)^{-a} \pmod{p} \quad \Rightarrow$$
$$y_2 y_1^{-a} \equiv m \pmod{p}$$

A seguir, será apresentada a versão do modelo criptográfico ElGamal para Curvas Elípticas.

Modelo Criptográfico ElGamal para Curvas Elípticas

Duas entidades *A* e *B* desejam trocar mensagens criptografadas utilizando-se para isso o sistema Criptográfico ElGamal para Curvas Elípticas. Analogamente ao modelo descrito anteriormente, trabalhar-se-á com o caso em que a entidade *A* deseja enviar uma mensagem *m*, criptografada, para a entidade *B*. O caso inverso é absolutamente análogo. Primeiramente, é necessário que *B* escolha a sua chave privada, e divulgue a chave pública associada à chave privada escolhida. Então, *B* escolhe uma Curva Elíptica *E* e um corpo finito *K*, tais que o Problema do Logaritmo Discreto seja difícil de ser resolvido quando a Curva *E* está definida sobre *K*. A entidade *B* também escolhe um ponto $P \in E$, tal que a ordem de *P* possua, pelo menos, um fator primo grande. Isso é necessário, pois assim previne-se um tipo de ataque ao Problema do Logaritmo Discreto denominado método de Pohlig-Hellman. Na prática, muitas vezes toma-se um ponto *P*,

tal que sua ordem seja um número primo grande, sem outros fatores. Por fim, *B* também escolhe um número inteiro *s*, e calcula $Q = sP$. Então, *B* divulga *E*, *K*, *P* e *Q* como sua chave pública e mantém *s* secreto, como sua chave privada. A entidade *A*, que deseja enviar a mensagem *m* para a entidade *B*, procede da seguinte maneira:

1. Toma conhecimento da chave pública (*E*, *K*, *P* e *Q*) de *B*.
2. Expressa sua mensagem *m* como um ponto $M \in E$. Isso pode ser feito utilizando-se o método descrito na seção 3.4.1.
3. Escolhe, aleatoriamente, um número inteiro *k*, calcula $M_1 = kP$, e mantém *k* em segredo.
4. Calcula também $M_2 = M + kQ$.

A entidade *A* envia então (M_1, M_2) para a entidade *B*. Essa é a mensagem criptografada. Para descriptografá-la, *B* calcula:

$$M = M_2 - sM_1$$

obtendo assim a mensagem original.

Esse procedimento funciona, pois:

$$M_2 - sM_1 = (M + kQ) - s(kP) \quad \Rightarrow$$
$$M_2 - sM_1 = M + k(sP) - skP \quad \Rightarrow$$
$$M_2 - sM_1 = M$$

Supondo-se que o canal utilizado por *A* para transmitir a mensagem criptografada para *B* não seja seguro, e haja uma entidade espiã *C* capaz de interceptar a mensagem (M_1, M_2) enviada por *A*. A entidade *C* também conhece (*E*, *K*, *P* e *Q*), que constituem a chave pública de *B*. A partir dessas informações, para que a entidade *C* consiga obter a mensagem *M*, é necessário que ela conheça *s* e calcule $M = M_2 - sM_1$, ou que ela conheça *k* e calcule $M = M_2 - kQ$. Porém, como $Q = sP$, para se obter *s* a partir de *P* e *Q*, é necessário que a entidade *C* resolva o Problema do Logaritmo Discreto para Curvas Elípticas, o qual, para o caso de uma boa escolha de *E*, *K* e *P*, é extremamente complexo de ser resolvido computacionalmente (não se conhecem

algoritmos que o resolvam em tempo polinomial). O mesmo ocorre quando se tenta obter k a partir de M_1 e P, pois $M_1 = kP$. Dessa forma, está assegurada a segurança do algoritmo. A seguir, será apresentado um exemplo numérico a título de ilustração.

Supondo-se que uma entidade *A* deseja enviar uma mensagem *m*, representada pelo ponto $M = (5, 1743)$ para uma entidade *B*. A entidade *B* publicou sua chave pública como sendo:

E: $y^2 = x^3 + 3x + 45$
K: $\mathbb{Z}_{8831}$
$P = (4, 11)$

Secretamente, *B* escolheu $s = 3$, e também publicou o ponto $Q = 3P = (413, 1808)$ como sua chave pública.

A entidade *A* escolhe aleatoriamente um número inteiro $k = 8$, por exemplo, e calcula:

$M_1 = 8P = (5415, 6321)$
$M_2 = M + 8Q = (6626, 3576)$

Então *A* mantém *k* em segredo, e envia para *B* a mensagem criptografada (M_1, M_2). Para descriptografá-la, *B* calcula:

$M = M_2 - 3M_1 = (5, 1743)$

obtendo-se assim a mensagem original.

3.4.3 Restrições para a Utilização de Curvas Elípticas em Criptografia

Vale ressaltar que algumas classes especiais de Curvas Elípticas devem ser evitadas para a aplicação criptográfica, a saber, as Curvas denominadas Supersingulares e Anômalas.

Seja uma Curva Elíptica E definida sobre um corpo K com $q = p^m$ elementos (p primo e m inteiro. O número p é denominado característica de K), e $\#E = q + 1 - a$. A Curva E é denominada Supersingular se p divide a. Em outras palavras, a Curva E é denominada Supersingular se $a \equiv 0 \pmod{p}$. Se $p = 2$ ou $p = 3$, pode-se mostrar que a Curva E é Supersingular se, e somente se, $j(E) = 0$. As Curvas Supersingulares devem ser evitadas porque o Problema do Logaritmo Discreto em Curvas Elípticas para essa classe de Curvas, quando submetido a um ataque conhecido como ataque MOV (Menezes, Okamoto, Vanstone), pode ser convertido em um Problema do Logaritmo Discreto convencional, consideravelmente mais simples de ser resolvido utilizando-se para tal o ataque denominado *Index Calculus*. Para mais detalhes acerca desses métodos de ataque, podem ser consultadas as referências (Menezes, 1993) e (Washington, 2008).

Seja uma Curva Elíptica E definida sobre um corpo K com q elementos. A Curva E é denominada Anômala, se $\#E = q$. Vale ressaltar que uma Curva Elíptica E Anômala quando definida sobre um corpo K não necessariamente será Anômala quando definida sobre um corpo K'. As Curvas Anômalas devem ser evitadas porque o Problema do Logaritmo Discreto em Curvas Elípticas para essa classe de Curvas pode ser resolvido de maneira consideravelmente rápida, comprometendo-se assim a segurança do processo criptográfico. Para uma demonstração desse resultado, pode ser consultado (Washington, 2008).

Também se deve ressaltar que a escolha da Curva Elíptica E, do corpo K sobre o qual ela está definida e do ponto $P \in E$ utilizado no processo de troca de mensagens deve respeitar algumas condições. Seja $Q = kP$ o Problema do Logaritmo Discreto sob o qual se baseia o protocolo criptográfico utilizado para a troca de mensagens entre duas entidades. Seja n a ordem do ponto P. Então, para se garantir a segurança do processo criptográfico, deve-se sempre utilizar um ponto P cuja ordem n possua ao menos um fator primo "grande", pois caso n possa ser decomposto em fatores primos "pequenos", o Problema do Logaritmo Discreto torna-se frágil diante de um ataque conhecido como método de Pohlig-Hellman. Consequentemente, devem-se sempre utilizar Curvas Elípticas E, tais que $\#E$ possua ao menos um fator primo "grande", pois, caso contrário, de acordo com o Teorema de Lagrange, não haveria pontos $P \in E$ com fatores primos "grandes", o que tornaria o processo susceptível ao ataque de Pohlig-Hellman. Para

mais detalhes sobre o método, podem ser consultados (Enge, 1999) e (Washington, 2008).

3.5 Utilização do Algoritmo de Curvas Elípticas em Assinatura Digital

Conforme apresentado na seção 1.3, quando se utilizam algoritmos criptográficos assimétricos, surge naturalmente a necessidade de se verificar a integridade e a autenticidade das mensagens recebidas por um receptor, pois qualquer entidade conhecedora da sua chave pública pode lhe enviar mensagens. Dessa forma, é necessário que a entidade emissora "assine" digitalmente a mensagem, conforme metodologia já apresentada na seção 1.3. Na realidade, a entidade emissora não assina a própria mensagem, mas sim o seu *Hash*.

Na seção 2.5, foi apresentada a metodologia de funcionamento de um processo de assinatura digital utilizando-se como base o algoritmo RSA. Analogamente, nesta seção será apresentado um modelo de assinatura digital utilizando-se como base um algoritmo de ECC.

Modelo Criptográfico ElGamal de Assinatura Digital com Curvas Elípticas

Supondo-se que uma entidade emissora A deseja enviar uma mensagem (não secreta) assinada digitalmente para uma entidade receptora B (na realidade, A não envia a própria mensagem assinada, mas sim o seu *Hash*). Primeiramente, a entidade A escolhe uma Curva Elíptica E e um corpo finito K, tais que o Problema do Logaritmo Discreto seja difícil de ser resolvido quando a Curva E está definida sobre K. A também escolhe um ponto $P \in E$, tal que a ordem de P possua, pelo menos, um fator primo grande. A ordem de P será representada por N. Na prática, escolhe-se um ponto P, tal que sua ordem N seja um número primo grande, sem outros fatores. Por fim, a entidade A escolhe um número inteiro a, calcula $Q = aP$ e escolhe também uma função $f : E \rightarrow \mathbb{Z}$ que relaciona cada ponto da Curva E com um número inteiro. A título de exemplo, utilizar-se-á a função $f(x, y) = x$, que relaciona a cada ponto $P = (x, y) \in E$ um número inteiro x, representado pela sua própria coordenada. A entidade A então divulga

E, *K*, *f*, *P* e *Q*, e mantém *a* em segredo. Para enviar a mensagem assinada digitalmente para a entidade *B*, a entidade *A* procede da seguinte maneira:

1. Expressa a mensagem a ser enviada assinada como um número inteiro *m*, tal que $m \leq N$. Na prática, o número inteiro *m* expressa o *Hash* da mensagem a ser assinada. Caso $m > N$, deve-se escolher uma outra Curva Elíptica de ordem maior.
2. Escolhe um número inteiro aleatório *k*, tal que MDC (*k, N*) = 1, e calcula $R = kP$.
3. Em seguida, calcula $s \equiv k^{-1}\big(m - af(R)\big) \pmod{N}$.
4. Envia então (*m*, *R*, *s*) como a mensagem assinada para *B*. Vale ressaltar que *m* e *s* são números inteiros, e *R* é um ponto de *E*.

Para verificar a autenticidade da assinatura de *A*, a entidade *B* procede da seguinte maneira:

1. Toma conhecimento dos parâmetros *E*, *K*, *f*, *P* e *Q* publicados por *A*.
2. Calcula $V_1 = f(R)Q + sR$.
3. Calcula $V_2 = mP$.
4. Se $V_1 = V_2$, então *B* considera a assinatura autêntica.

Esse procedimento é válido, pois:

$$V_1 = f(R)Q + sR \qquad \Rightarrow$$
$$V_1 = f(R)aP + skP$$

Como $s \equiv k^{-1}\big(m - af(R)\big) \pmod{N}$, então $sk = m - af(R) + zN$, com z $\in$ $\mathbb{Z}$. Então:

$$skP = \big(m - af(R)\big)P + zNP$$

Mas $NP =$ Ponto no Infinito da Curva Elíptica *E*, pois *N* representa a ordem do ponto *P*. Como o Ponto no Infinito é o próprio elemento neutro da Lei de Grupo para Curvas Elípticas, definida na seção 3.2.4, tem-se que:

$$skP = \big(m - af(R)\big)P + zNP = \big(m - af(R)\big)P$$

Portanto:

$$V_1 = f(R)aP + skP \quad \Rightarrow$$
$$V_1 = f(R)aP + \big(m - af(R)\big)P \quad \Rightarrow$$
$$V_1 = mP = V_2$$

Dessa forma, para que uma entidade estranha *C* possa assinar uma mensagem tentando se passar pela entidade *A*, é necessário que *C* conheça *a* e *k* para calcular $s \equiv k^{-1}\big(m - af(R)\big) \pmod N$ e $R = kP$, respectivamente. Porém, como $Q = aP$, para se obter *a* a partir de *P* e *Q*, é necessário que a entidade *C* resolva o Problema do Logaritmo Discreto para Curvas Elípticas, o qual, para o caso de uma boa escolha de *E*, *K* e *P*, é extremamente complexo de ser resolvido computacionalmente. O mesmo ocorre quando se tenta obter *k* a partir de *R* e *P*, pois $R = kP$. Portanto, a entidade *B* pode considerar a assinatura digital da entidade *A* autêntica quando $V_1 = V_2$, pois não há maneiras de uma entidade estranha *C* assinar a mensagem se passando por *A* sem que *C* conheça *a* e *k*. Como é necessário que a entidade *C* resolva o Problema do Logaritmo Discreto para Curvas Elípticas para encontrar os valores de *a* e *k*, pode-se considerar o algoritmo criptográfico de assinatura digital ElGamal para Curvas Elípticas como sendo seguro, desde que o Problema do Logaritmo Discreto para Curvas Elípticas permaneça insolúvel em tempo de processamento polinomial. A seguir, será apresentado um exemplo numérico a título de ilustração.

Supondo-se que uma entidade emissora *A* deseja enviar uma mensagem *m* = 100 não secreta assinada digitalmente para uma entidade receptora *B*. A entidade *A* escolhe e publica, por exemplo, os seguintes parâmetros:

$E\colon\ y^2 = x^3 + 3x + 45$

$K\colon\ \mathbb{Z}_{8831}$

$P = (4, 11)$

$f(x, y) = x$

A calcula a ordem do ponto *P* como sendo $N = 4427$ e também, secretamente, escolhe um número inteiro $a = 3$, publicando então o ponto $Q = 3P = (413, 1808)$.

Para enviar a mensagem *m* = 100 assinada digitalmente para a entidade *B*, *A* procede da seguinte forma:

1. Escolhe, por exemplo, um inteiro aleatório $k = 8$, tal que MDC (8, 4427) = 1, e calcula $R = 8P = (5415, 6321)$.
2. Em seguida, *A* calcula:

   $s \equiv 8^{-1}(100 - 3 \times 5415) \pmod{4427} \quad \Rightarrow$

   $s \equiv 4069 \pmod{4427}$

3. *A* então envia (100, $(5415, 6321)$, 4069) como a mensagem assinada para a entidade *B*.

Para verificar a autenticidade da assinatura de *A*, a entidade *B* procede da seguinte maneira:

1. *B* calcula $V_1 = 5415(413, 1808) + 4069(5415, 6321) = (1296, 8024)$
2. Em seguida, *B* calcula $V_2 = 100(4, 11) = (1296, 8024)$

Como $V_1 = V_2 = (1296, 8024)$, *B* então concluiu que a assinatura de *A* é autêntica.

3.6 Aspectos Complementares dos Algoritmos de ECC

Quando se analisam os algoritmos de ECC, surge, com bastante naturalidade, o seguinte questionamento: por que utilizar algoritmos de ECC? Existem várias vantagens que justificam a sua utilização, quando comparado ao modelo RSA, por exemplo. Uma grande vantagem da utilização de algoritmos criptográficos baseados em Curvas Elípticas é a sua enorme flexibilidade. Quando se utiliza um protocolo baseado em ECC, pode-se escolher qual o corpo finito sobre o qual a curva será definida. Também, pode-se escolher qual será o grupo abeliano finito utilizado para a formulação do problema do logaritmo discreto, pois se tem a liberdade para escolher qual será a Curva Elíptica utilizada no processo. Claro que há uma série de restrições a serem respeitadas, para se garantir a segurança do algoritmo (várias dessas restrições já foram abordadas nas seções anteriores), porém ainda assim o usuário goza de uma enorme autonomia para a definição dos parâmetros do seu sistema criptográfico. Dessa forma, é possível quantificar qual o tamanho dos parâmetros necessário para se obter o nível de segurança desejado. Uma outra enorme vantagem da utilização dos sistemas de ECC é o tamanho relativamente pequeno das chaves utilizadas para se obter níveis de segurança semelhantes aos obtidos utilizando-se chaves consideravelmente maiores, como, por exemplo, as chaves da ordem de 1024 bits utilizadas no algoritmo RSA. Dessa forma, os algoritmos de ECC necessitam de uma quantidade menor de memória para serem implementados com os mesmos níveis de segurança de outros algoritmos. Para a utilização de criptografia em sistemas embarcados, ou mesmo a sua utilização em *smart cards*, por exemplo, essa é uma vantagem poderosíssima, haja vista as limitações existentes nesses dois ambientes.

Existem vários métodos amplamente conhecidos atualmente para o ataque do Problema do Logaritmo Discreto para Curvas Elípticas, porém nenhum deles é eficiente o suficiente para apresentar riscos consideráveis ao processo criptográfico, desde que sejam respeitadas algumas restrições de escolha dos parâmetros do protocolo utilizado. Como exemplos de métodos de ataque ao problema do Logaritmo Discreto, podem-se citar o método da força bruta (que consiste em se realizar tentativas de todos os possíveis valores de k, algo bastante ineficiente quando se tem k suficientemente grande), o método de Pohlig-Hellman, o método denominado *Baby Step, Giant Step*, os métodos de Pollard ρ e λ e vários outros métodos. Devido às limitações de escopo deste Trabalho, nenhum desses métodos foi abordado de maneira expositiva, apenas foram

feitas citações aos mesmos, quando tais foram pertinentes. Para uma abordagem mais profunda desses métodos, podem ser consultadas as referências (Washington, 2008), (Menezes, 1993) e (Enge, 1999).

4 Análise Comparativa e Conclusões

Conforme estabelecido na seção 3.6, um dos principais motivos para a utilização criptográfica de Curvas Elípticas é o tamanho relativamente pequeno das suas chaves, quando comparado a outros algoritmos criptográficos assimétricos, como, por exemplo, o modelo RSA. Para se garantir um nível de segurança aproximadamente equivalente entre estes dois sistemas criptográficos, observa-se que há uma clara vantagem quando se utilizam os algoritmos de ECC, em detrimento dos algoritmos baseados no modelo RSA. Por exemplo, de acordo com (Washington, 2008), quando se utiliza o algoritmo criptográfico RSA com uma chave de 4096 bits, obtém-se aproximadamente o mesmo nível de segurança obtido quando se utiliza um algoritmo de ECC com uma chave de 313 bits. A partir desta constatação, torna-se bastante clara a vantagem observada na utilização de algoritmos de ECC em *chips* de tamanho reduzido, em *smart cards* ou mesmo em sistemas embarcados. Também, devido ao reduzido tamanho das chaves, observa-se uma menor necessidade de poder de processamento das máquinas utilizadas na troca de mensagens, bem como uma economia de tempo e energia. A **Tabela 1**, retirada de (Aguiar, 2008), apresenta uma comparação entre os tamanhos de chaves necessários para se garantir aproximadamente o mesmo nível de segurança quando se utilizam os algoritmos RSA e de ECC.

Tabela 1 - Comparação entre Chaves de RSA e ECC

Tamanho da Chave para RSA (bits)	**Tamanho da Chave para ECC (bits)**
512	106
1024	160
2048	210
4096	313

Diante da constatação da vantagem evidente na utilização de algoritmos de ECC em comparação com o modelo RSA, no quesito tamanho das chaves, torna-se necessária uma observação acerca da utilização atual dos dois modelos. Mesmo que o modelo de ECC apresente uma melhor eficiência, do ponto de vista das chaves, que o modelo RSA, este ainda é mais amplamente utilizado que aquele. Isso ocorre devido ao caráter relativamente recente dos estudos envolvendo os modelos de ECC. Já o modelo RSA, além de possuir propriedades e metodologia de funcionamento relativamente simples se comparado aos modelos de ECC, começou a ser amplamente estudado e aplicado como padrão criptográfico cerca de 10 anos antes do surgimento dos modelos de ECC. Porém, nos últimos anos, tem-se observado um crescimento bastante acentuado da utilização dos modelos de ECC, principalmente com a sua inclusão em alguns dos padrões criptográficos estabelecidos pelo NIST (*National Institute of Standards and Technology*), instituto norte americano bastante respeitado mundialmente por sua atuação no estabelecimento de padrões criptográficos para comunicação segura. Para mais informações sobre as publicações do NIST, podem ser consultadas as referências (National Institute of Standards and Technology, 1999), (National Security Agency - United States of America, 2009), (National Institute of Standards and Technology, 2006) e (National Institute of Standards and Technology, 2009).

Por fim, vale salientar que a utilização de modelos criptográficos assimétricos, sejam baseados no algoritmo RSA, sejam baseados em ECC, não substitui a utilização de algoritmos criptográficos simétricos. A utilização de algoritmos assimétricos para a troca corriqueira de mensagens criptografadas é absolutamente impraticável, haja vista as necessidades computacionais e de tempo necessárias à execução dos protocolos assimétricos. Dessa forma, a utilização dos algoritmos simétricos, cuja implementação computacional é significativamente mais “leve”, não deve ser negligenciada, mas sim utilizada em conjunto com a utilização dos algoritmos assimétricos. Estes, via de regra, costumam ser utilizados para a distribuição das chaves dos algoritmos simétricos, assim como em processos de assinatura digital, entre outras aplicações. Como a segurança do processo criptográfico simétrico está baseada no caráter secreto da chave comum entre emissor e receptor, torna-se absolutamente necessário que haja um veículo seguro para o estabelecimento dessa chave. Nesse ponto, os algoritmos assimétricos podem ser amplamente aproveitados, permitindo-se assim que se estabeleça uma chave secreta comum entre emissor e receptor de maneira periódica e

segura, sem que haja uma necessidade contínua de altas capacidades de processamento, demandadas pelos modelos assimétricos. A **Tabela 2**, retirada de (National Security Agency - United States of America, 2009), apresenta uma lista com tamanhos de chaves recomendadas pelo NIST para criptografia simétrica (por exemplo, com o algoritmo AES) e os respectivos tamanhos de chaves de criptografia assimétrica necessárias para se garantir um nível aceitável de segurança, quando se utilizam os dois processos concomitantemente (distribuição de chaves por meio de algoritmos assimétricos e criptografia e transmissão de dados por meio de criptografia simétrica).

Tabela 2 - Tamanhos de Chaves Recomendadas pelo NIST

Chave Simétrica (bits)	Chave Assimétrica RSA (bits)	Chave Assimétrica ECC (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Para mais detalhes sobre algoritmos criptográficos simétricos, podem ser consultadas as referências (Stinson, 2002), (Trappe, et al., 2002) e (Póvoa, et al., 2008).

Finalmente, como conclusão maior deste Trabalho de Graduação, fica evidente a enorme importância da utilização criptográfica de algoritmos fortemente fundamentados em propriedades matemáticas, de forma que se possam garantir certos níveis de segurança aos processos de troca de mensagens secretas. Fica evidente a necessidade de um forte programa de pesquisas matemáticas e computacionais nessa área, pois, diante dos crescentes avanços da tecnologia, juntamente com a possibilidade de colapso dos algoritmos assimétricos utilizados na atualidade com o surgimento de um possível computador quântico, é absolutamente necessário que, para que um país possa utilizar protocolos criptográficos de maneira segura e independente de outros países para a troca de mensagens secretas, nele existam pesquisadores dedicados à produção de conhecimento nacional e inovador na área criptográfica. Esse ainda é um grande desafio para o Brasil, que, infelizmente, ainda não conta com uma

estrutura fortemente arraigada para a pesquisa matemática voltada para a área criptográfica, esse campo tão amplo e ao mesmo tempo tão fascinante daquela que um dia já foi chamada de “Rainha das Ciências”.

Referências

Agrawal, Manindra, Kayal, Neeraj and Saxena, Nitin. 2004. PRIMES is in P. *Annals of Mathematics.* 2004, Vol. 160.

Aguiar, Eduardo Vieira de Oliveira. 2008. Estudo comparativo dos emparelhamentos de Tate e Ate para aplicação em criptografia de curvas elípticas. *Trabalho de Graduação do Instituto Tecnológico de Aeronáutica.* São José dos Campos : s.n., 2008.

Alencar, Edgard de. 1992. *Teoria Elementar dos Números.* São Paulo : NOBEL, 1992. 85-213-0341-6.

Coutinho, Severino C. 2000. *Números Inteiros e Criptografia RSA.* Rio de Janeiro : IMPA/SBM, 2000. 85-244-0124-9.

Enge, Andreas. 1999. *Elliptic Curves and their Applications to Cryptography An Introduction.* Massachusetts : Kluwer Academic Publishers, 1999. 0-7923-8589-6.

Garcia, Arnaldo e Lequain, Yves. 2002. *Elementos de Álgebra.* Rio de Janeiro : IMPA, 2002. 85-244-0190-7.

Koblitz, Neal. 1993. *Introduction to Elliptic Curves and Modular Forms.* Nova Yorque : Springer-Verlag, 1993. 3-540-97966-2.

Lang, Serge. 1972. *Estruturas Algébricas.* Rio de Janeiro : AO LIVRO TÉCNICO S.A., 1972.

Lucchesi, Cláudio Leonardo. 1986. *Introdução à Criptografia Computacional.* Campinas : EDITORA DA UNICAMP, 1986.

Menezes, Alfred J. 1993. *Elliptic Curve Public Key Cryptosystems.* Boston : KLUWER ACADEMIC PUBLISHERS, 1993. 0-7923-9368-6.

Nachbin, Leopoldo. 1974. *Introdução à Álgebra.* Rio de Janeiro : McGRAW-HILL DO BRASIL, 1974.

National Institute of Standards and Technology. [Online]

—. 2009. Digital Signature Standard (DSS). *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - FIPS PUB 186-3.* [Online] Junho 2009. [Cited: Novembro 6, 2010.] http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

—. 2006. Minimum Security Requirements for Federal Information and Information Systems. *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - FIPS PUB 200.* [Online] Março 2006. [Cited: Novembro 6, 2010.] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

—. 1999. Recommended Elliptic Curves for Federal Government Use. *Computer Security Resource Center.* [Online] Julho 1999. [Cited: Novembro 6, 2010.] http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf.

National Security Agency - United States of America. 2009. The Case for Elliptic Curve Cryptography. *National Security Agency.* [Online] Janeiro 12, 2009. [Cited: Novembro 6, 2010.] http://www.nsa.gov/business/programs/elliptic_curve.shtml.

Póvoa, Thiago M. E. e Rabello, Tânia N. 2008. Análise de Algoritmos Necessários à Implementação de uma Infra-Estrutura de Chaves Públicas no ITA. *Anais do 14º Encontro de Iniciação Científica e Pós-Graduação do ITA.* 2008.

Shor, Peter. 1997. POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER. *SIAM J. COMPUT.* 1997, Vol. 26, 5.

Silverman, Joseph H. 1992. *The Arithmetic of Elliptic Curves.* Nova Yorque : Springer-Verlag, 1992. 3-540-96203-4.

Stinson, Douglas R. 2002. *CRYPTOGRAPHY Theory and Pratice.* Florida : CHAPMAN & HALL/CRC, 2002.

Tilborg, Henk C. A. van. 2000. *Fundamentals of Cryptology A Professional Reference and Interactive Tutorial.* Boston : KLUWER ACADEMIC PUBLISHERS, 2000. 0-7923-8675-2 .

Trappe, Wade and Washington, Lawrence C. 2002. *Introduction to Cryptography with Coding Theory.* Nova Jersey : Prentice Hall, 2002. 0-13-061814-4.

Washington, Lawrence C. 2008. *Elliptic Curves Numbers Theory and Cryptography.* Florida : Chapman & Hall/CRC, 2008. 978-1-4200-7146-7.

APÊNDICE A

Tópicos Básicos de Teoria dos Números

Princípio da boa ordenação dos Inteiros: Seja A um subconjunto não vazio do conjunto dos números inteiros positivos. Então, A contém um elemento n, tal que $n \leq x$, para todo $x \in A$. Em outras palavras, todo subconjunto não vazio de inteiros positivos admite um mínimo.

Princípio da Indução Matemática: Seja $A(n)$ uma proposição associada a cada inteiro positivo n, com as seguintes propriedades:

-Se $A(k)$ é verdadeira, então $A(k+1)$ também o é;

-$A(1)$ é verdadeira.

Então, necessariamente, $A(n)$ é verdadeira para todo inteiro positivo n.

Divisores de um Número Inteiro: Sejam a e b dois números inteiros, com $b \neq 0$. Diz-se que a é divisor de b, ou, equivalentemente, que b é múltiplo de a, se existe um número inteiro c, tal que $a.c = b$

Número Primo: Um número inteiro q maior que 1 é chamado de número primo se os únicos divisores positivos de q são 1 e ele mesmo. Caso contrário, o número é denominado composto.

Algoritmo da Divisão: Sejam a e b dois números inteiros, com $b > 0$. Então há dois números inteiros únicos q e r, tais que $a = b.q + r$, e $0 \leq r < b$.

Menor Múltiplo Comum: Chama-se MMC (Menor Múltiplo Comum) entre dois números inteiros positivos a e b um terceiro número inteiro positivo c, tal que:

-c é múltiplo de a, c é múltiplo de b, e c é divisor de qualquer múltiplo positivo de a e b simultaneamente.

Maior Divisor Comum: Chama-se MDC (Maior Divisor Comum) entre dois números inteiros positivos a e b um terceiro número inteiro positivo c, tal que:

-a é múltiplo de c, b é múltiplo de c, e c é múltiplo de qualquer divisor positivo de a e b simultaneamente.

Propriedades do MMC e do MDC: O MDC e o MMC de dois inteiros positivos existem e são únicos.

Pode-se também expressar o MDC entre dois números inteiros positivos a e b como a menor combinação linear positiva que se pode expressar com a e b.

Números Primos entre si: Diz-se que dois números inteiros não nulos *a* e *b* são primos entre si se, e somente se, MDC (*a*,*b*) = 1.

Teorema Fundamental da Aritmética: Todo número inteiro maior que 1 pode ser representado como o produto de um ou mais fatores primos, e essa representação é única.

Congruências: Seja *n* um número inteiro positivo fixado. Sejam *a* e *b* números inteiros. Diz-se que *a* é congruente a *b* modulo *n*, e se escreve $a \equiv b \pmod{n}$, se $a - b$ é um múltiplo de *n.*

Algumas propriedades:

1. $a \equiv a \pmod{n}$ (Propriedade Reflexiva)
2. Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$ (Propriedade Simétrica)
3. Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$ (Propriedade Transitiva)
4. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$, e também $a.c \equiv b.d \pmod{n}$.

Classes de Congruência: Para cada número inteiro positivo *n* fixado, chama-se de classe de congruência (ou classe residual) de um outro número inteiro *p* em relação a *n* o conjunto de números inteiros que são congruentes a *p* modulo *n*, e representa-se tal classe de congruência por [*p*] = {$x \in \mathbb{Z}$, tal que $p \equiv x \pmod{n}$ }.

Inteiros Modulo *n*: Define-se como Conjunto de Inteiros modulo *n*, e denota-se por $\mathbb{Z}_n$ o conjunto formado pela união dos conjuntos das classes de congruência em relação a *n*. Em outras palavras, $\mathbb{Z}_n$= { [0], [1], [2], ..., [*n*-1] }.

Pequeno Teorema de Fermat: Seja *p* um número primo, e *a* um número inteiro não divisível por *p*. Então $a^{p-1} \equiv 1 \pmod{p}$.

Teorema de Wilson: Se *p* é um número primo, então $(p-1)! \equiv -1 \pmod{p}$.

Vale também a recíproca: Se $(n-1)! \equiv -1 \pmod{n}$, então *n* é primo.

Pode-se utilizar esse teorema como um teste de primalidade.

Função fi de Euler: Chama-se função fi de Euler a função $\phi(n)$ que fornece a quantidade de inteiros positivos menores ou iguais *n* e que são primos com *n*. Em outras palavras, $\phi(n)$ = quantidade de elementos do conjunto: { $x \in \mathbb{N} \mid 1 \leq x \leq n$ e MDC (*x*,*n*) = 1 }

Teorema de Euler: Sejam *a* e *n* dois inteiros positivos primos entre si. Então:

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

Para p primo, $\phi(p) = p - 1$. Nesse caso, percebe-se que o Pequeno Teorema de Fermat é um caso particular do Teorema de Euler.

Teorema Chinês do Resto: Sejam m_1, m_2, ... , m_r números inteiros primos entre si dois a dois, isto é, tais que MDC $(m_i, m_j) = 1$, $\forall\, i \neq j$. Nestas condições, existe uma única solução x modulo $m = m_1 m_2 \ldots m_r$ para o sistema de congruências lineares:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x \equiv a_r \pmod{m_r}$$

Número de Mersenne: Chama-se número de Mersenne a todo número inteiro positivo da forma:

$$M_n = 2^n - 1, \forall\, n \geq 2$$

Se M_n é um número primo, então M_n é denominado primo de Mersenne.

Número de Fermat: Chama-se número de Fermat a todo número inteiro positivo da forma:

$$F_n = 2^{2^n} + 1, \forall\, n \geq 0$$

Se F_n é um número primo, então F_n é denominado primo de Fermat.

Teorema dos Números Primos: Seja x um número real positivo. Então:

$$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$$

Sendo $\pi(x)$ a função que estabelece o número de primos positivos menores ou iguais a x.

APÊNDICE B

Tópicos Básicos de Álgebra

Grupos: Um conjunto *G*, munido de uma operação

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$

é um grupo, se satisfaz as seguintes condições:

1. A operação é associativa, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall\, a, b, c \in G$
2. Existe um elemento neutro, isto é, $\exists\, e \in G$, tal que $\forall\, a \in G,\ e \cdot a = a$ e $a \cdot e = a$
3. Todo elemento possui um elemento inverso, isto é, $\forall\, a \in G$, $\exists\, b \in G$, tal que $a \cdot b = e$ e $b \cdot a = 0$. Se a operação é comutativa, isto é, $a \cdot b = b \cdot a$, diz-se que o grupo é abeliano ou comutativo.

Frequentemente, deixa-se de indicar a operação do grupo, escrevendo-se apenas *G* para se denotar um grupo $(G,\ \cdot)$.

O elemento neutro *e* é único.

O elemento inverso é único. Seja um elemento $a \in G$, então seu elemento inverso é comumente denotado por a^{-1}.

Seja *G* um grupo, com elemento neutro *e*. Seja um elemento $a \in G$. Define-se $a^0 = e$, $a^t = a \cdot a^{t-1}$ e $a^{-t} = (a^t)^{-1}$, $\forall\, t \in \mathbb{Z}$.

Seja $(G,\ \cdot)$ um grupo. Um subconjunto não-vazio *H* de *G* é um subgrupo de *G* quando, com a operação de *G*, o conjunto *H* é um grupo.

O elemento neutro e_H de *H* é necessariamente igual ao elemento neutro *e* de *G*.

Dado o elemento $h \in H$, o inverso de *h* em *H* é necessariamente igual ao inverso de *h* em *G*.

Seja *G* um grupo, e $g \in G$. Então, o conjunto $\{g^t$, com $t \in \mathbb{Z}\}$, denotado por $\langle g \rangle$, é um subgrupo de *G*. Nesse caso, diz-se que $\langle g \rangle$ é o subgrupo gerado por g.

Seja *G* um grupo. *G* é denominado cíclico se $\exists\, g \in G$, tal que $G = \langle g \rangle$.

Seja *G* um grupo. Define-se ordem de *G*, e denota-se por $|G|$, o número de elementos de *G*. Seja $g \in G$. Define-se ordem de g, e denota-se por $\mathcal{O}(g)$, o número de elementos de $\langle g \rangle$.

Sejam g um elemento do grupo *G* e $\langle g \rangle$ o subgrupo gerado por g. Então, diz-se que a ordem de $\langle g \rangle$ é finita se, e somente se, $\exists\, t \geq 1$, tal que $g^t = e$. Neste caso, denotando-se por n a ordem de g, então $\{t \geq 0;\ g^t = e\} = \{0, n, 2n, \ldots\}$ e $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$.

Seja *G* um grupo de ordem prima. Então, *G* é um grupo cíclico.

Sejam *G* um grupo finito e *H* um subgrupo de *G*. Então, a ordem de *H* divide a ordem de *G*. Esse resultado é conhecido como Teorema de Lagrange.

Anéis: Um anel $(A, +, \cdot)$, comutativo e com unidade, é definido como um conjunto *A* com pelo menos dois elementos, munido de uma operação denotada por + (chamada adição) e de uma operação denotada por $\cdot$ (chamada multiplicação) que satisfazem as seguintes condições:

1. A adição é associativa, isto é, $\forall\, x, y, z \in A, (x + y) + z = x + (y + z)$
2. Existe um elemento neutro com respeito à adição, isto é, $\exists\, 0 \in A$, tal que $\forall\, x \in A,\ 0 + x = x$ e $x + 0 = x$
3. Todo elemento de *A* possui um inverso com respeito à adição, isto é, $\forall\, x \in A, \exists z \in A$, tal que $x + z = 0$ e $z + x = 0$
4. A adição é comutativa, isto é, $\forall\, x, y \in A,\ x + y = y + x$
5. A multiplicação é associativa, isto é, $\forall\, x, y, z \in A,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$
6. Existe um elemento neutro com respeito à multiplicação, isto é, $\exists\, 1 \in A$, tal que $\forall\, x \in A,\ 1 \cdot x = x$ e $x \cdot 1 = x$
7. A multiplicação é comutativa, isto é, $\forall\, x, y \in A,\ x \cdot y = y \cdot x$
8. A adição é distributiva relativamente à multiplicação, isto é, $\forall\, x, y, z \in A,$ $x \cdot (y + z) = x \cdot y + x \cdot z$

Frequentemente, deixa-se de indicar as operações do anel, escrevendo-se apenas *A* para se denotar um anel $(A, +, \cdot)$.

O elemento neutro com respeito à adição é único. Esse elemento neutro é comumente chamado de *zero*, e denotado por 0.

O elemento neutro com respeito à multiplicação é único. Esse elemento neutro é comumente chamado de *um*, e denotado por 1.

O elemento inverso com respeito à adição é único. Seja um elemento $x \in A$, então seu elemento inverso com respeito à adição é comumente denotado por $-x$.

O elemento neutro da adição 0 tem a seguinte propriedade: $0 \cdot x = 0, \forall\, x \in A$.

Corpos: Seja um anel comutativo com unidade $(K, +, \cdot)$. Este anel é denominado corpo se satisfaz a seguinte condição:

1. $\forall\, x \in K \setminus \{0\}, \exists\, y \in K$, tal que $x \cdot y = 1$. Em outras palavras, todo elemento não-nulo de *K* possui inverso com respeito à multiplicação.

Frequentemente, deixa-se de indicar as operações do corpo, escrevendo-se apenas *K* para se denotar um corpo $(K, +, \cdot)$.

O elemento inverso com respeito à multiplicação de um corpo *K* é único. Seja um elemento $x \in K$, então seu elemento inverso com respeito à multiplicação é comumente denotado por x^{-1}.

Seja *K* um corpo. Então $\forall\, x, y \in K,\ x \cdot y = 0 \Leftrightarrow x = 0$ ou $y = 0$.

Diz-se que um corpo *K* é finito se *K* possui um número finito de elementos. Os corpos finitos são também denominados corpos de Galois e são comumente representados por *GF*.

Os elementos não-nulos de um corpo *K*, munidos da operação de multiplicação, formam um grupo abeliano finito. Esse grupo é denominado grupo multiplicativo do corpo *K*, e comumente denotado por K^*.

Seja *K* um corpo. Define-se uma operação que associa um elemento $x \in K$ com um elemento $n \in \mathbb{Z}$, e resulta em um elemento de *K*, denotado por *nx*, tal que:

1. $0x = 0,\ \forall\, x \in K.$
2. $(k+1)x = kx + x, \forall\, x \in K$ e $k \in \mathbb{N}$
3. $(-k)x = -(kx), \forall\, x \in K$ e $k \in \mathbb{N}^*$

O elemento *nx* é denominado múltiplo inteiro de *x*.

Seja K um corpo, com elemento neutro aditivo 0 e elemento neutro multiplicativo 1. Seja um conjunto A_K, definido por $A_K = \{n \in \mathbb{Z}$, tal que $n1 = 0\}$. Caso $A_K = \{0\}$, diz-se que o corpo *K* possui característica 0. Caso contrário, existe um menor inteiro positivo *p* em A_K. Nesse caso, diz-se que *K* possui característica *p*.

Seja *K* um corpo com característica *p*. Então *p* é um número primo.

Seja K um corpo com característica p. Então A_K é formado pelos múltiplos inteiros de *p*.

Seja *K* um corpo finito com característica *p*. Então o número de elementos de *K* é dado por p^m, com $m \in \mathbb{N}^*$.

FOLHA DE REGISTRO DO DOCUMENTO

1. CLASSIFICAÇÃO/TIPO	2. DATA	3. REGISTRO N°	4. N° DE PÁGINAS
TC	16 de novembro de 2010	DCTA/ITA/TC-067/2010	87

5. TÍTULO E SUBTÍTULO:

Estudo dos Algoritmos Criptográficos Assimétricos RSA e de Curvas Elípticas

6. AUTOR(ES):

Thiago Marques Esteves Póvoa

7. INSTITUIÇÃO(ÕES)/ÓRGÃO(S) INTERNO(S)/DIVISÃO(ÕES):

Instituto Tecnológico de Aeronáutica – ITA

8. PALAVRAS-CHAVE SUGERIDAS PELO AUTOR:

Criptografia assimétrica; Chave pública; RSA; Criptografia de curvas elípticas; Assinatura digital

9.PALAVRAS-CHAVE RESULTANTES DE INDEXAÇÃO:

Criptografia de chave pública; Algoritmos; Curvas elípticas; Segurança da informação de computadores; Assinatura digital; Protocolos criptográficos; Matemática aplicada; Comunicação; Matemática

10. APRESENTAÇÃO: **X Nacional** **Internacional**

ITA, São José dos Campos. Curso de Graduação em Engenharia Civil-Aeronáutica. Orientadora: Tânia Nunes Rabello. Publicado em 2010.

11. RESUMO:

Na sociedade moderna, com o advento da internet, há um fluxo intenso de informações dos mais variados tipos. Esse fluxo de comunicação se dá entre um número enorme de entidades diferentes, desde grandes corporações e órgãos governamentais até simples usuários de serviços de e-mail ou *internet banking*. Muitas vezes, as informações que se deseja transmitir são de caráter confidencial, sendo assim necessário que se apliquem algumas técnicas para tornar a mensagem secreta no processo de transmissão. Diante da crescente necessidade de protocolos criptográficos para a encriptação de mensagens dos mais variados tipos e tamanhos, surge em todo o mundo uma enorme corrente de pesquisas matemáticas e computacionais dedicada ao estudo dos algoritmos criptográficos já conhecidos e empenhada no desenvolvimento de novos modelos. Este Trabalho de Graduação pautou-se no estudo de dois algoritmos amplamente utilizados na atualidade em processos de criptografia assimétrica (também denominada criptografia de chave pública): O modelo RSA, e o modelo criptográfico baseado nas propriedades algébricas de Curvas Elípticas sobre corpos finitos. Ao longo do Trabalho, procurou-se tratar cada algoritmo de maneira específica, abordando sua metodologia de funcionamento, propriedades matemáticas relacionadas, tipos de aplicações, bem como sua presença nos protocolos criptográficos utilizados na atualidade. Por fim, procurou-se estabelecer um paralelo entre ambos, apontando assim algumas vantagens dos modelos criptográficos de Curvas Elípticas frente ao modelo RSA, tais como a possibilidade de uma escolha mais diversificada dos parâmetros necessários ao funcionamento do algoritmo (corpos finitos, Curvas Elípticas e pontos pertencentes à Curva) e também o caráter bastante reduzido do tamanho das chaves necessárias para que sejam mantidos níveis de segurança semelhantes aos alcançados quando se utiliza o modelo RSA. Vale ressaltar que este Trabalho preocupou-se com uma abordagem matemática dos algoritmos, de forma que seus aspectos computacionais não foram tratados de maneira específica.

12. GRAU DE SIGILO:

(X) OSTENSIVO **( ) RESERVADO** **( ) CONFIDENCIAL** **( ) SECRETO**