Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologias
Departamento de Informática
Curso de Ciência da Computação

Jander Rocha Alves

AVALIAÇÃO DE DESEMPENHO DOS CRIPTOSSISTEMAS DE CURVAS ELÍPTICAS DE MENEZES-VANSTONE E DO ANÁLOGO DE ELGAMAL NO CONTEXTO DE ENCRIPTAÇÃO DE IMAGENS

São Luís

2017

JANDER ROCHA ALVES

Avaliação de desempenho dos Criptossistemas de Curvas Elípticas de Menezes-Vanstone e do Análogo de Elgamal no contexto de encriptação de imagens.

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof Msc. Antônio de Abreu Batista Júnior

São Luís

2017

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

Alves, Jander Rocha.
Avaliação de desempenho dos Criptossistemas de Curvas Elípticas de Menezes-Vanstone e do Análogo de Elgamal no contexto de encriptação de imagens / Jander Rocha Alves. - 2017.
49 f.

Orientador(a): Antônio de Abreu Batista Júnior.
Monografia (Graduação) - Curso de Ciência da Computação, Universidade Federal do Maranhão, São Luís, 2017.

1. Criptografia. 2. ECC. 3. Elgamal. 4. Menezes-Vanstone. I. Júnior, Antônio de Abreu Batista. II. Título.

Jander Rocha Alves

Avaliação de desempenho dos Criptossistemas de Curvas Elípticas de Menezes-Vanstone e do Análogo de Elgamal no contexto de encriptação de imagens

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação

Orientador: Prof. Me. Antônio de Abreu Batista Júnior

Aprovada em 26/01/17

BANCA EXAMINADORA

Antonio de Abreu Batista Junior

Prof. Me. Antônio de Abreu Batista Junior
Mestre em Ciência da Computação
Universidade Federal do Maranhão

Prof. Dr. Luciano Reis Coutinho
Doutor em Ciências
Universidade Federal do Maranhão

Prof. Dr. Mario Antonio Meireles Teixeira
Doutor em Ciências da Computação
Univerisade Federal do Maranhão

AGRADECIMENTOS

Agradeço à minha mãe, que me criou mediante muita dificuldade sempre dando seu melhor por mim e me ensinou o valor da educação.

À minha namorada Samiris Costa por estar sempre ali me apoiando nos momentos de dificuldade, sendo meu refúgio nos momentos mais difíceis bem como pela revisão ortográfica.

Aos amigos de curso, Wendell, Weslley, Ginaldo, Mateus, Willian, Pedro Paulo, Guilherme, Bruno, Flávio, Ivan, Thalles Alencar, Thales Levi ,que compartilharam momentos de alegria e tristeza, dificuldades e superações durante estes quase 6 anos de UFMA.

Aos amigos Samuel Silva e Adriano Sousa por terem me ajudado com suas experiências e provendo momentos de descontração muito necessários.

Ao amigo Thiago Carmo, que mesmo distante sempre me apoiou com bons conselhos, boas recomendações musicais ou simplesmente um bom papo descontraído que sempre ajudava a acalmar a mente.

Ao professor Antonio de Abreu, sem o qual este trabalho teria sequer sido idealizado, por sua paciência com minhas perguntas constantes e pela orientação ativa e constante.

Ao professor Mário Meireles por ter aceitado compor a banca bem como ter me orientado nos primeiros passos em relação à avaliação de desempenho.

Ao professor Luciano Reis por ter aceitado compor a banca bem como ter sido indiretamente uma referência em relação aos desafios da criptografia.

A quaisquer outras pessoas que tenham contribuído para a produção deste trabalho direta ou indiretamente.

RESUMO

No mundo conectado da atualidade, a informação tem um valor imensurável para todos os componentes da sociedade, desde o governo até o indivíduo comum. Imagens são capazes de transmitir muita informação, desde informações irrelevantes como uma paisagem a informações sigilosas como contratos ou patentes. Diariamente, milhares delas são transferidas por meio da rede e muitas são confidenciais. Quando se deseja que estas imagens sejam transferidas confidencialmente, a criptografia é a técnica utilizada para garantir este e outros requisitos. Neste trabalho nós comparamos os métodos de criptografia de curvas elípticas de Menezes-Vanstone e ElGamal, no contexto de encriptação de imagens, tendo em vista que esses estão dentre os métodos mais abordados pela literatura, a fim de determinar qual dos dois tem o melhor desempenho com o menor custo.

Palavras-chave: ECC. criptografia. ElGamal. Menezes-Vanstone.

ABSTRACT

In the modern connected world, information has an immensurable value for every part of the society, from the government to the common person. Images can transmit a lot of information, from irrevelant ones such as a landscape to top secret ones like contracts or patents. Everyday, thousands of them are transfered through the internet and a lot contain sensible information. When secrecy is desired, cryptography is used to assure this and some other requirements. In this study we compare the Elliptic curve based methods, Menezes-Vanstone and ElGamal in the context of images aiming to define which has best performance with lesser cost.

Keywords: ECC. Cryptography. Elgamal. Menezes-Vanstone.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptosystem
ECIES	Elliptic Curve Integrated Encryption Scheme
GIF	Graphics Interchange Format
JPEG	Joint Photographic Experts Group
NIST	National Institute of Standards and Technology
PNG	Portable Network Graphics
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
SECG	Standards for Efficient Cryptography Group

LISTA DE SÍMBOLOS

Γ	Letra grega Gama
Λ	Lambda
$\in$	Pertence
$\equiv$	Equivalência

SUMÁRIO

1 INTRODUÇÃO

No mundo atual, as conexões via Internet mudaram a maneira do mundo tratar certos procedimentos. Muitos se tornaram mais ágeis, e até mesmo coisas que não eram possíveis antes se tornaram rotineiras graças à capacidade de transcender a barreira da distância.

Devido a essa situação, mais e mais arquivos são transferidos por meio de conexões em ambientes públicos. Garantir a privacidade e segurança destes arquivos é uma tarefa complicada. Boa parte destes arquivos são imagens, como por exemplo: contratos, acordos entre duas partes, plantas desenvolvidas por um engenheiro, projetos de dispositivos eletrônicos, imagens biométricas, dentre outros.

Neste contexto, a criptografia assume um papel importante para garantir a integridade e a confidencialidade destes arquivos. No entanto, na maioria das vezes, deseja-se que estes métodos sejam também eficientes computacionalmente. Um número de trabalhos tem sido proposto a fim de propor novos métodos de criptografia para imagens (SOLEYMANI et al., 2013) (SOLEYMANI; NORDIN; ALI, 2013) (BELAZI; EL-LATIF; BELGHITH, 2016). Alguns trabalhos tem investigado o emprego de algoritmos conhecidos como o RSARSARivest-Shamir-Adleman, AESAESAdvanced Encryption Standard (ZEGHID et al., 2007) (SILVA et al.,). No entanto, este tópico ainda tem espaço para muitas pesquisas, não só de métodos como de comparações entre estes para diferentes situações.

Neste trabalho comparam-se técnicas de criptografia assimétrica baseada em curvas elípticas para assegurar a transmissão segura de imagens. Para isso foi delimitado como objetivo geral do trabalho comparar os métodos de criptografia de curvas elípticas de Menezes-Vanstone (MENEZES; VANSTONE, 1993) e o análogo do ElGamal (GAMAL, 1985) com curvas elípticas, no contexto de encriptação de imagens, a fim de determinar qual dos dois métodos tem o mais alto desempenho com o menor custo. Para chegar a tal conclusão foram determinados alguns passos intermediários ou objetivos específicos dentro do trabalho, são eles:

- Realizar um estudo teórico dos dois os métodos envolvidos;
- Determinar fatores a serem analisados que podem influenciar na performance dos algoritmos;
- Determinar quais fatores mais impactam na performance dos algoritmos analisados.

O restante deste trabalho está organizado como segue: no capítulo 2 é dada uma revisão teórica sobre criptografia baseada em curvas elípticas e sobre representações de imagens. No capítulo 3 apresentamos o método utilizado para avaliação de desempenho dos métodos escolhidos. Nesse capítulo também apresentamos um estudo de caso proposto e como os processos de encriptação e decriptação foram feitos. No capítulo 4 apresentamos os resultados obtidos e uma discussão acerca destes. Por fim, no capítulo 5, apresentamos nossas conclusões e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Definições matemáticas

Para que possamos entender a criptografia, é necessário primeiramente definir alguns conceitos matemáticos que serão mencionados posteriormente. O primeiro deles é o conceito de corpo, um corpo pode ser entendido como um grupo onde todo elemento diferente de zero possui um elemento inverso referente à multiplicação.

O segundo conceito a ser definido aqui é o de grupo, um grupo pode ser entendido como o conjunto de todos os elementos associados a uma operação entre dois números que gere um terceiro elemento, desde cumpram algumas condições. Estas são: possuir um elemento neutro, um elemento inverso e apresentar associatividade. O elemento neutro é aquele que quando aplicado à operação não altera o valor do outro elemento envolvido. Já o elemento inverso é aquele que quando aplicado a um elemento resulta no elemento neutro. E a associatividade define que a ordem das operações executadas não afete o resultado final.

O último conceito importante a ser mencionado é o de ordem, que se refere à quantidade de elementos presentes em um grupo.

2.2 Definição de Criptografia

Criptografia pode ser entendida como um conjunto de técnicas e métodos que, por meio de uma chave ou conjunto de chaves, tem por fim de mascarar uma informação, denominada texto aberto ou textitcleartext convertendo esta em uma informação incompreensível denominada texto cifrado ou /textitcyphertext de maneira que somente quem saiba o segredo por trás do método consiga reverter o texto cifrado em texto claro.

O processo de conversão de texto claro para cifrado é chamado de encriptação ou cifragem. Já o processo reverso é chamado de decriptação ou decifragem. À medida que novos métodos são desenvolvidos, estes são divulgados para a comunidade e

validados com o passar do tempo, o que implica na importância da chave no quesito segurança. Logo o tamanho da chave é importante pois quando maior a chave mais seguro é o processo (TANENBAUM, 2003).

Os algoritmos de criptografia são classificados em dois grupos maiores de acordo com o tipo de chave que utilizam, os algoritmos de chave simétrica e os de chave pública, que serão explicados a seguir.

2.3 Criptografia simétrica

Os sistemas de chave simétrica caracterizam-se por utilizar uma única chave tanto para o processo de codificação quando de decodificação, por isso são chamados também de sistemas de chave privada.

(SMART, 2004) apresenta a seguinte relação para o processo de encriptação:

$$c = E_k(m) \tag{2.1}$$

onde:

c = texto cifrado

E = algoritmo de encriptação

m = texto claro

k = chave

Para o processo reverso o mesmo autor define:

$$m = D_k(c) \tag{2.2}$$

onde:

c = texto cifrado

D = algoritmo de decriptação

m = texto claro

k = chave

Esta definição ajuda a esclarecer um ponto importante da criptografia, geralmente E, De m são de conhecimento público, o que infere que a segurança do processo de criptografia está, quase que totalmente, no segredo da chave k.

Estes algoritmos costumam ser bem mais rápidos que os algoritmos assimétricos, porém trazem consigo problemas de gerenciamento de chave, visto que à medida que todas as partes envolvidas no processo devem saber a chave esta deve ser mantida em segredo de todos os outros.

Os algoritmos de chave simétrica costumam ser divididos em dois subgrupos: Os de fluxo ou *Stream Cyphers* e os de bloco ou *Block Cyphers*. Os de fluxo criptografam um símbolo (ou byte) por vez, já os de bloco operam em cima de um bloco de tamanho fixo e pré-definido de símbolos ou bytes por vez. Nos algoritmos de fluxo uma chave cifra um único símbolo, já nos de bloco cada chave cifra um bloco de símbolos (JUST, 2012). Exemplos de algoritmos simétricos amplamente utilizados são o DESDESData Encryption Standard e o AES.

2.4 Criptografia assimétrica

Também conhecida como criptografia de chave pública, nestes criptossistemas são utilizadas duas chaves, uma publica outra privada. A chave pública pode ser divulgada juntamente com o destino do usuário. Qualquer parte que desejar enviar uma mensagem a este usuário deve codificar a mesma utilizando a chave pública do usuário e enviá-la ao destinatário. A ideia é que somente o usuário com a chave privada correspondente seja capaz de decodificar a mensagem.

$$c = E_{k1}(m) \tag{2.3}$$

$$m = D_{k1}(c) \tag{2.4}$$

onde:

c = texto cifrado

E = algoritmo de encriptação

D = algoritmo de decriptação

m = texto claro

k1 = chave pública

k2 = chave privada

Estes sistemas funcionam devido às chaves estarem relacionadas matematicamente, de uma maneira que não seja possível obter informações da chave privada partindo da pública. No entanto, o texto codificado com a chave pública só pode ser decodificado com a chave privada relacionada. A ideia foi primeiro apresentada em (DIFFIE W.; HELLMAN, 2013). Mas o primeiro criptossistema implementando a ideia só foi apresentado um ano depois, o RSA.

Existem poucas ideias baseadas em algorítimos de chave pública devido a estas necessitarem de uma operação matemática que seja facilmente computável em um sentido e difícil no outro sentido (SMART, 2004). A seguir introduzimos criptografia de curvas elípticas

2.5 Criptografia de Curvas Elípticas

Trata-se de uma implementação de criptografia de chave pública utilizando um grupo de pontos de uma curva elíptica. Os ECCs (*Elliptic Curve Criptosystems*)ECCElliptic Curve Cryptosytem podem garantir o mesmo nível de segurança que outros algoritmos assimétricos como RSA utilizando uma chave menor o que normalmente implica em menor utilização de certos recursos como a memória e tempos de execuções mais rápidos.

2.5.1 Definição

Uma curva elíptica E sobre um corpo primo F_p é definida por:

$$E : y^2 \equiv x^3 + ax + b \ (mod\ p) \tag{2.5}$$

onde $a, b \in F_p$, $p \neq 2, 3$ e satisfaz a condição $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$. O grupo da curva elíptica $E(F_p)$ é o conjunto de todos os pontos (x, y) que satisfazem a equação 2.5 mais um ponto especial O no infinito (HANKERSON; MENEZES; VANSTONE, 2003).

2.5.2 Operações Aritméticas em Curvas

Adição em pontos da curva

Suponha que $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, onde $P \neq Q$ e ambos os pontos pertencem a uma curva E definida em 2.5. A soma $P + Q$ resulta em um terceiro ponto $R = (x_3, y_3$ que também pertence a E. A operação para realizar a soma dos dois pontos depende de algumas condições apresentadas a seguir:

Caso $P \neq Q \neq O$ e $x_1 \neq x_2$ então a soma de P e Q é definida por

$$P + Q = R \tag{2.6}$$

onde:

$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)} \tag{2.7}$$

$$x_3 \equiv (\lambda^2 - x_1 - x_2)\ (mod\ p) \tag{2.8}$$

$$y_3 \equiv (\lambda(x_1 - x_3) - y_1)\ (mod\ p) \tag{2.9}$$

Caso $x_1 = x_2$, mas $y_1 \neq y_2$ então $P + Q = O$.

Duplicação de pontos da curva

Sendo $P = (x_1, y_1)$ um ponto da curva E, duplicar o ponto é somar ele a ele mesmo. Ou seja:

$$P + P = 2P = R = (x3, y3) \tag{2.10}$$

onde:

$$\lambda = \frac{3{x_1}^2 + a}{2y_1} \tag{2.11}$$

$$x_3 \equiv (\lambda^2 - 2x_1)\ (mod\ p) \tag{2.12}$$

$$y_3 \equiv (\lambda(x_1 - x_3) - y1)\ (mod\ p) \tag{2.13}$$

Multiplicação Escalar

Sendo k um inteiro e $P = (x_1, y_1)$ um ponto da curva E, a multiplicação por escalar é definida por:

$$kP = P + P + P....P \tag{2.14}$$

isto é, somar um ponto a ele mesmo k vezes. Por exemplo, a operação $9P$ é computada como:

$$9P = 2(2(2P)) + P \tag{2.15}$$

Neste trabalho, utilizamos o método binário descrito na Tabela 1 para computar a Multiplicação Escalar.

Multiplicação Escalar: Método Binário
Entrada: representação binária de k e o ponto P **Saída:** $Q = k \cdot P$ $Q = P$ for $i = n - 1$ to 0 do $Q = 2 \cdot Q$ (Duplicação) if $k_i = 1$ então $Q = Q + P$ (Adição) Return Q

Tabela 1 – Algoritmo de Multiplicação Escalar.

Inversa de um ponto

Sendo $P = (x, y)$ a inversa de P é $Q = -P = (x, -y)$ onde $P + Q = O$

2.6 Criptossistemas de Curvas Elípticas

2.6.1 Análogo ElGamal

O criptossistema consiste de um algoritmo de geração de chave baseado no análogo de curva elíptica de Diffie-Hellman, e um algoritmo de encriptação e decriptação baseado no análogo de curva elíptica de ElGamal.

Parâmetros Públicos

Os parâmetros conhecidos do público a priori são:

1. A curva elíptica E
2. Um ponto da curva P, que gera um subgrupo de E
3. A ordem n do subgrupo de E

P é um gerador do subgrupo cíclico de E:

$$\langle P \rangle = \{\infty, P, 2P, 3P, ..., (n-1)P\}$$

Geração do Par de chaves

Como entrada são passados os parâmetros públicos definidos anteriormente. O procedimento executa os passos seguintes:

1. Escolhe $d \in_{u.a.r.} \{1, ..., n-1\}$
2. Computa $Q = dP$
3. O par de saída (Q, d). chave pública: Q, chave privada: d.

Observa-se que computar a chave privada d partindo da chave pública Q requer resolver o problema do logaritmo discreto, o qual será explicado mais a frente.

Encriptação

Além dos parâmetros públicos, passam-se a chave pública Q. Queremos encriptar uma mensagem M, que é codificada como um ponto da curva elíptica. Foi elaborado como fazer a codificação a seguir.

1. Escolha $k \in_{u.a.r.} \{1, ..., n-1\}$
2. Compute $C_1 = kP$
3. Compute $C_2 = M + kQ$
4. texto cifrado: (C_1, C_2)

Uma observação é que uma vez que k é escolhido randomicamente, $C_2 = M + kQ$ na verdade também parece ser randômico.

Codificação da Mensagem

Neste trabalho utilizamos o método de Koblitz para codificar números inteiros em pontos da curva e vice-versa. A seguir o método é descrito.

Seja K um inteiro grande tal que uma taxa de falha de $\frac{1}{2^k}$ possa ocorrer quando tentando codificar uma mensagem em um ponto. Para $j \in \{0, 1, 2, ..., k-1\}$ verifique se para $x = mK + j$, $x^3 + ax + b \ (mod\ p)$ é um quadrado de um inteiro y, ou seja, $y^2 \equiv x^3 + ax + b \ (mod\ p)$. Se um tal j for encontrado, a codificação é feita, Se não o algoritmo falha com probabilidade de $\frac{1}{2^k}$.

A fim de recuperar a mensagem m a partir do ponto (x, y), computa-se:$\lfloor \frac{x}{k} \rfloor$.

Decriptação

É passado o par de texto cifrado (C_1, C_2), e a chave privada d. O objetivo é reconstruir o ponto que representa a mensagem M:

1. $C_2 - dC_1 = M + kQ - \underbrace{dkP}_{=k(dP)=kQ} = M$

2.6.2 O método Menezes-Vanstone

O método Menezes-Vanstone é um criptossistema que diferentemente do método ElGamal, não possui análogo para o problema do logaritmo discreto. Logo não é necessário mapear o texto em claro para pontos da curva, mas somente mascará-lo, substituindo cada caractere do texto por um par ordenado que não precisa necessariamente fazer parte da curva escolhida.

Quando o remetente A quer enviar uma mensagem $M = (m1, m2)$, para B, eles precisam escolher uma curva *E(Fp)* e um ponto base *G*. Cada parte escolhe sua chave privada do intervalo $[1, n]$. Assumindo *d* como a chave privada do usuário A e *e* como a chave privada de B. Cada parte calcula sua chave pública multiplicando a chave privada pelo ponto base *G*. Logo temos $Pa = (d.G)$ e $Pb = (e.G)$. O usuário A então calcula a chave secreta *K* multiplicando sua chave privada *d* pela chave pública de B *Pb* e B pode calcular a mesma chave usando sua chave privada e a chave pública de A. O que resulta em:

$$K = e.Pa = d.Pb = d.e.G = (k_1, k_2) \tag{2.16}$$

então A codifica a mensagem calculando:

$$\begin{aligned} c_1 &= m_1 * k_1 \ (mod\ p) \\ c_2 &= m_2 * k_2 \ (mod\ p) \end{aligned} \tag{13}$$

Para B decodificar a mensagem de A ele calcula:

$$m_1 = c_1 * k_1^{-1} \ (mod\ p)$$
$$m_2 = c_2 * k_2^{-1} \ (mod\ p) \tag{14}$$

2.7 Curvas Padrão

Conforme apresentado anteriormente, em criptografias baseadas em ECC deve haver um acordo nos parâmetros da curva utilizada. Caso esses parâmetros não tenham sido previamente validados é necessário validá-los antes que possam ser usados. Como essa é uma operação demorada e custosa, não é aplicada na prática.

Vários grupos publicaram parâmetros de curvas padrão para os tamanhos de campo mais utilizados na prática. Estes já validados e testados contra os ataques existentes. Estes parâmetros são chamados de Curvas padrão ou curvas nomeadas. Dentre estes grupos temos o NIST (*National Institue of Standards and Technology*), o SECG (*Standards for Efficient Cryptography Group*) e o ECC Brainpool. Muitos dos parâmetros presentes na lista de um orgão também estão presentes na lista de outro, não sendo exclusivos de um ou outro.

Neste trabalho usaremos 4 curvas sugeridas: a secp160r1, secp160k1, secp256r1, secp256k1. Onde os números apresentados nas curvas definem o tamanho da chave em bits e a letra define se os parametros foram definidos aleatoriamente (curvas r) ou não (curvas k).

2.8 Segurança dos Criptossistemas Utilizados

Ambos os criptossistemas estudados neste trabalho são baseados no Problema do Logarítmo Discreto em Curvas Elípticas. Para quebrar estes criptossistemas é preciso resolver o problema do logaritmo Hoje, os melhores métodos conhecidos tem complexidade exponencial.

A seguir é dada uma definição do problema do logarítmo discreto um curvas elípticas atribuída a Koblitz.

2.8.1 Definição

Dada uma Curva E definida sobre $GF(q)$ e dois pontos $P, Q \in E$, encontrar um inteiro x tal que $Q = xP$ se tal x existir. Como um exemplo considere a Curva Elíptica E dada pela equação $Y^2 = X^3 + X - 1 \; mod \; 7$ e o ponto gerador $P(1, 6)$. Na tabela 2 é mostrado todos os pontos da Curva E gerados por P.

Tabela 2 – Todos os pontos da Curva E gerados por P por meio da multiplicação por um escalar x

Pontos	$x * P$
(1,6)	P
(2,3)	2P
(6,2)	3P
(4,2)	4P
(3,6)	5P
(3,1)	6P
(4,5)	7P
(6,5)	8P
(2,4)	9P
(1,1)	10P
infinity	11P

Dados os pontos $P(1, 6)$ e $G(1, 1)$ pertencentes a Curva E, o problema do Logaritmo discreto é encontrar um x tal que $xP = G$. Pela Tabela 2 o valor de x é 10.

2.9 Representação de Cores em Imagens

Antes de prosseguirmos para a definição da metodologia e aplicação do estudo de caso, é necessário abordar alguns tópicos no que se refere a representação de imagens para que seja possível acompanhar a explicação do estudo de caso desenvolvido.

Começamos lembrando que a aparência de um objeto é resultado da natureza da luz refletida pelo objeto, suas características óticas e a percepção humana. As cores basicamente são ondas eletromagnéticas descritas pelo seu comprimento de onda.

Existem quatro atributos que caracterizam a luz: intensidade, radiação, luminância e brilho. No caso da luz acromática somente a intensidade está envolvida. Neste caso a chamada escala de cinza ou grayscale é usada: intensidade que varia de preto a branco com tons de cinza entre eles. No caso de luz cromática, os outros três atributos são usados para mensurar a qualidade da fonte de luz. A radiação se refere à quantidade de energia emitida pela fonte de luz e é medida em watts (W). A luminância mede a quantidade de radiação percebida por um observador e é mensurada em lúmens (lm). O brilho é associado com a intensidade da luz, e apesar de ter uma definição precisa em imagens monocromáticas, é uma propriedade mais subjetiva quando se trata de imagens cromáticas.

Devido às características de absorção do olho humano, considera-se que as cores são formadas por diferentes combinações das cores primárias vermelho, verde e azul. Essas três cores podem ser combinadas para formar cores secundárias magenta (vermelho + azul), ciano (verde + azul) e amarelo (verde + vermelho). A cor branca é formada combinando as 3 cores primárias ou combinando uma cor secundária com a sua oposta primária (nas intensidades adequadas).

Em análise de imagens coloridas utiliza-se três atributos para diferenciar uma cor da outra: brilho, matiz e saturação. A matiz contem informação acerca do comprimento de onda da cor e a saturação descreve o nível de “pureza” da cor, quanto mais pura menos presença de branco há na cor. A profundidade de cor mede a quantidade de informação de cor disponível para cada pixel de imagem. Uma profundidade maior resulta em maior variedade de cores disponíveis e consequentemente a uma representação mais precisa da cor. Por exemplo, um pixel com um bit de profundidade só tem duas cores possíveis: preto ou branco. Um pixel com 8 bits de profundidade tem 256

valores possíveis de cores e um pixel com 24 bits tem mais de 16milhões de valores possíveis.

Modelos de cores são utilizados para especificar cores como pontos em um sistema de coordenadas. O próximo tópico abordará o modelo RGB, que é de fundamental importância para este trabalho, um pouco mais a fundo .

2.9.1 Modelo RGB

O modelo RGB (Red, Green, Blue) é um dos mais utilizados, principalmente em imagens de 8 bits. Normalmente utilizado para representação não só em imagens como em dispositivos eletrônicos como monitores e câmeras digitais (FRERY, 2013).

O modelo RGB é um modelo aditivo onde vermelho, verde e azul são combinados em quantidades variadas para representar as outras cores. Os pixels de uma imagem apresentada neste modelo geralmente possuem 8 bits de profundidade resultando em 256 variações possíveis variando entre 0 e 255 para cada uma das três cores do modelo.

Uma cor neste modelo pode ser descrita por meio de seus valores de vermelho, verde e azul. Cada cor varia entre o valor mínimo (completamente escuro) e o valor máximo (completamente intenso). Quando todas as cores apresentam o valor mínimo a cor preta se forma, do outro lado quando todos os valores estão no máximo forma-se a cor branca.

2.10 Formatos de imagem

Existem duas classes de informação visual que podem ser armazenadas de forma digital. As imagens do tipo Vector e as imagens do tipo Raster. A primeira é composta da descrição geométrica dos elemento que compõem a imagem. Já a segunda classe o elemento básico é o valor associado a uma posição (valor de cor de um pixel por exemplo). Por ser o modelo utilizado neste trabalho, o tipo raster será descrito em mais detalhes a seguir.

2.10.1 Formato Raster

No contexto de imagens digitais, um formato pode ser entendido com uma maneira padronizada de organizar e armazenar dados. O formato define como os dados são organizados e combinados. No caso das imagens em formato raster a representação são dados armazenados em coordenadas fixas ou pixels. Exemplos disso são fotos digitais ou imagens digitalizadas.

Alguns formatos comuns de imagens raster são GIF, JPEG e PNG. As imagens utilizadas neste trabalho são do formato .PNG, logo faz-se necessária uma explicação sobre este formato.

O formato PNG foi desenvolvido como uma versão opensource do GIF. Este formato tem profundidade de 16 milhões de cores enquanto o GIF suporta apenas 256. O PNG é ideal para edição e conversões por ser um formato livre de perdas, ao contrário do JPEG por exemplo que comprime a imagem dispensando parte da informação em prol de um menor tamanho de imagem, devido a isso imagens PNG costumam ter tamanhos maiores.

3 TÉCNICAS DE AVALIAÇÃO DE DESEMPENHO

Neste trabalho, serão aplicadas as técnicas de avaliação de desempenho para sistemas computacionais como propostas por (JAIN, 1991).

A avaliação de desempenho é útil para determinar a melhor configuração de um determinado cenário de software e/ou hardware associados, permitindo aferir qual deles é mais eficiente na solução de um problema e o quão melhor ele é em relação às demais opções disponíveis. O propósito dessa avaliação é obter os resultados com o mais alto desempenho possível com o menor custo.

A carga medida para obter os resultados pode ser real ou sintética, cargas reais são aquelas geradas com o sistema em funcionamento, como não podem ser replicadas e não é possível controlar as variáveis desejadas este tipo de carga não é recomendada para experimentos. Cargas sintéticas são aquelas semelhantes à cargas reais porem geradas em ambientes controlados. Por permitir controle das variáveis desejadas e poder ser replicada múltiplas vezes é utilizada e desenvolvida para estudos (JAIN, 1991).

A seguir, discute-se a abordagem de (JAIN, 1991).

3.1 Abordagem

Segundo (JAIN, 1991) os passos necessários para se realizar uma avaliação de desempenho sistemática são:

1. **Definir os objetivos e o sistema:** O primeiro passo é definir o objetivo do estudo, o sistema e suas fronteiras..
2. **Listar serviços e saídas:** nem todas as saídas do sistema escolhido são relevantes ao estudo, é necessário definir o que será monitorado.
3. **Selecionar métricas:** definir quais os critérios de comparação serão utilizados.

4. **Definir parâmetros:** Listar quais parâmetros afetam a performance. Dentre estes deve-se definir quais serão manipulados no estudo e quais serão constantes.
5. **Selecionar a técnica de avaliação:** Jain define três técnicas de avaliação: modelagem analítica, simulação e aferição em sistemas reais. É necessário definir qual a técnica mais adequada para o resultado desejado.
6. **Selecionar a carga de trabalho:** A carga de trabalho consiste nas entradas que o sistema vai receber, que deve ser sempre o mais proximo do funcionamento real do sistema para maior precisão.
7. **Projeto de experimentos:** definir quais experimentos serão realizados para obter o maior número de informações desejadas no sistema.
8. **Analisar e interpretar dados:** Após os experimentos é necessário avaliar os resultados obtidos. Um conhecimento profundo do sistema analisado é importante nesta etapa pois pode ajudar a detectar discrepâncias nos resultados.
9. **Apresentar resultados:** A etapa final consiste em apresentar os resultados obtidos após a avaliação de maneira que seja facilmente compreendida.

(JAIN, 1991) define alguns termos específicos utilizados nas etapas de criação e análise dos experimentos, estas são relevantes para este trabalho e são definidas a seguir:

1. **Variável de Resposta:** A saída ou saídas do sistema que serão utilizadas como métrica da avaliação de desempenho
2. **Fatores:** Variáveis que serão manipuladas durante os experimentos e que afetam a variável de resposta
3. **Níveis:** Os valores que serão atribuídos aos fatores durante os experimentos

Outro ponto relevante que (JAIN, 1991) define são os 3 tipos de projeto mais utilizados atualmente:

1. **Fatorial simples:** Onde varia-se somente um fator por vez e analisa-se a influência dele nas variáveis de resposta

2. **Fatorial completo:** Onde todas as combinações possíveis de fatores e níveis são testadas, tem como vantagem apresentar um retrato mais amplo do sistema avaliado.

3. **Fatorial parcial:** Para experimentos muito grandes, trabalha-se somente com uma parte das possíveis combinações de níveis e fatores.

Na próxima seção é descrita a plataforma computacional que foi usada nos testes.

3.2 Plataforma

Para os testes foi utilizado um notebook Dell Inspiron 15r com 8gb de RAM e sistema operacional Windows 10. Os algoritmos foram de implementação do autor, utilizando a linguagem Java. Os mesmos foram desenvolvidos e executados no IDE Eclipse para Windows, versão Neon. A seguir discute-se o estudo de caso.

3.3 Estudo de Caso

O objetivo do estudo de caso proposto é comparar os métodos de criptografia de curvas elípticas de Menezes-Vanstone e o análogo de ElGamal com curvas elípticas, quando aplicados a encriptação de imagens, a fim de determinar qual dos dois métodos tem o mais alto desempenho com o menor custo. Neste estudo de caso as variáveis de resposta são o tempo de cifragem, o tempo de decifragem, tamanho do arquivo cifrado e o tamanho do arquivo decifrado.

Cada experimento será executado 30 vezes para que se obtenha o valor da média. O tipo de projeto experimental adotado é o fatorial completo. Na Tabela 3 é mostrado cada um dos fatores considerado nos experimentos e os níveis de cada um deles.

Tabela 3 – Fatores e Níveis Abordados

Fatores	**Níveis**			
Algoritmo	ElGamal ECC		MVECC	
Curva elíptica	secp160r1	secp160k1	secp256r1	secp256k1
Tamanho da Imagem	128x128 (15kbs)	256x256 (68kbs)	512x512 (464kbs)	

A seguir é descrito por meio de fluxogramas os passos para encriptação e decriptação de imagens utilizando cada um dos métodos. O fluxograma também mostra o processo de transformação das imagens para uma representação adequada que possa ser criptografada utilizando cada um deles.

3.3.1 Análogo ElGamal com Curvas Elípticas

Nos fluxogramas 1 e 2 o método ElGamal é utilizado. Primeiramente, a imagem é pre-processada, a matriz RGB é gerada. Os elementos desta matriz são inteiros compostos de 4 bytes onde cada byte varia entre 0 a 255. Em seguida, cada elemento desta matriz é convertido em um ponto da Curva. O método de Koblitz é utilizado para converter inteiros em pontos da Curva e vice-versa. Para cada elemento da matriz de pontos gerada o método de encriptação ElGamal é chamado. A saída do método ElGamal é uma matriz de pares de pontos. Esta matriz de pares de pontos é convertida em uma matriz de pares de inteiros utilizando novamente Koblitz. Por fim, esta matriz de pares de inteiro é utilizada para gerar a imagem cifrada.

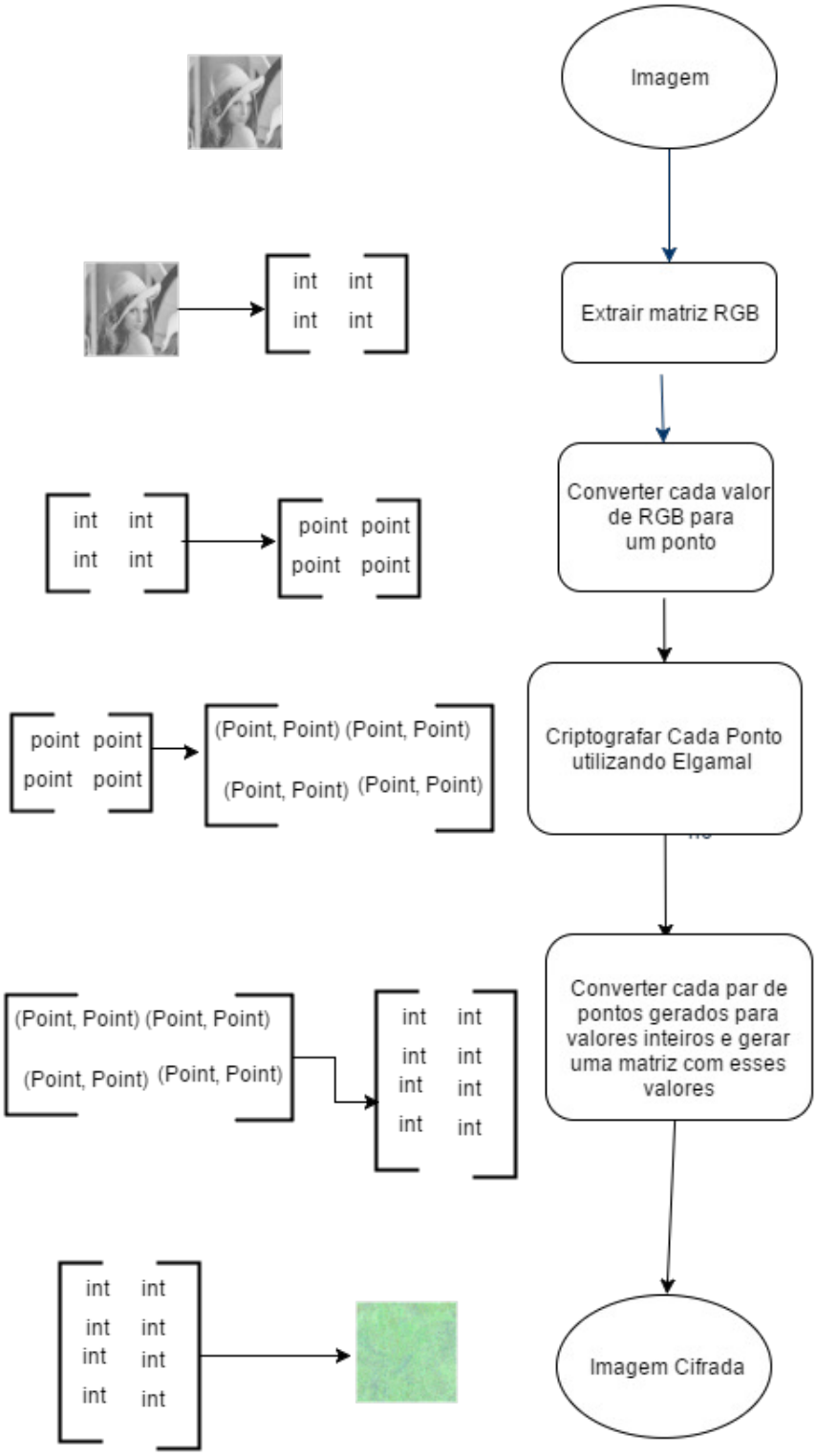


Figura 1 – Fluxograma cifragem por Elgamal

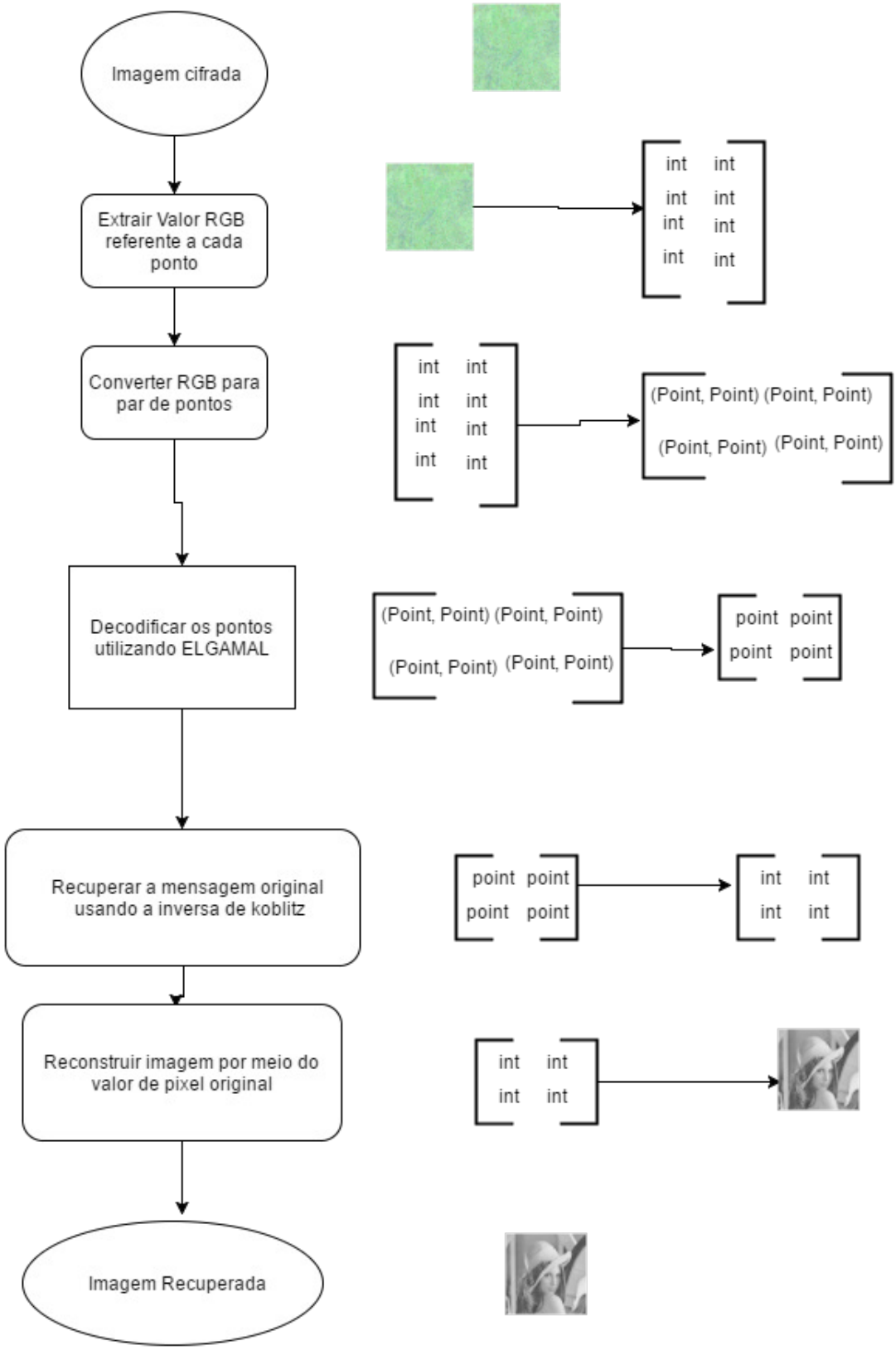


Figura 2 – Fluxograma decifragem por Elgamal

Na Figura 3 é mostrada a imagem original e o resultado após a cifragem da imagem.

Figura 3 – Lena original e Criptografada

3.4 Menezes-Vanstone

Nos fluxogramas 4 e 5 o método Menezes-Vanstone é utilizado. Novamente é feito o pré-processamento da imagem afim de obter a matriz RGB. Os elementos desta matriz são agrupados em pares ordenados e cifrados realizando a multiplicação pela chave K, que é obtida por meio de parâmetros da curva escolhida como explicado na seção 2.6.2 A saída do método é uma matriz de pares de inteiros que é utilizada para gerar a imagem cifrada. Para a recuperação da imagem é feito o mesmo processo na imagem cifrada, extrai-se a matriz RGB, depois agrupa-se em pares ordenados e realiza-se a decifragem por meio da operação inversa, que foi apresentada na mesma seção da cifragem. Após isso reconstrói-se a matriz RGB e reconstrói-se a imagem. A seguir são apresentadas a imagem original e o resultado final do processo de cifragem por Menezes-Vanstone.

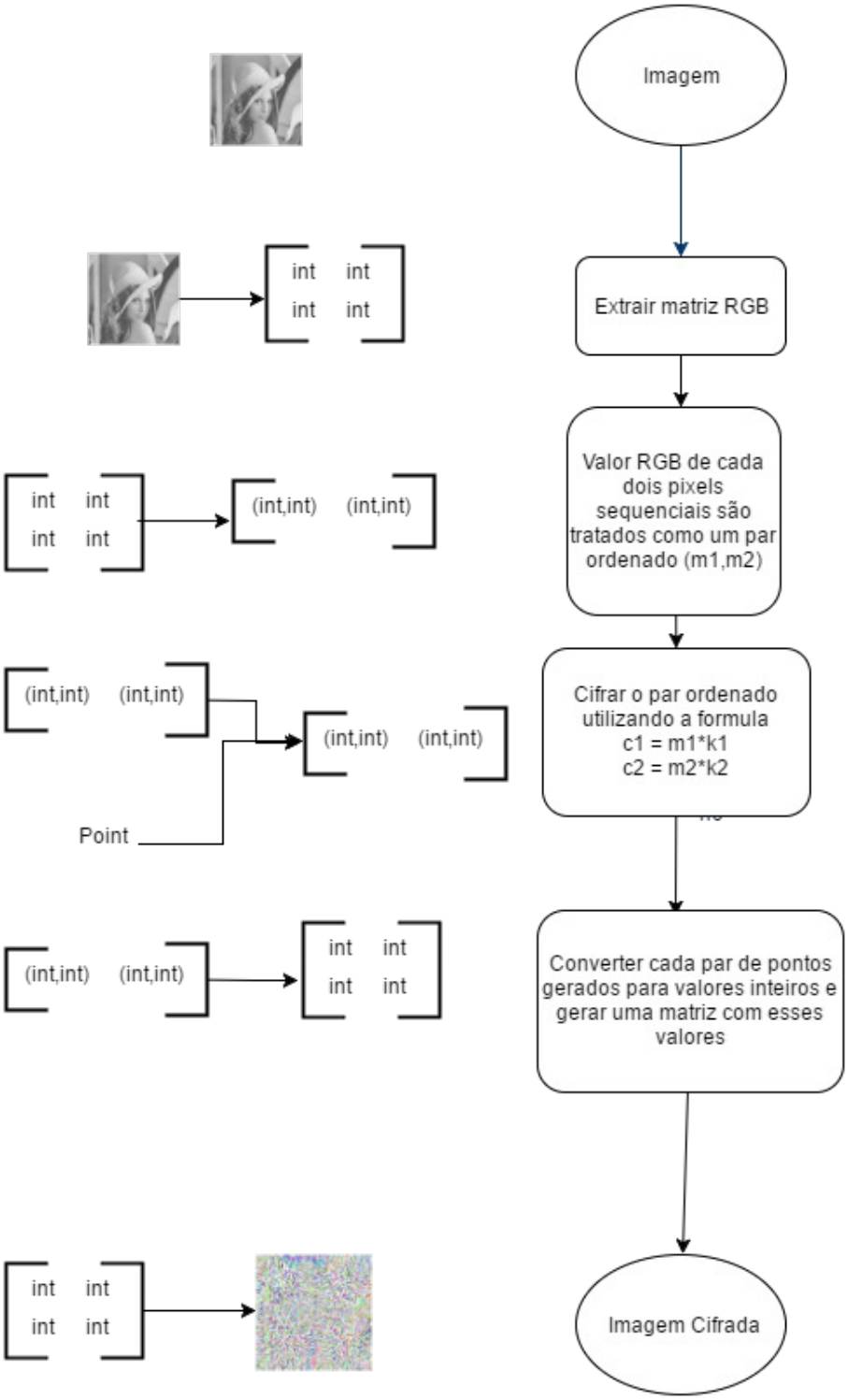


Figura 4 – Fluxograma cifragem por Menezes-Vanstone

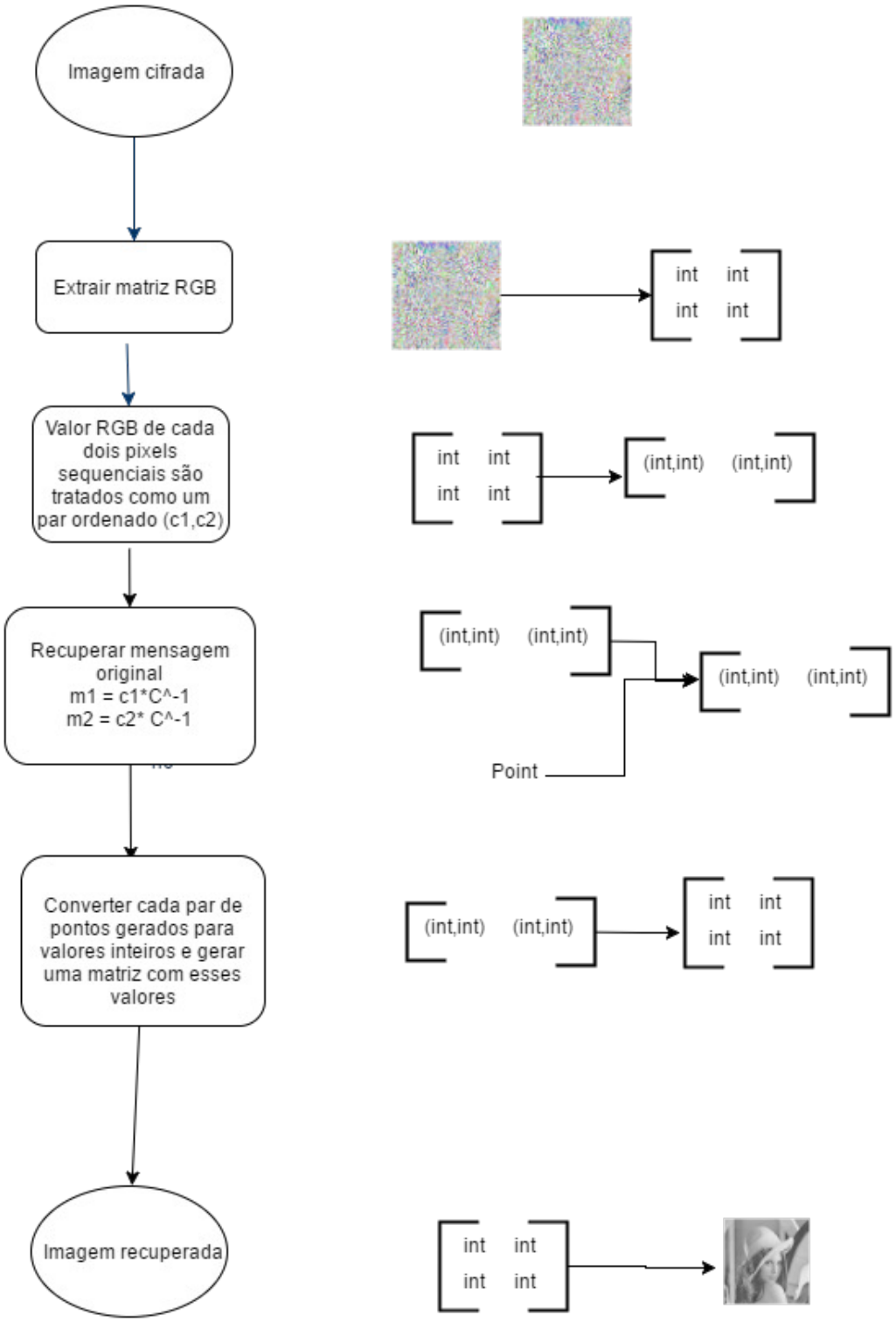


Figura 5 – Fluxograma decifragem por Menezes-Vanstone

Figura 6 – Lena original e Criptografada

4 RESULTADOS E DISCUSSÃO

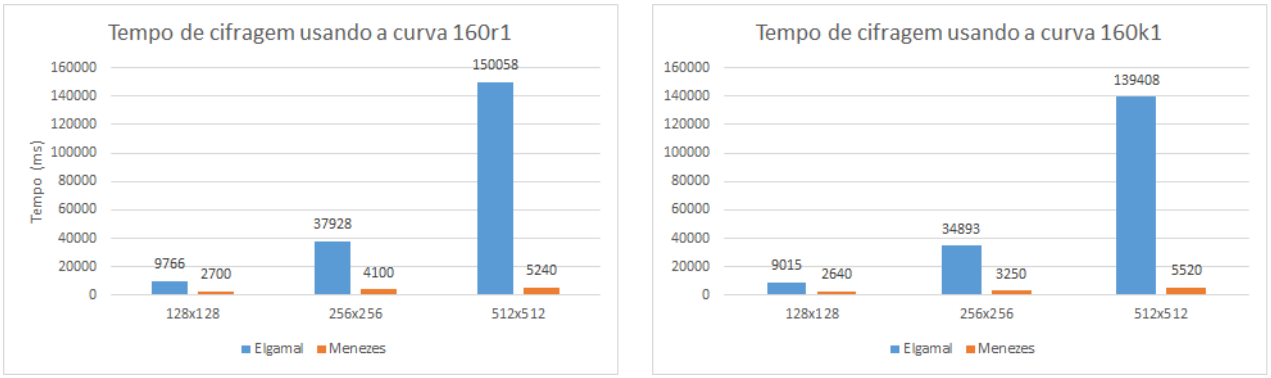
Nesta seção, os resultados obtidos nos testes são apresentados e discutidos. Os algoritmos foram avaliados com relação ao tempo de cifragem e decifragem. Os valores de tempo foram medidos utilizando a biblioteca Time do java. Os processos de acordo de chaves e geração de chaves não foram mensurados.

Também é analisado os tamanhos dos arquivos criptografados e recuperados. O tamanho da imagem recuperada pode ser diferente da imagem original. No entanto, a imagem recuperada ainda revela a informação desejada. Consequentemente, isso não afeta o processo de decifragem. O destinatário da imagem, e somente ele, tem acesso a informação original, não a imagem original.

4.1 Tempo de cifragem

O tempo de cifragem medido inclui o tempo de pré-processamento da imagem. Ele começou a ser medido imediatamente antes da obtenção da matriz RGB e ele é parado logo após a imagem cifrada ter sido gerada. Os gráficos e tabelas com os resultados, para cada curva padrão e tamanho de arquivo, são apresentados e discutidos a seguir.

Tempo de cifragem



a) b)

Figura 7 – Tempos de cifragem das curva 160 bits para Elgamal (a) e Menezes-Vanstone (b)

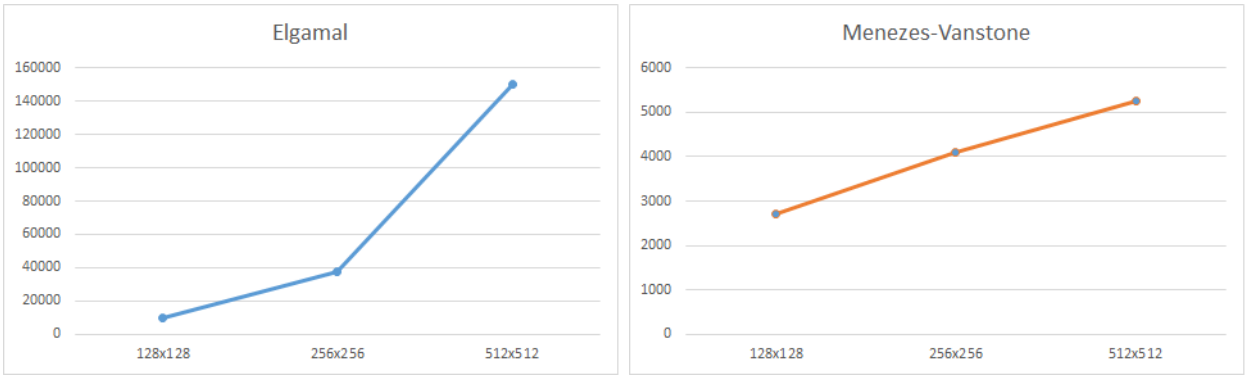
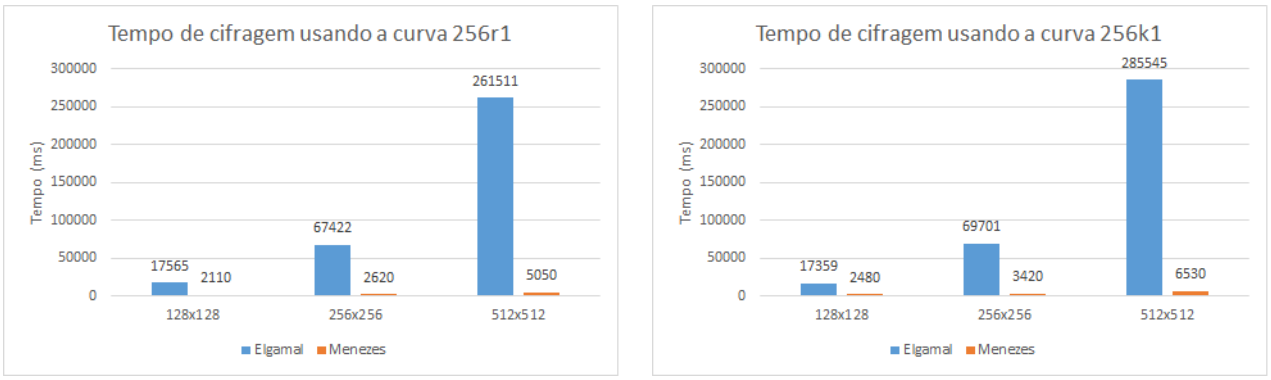


Figura 9 – Crescimento das funções de tempo de cifragem

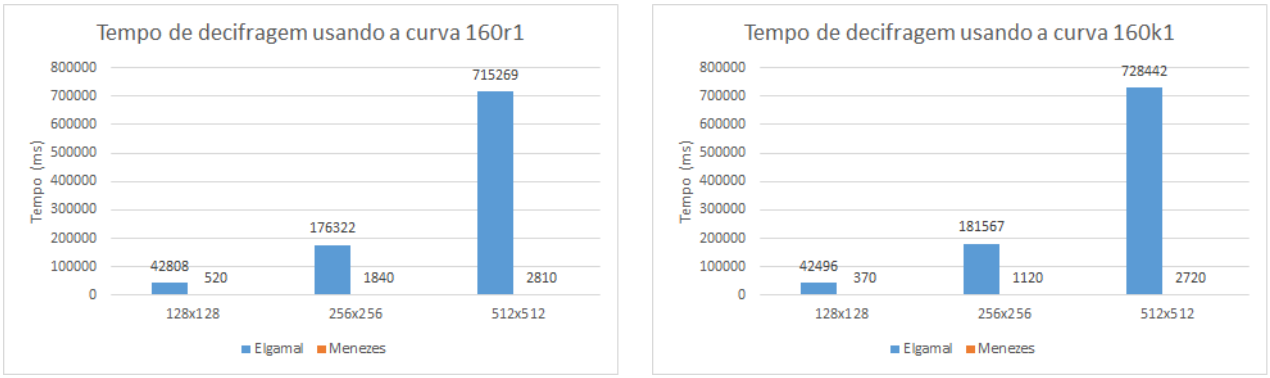


a) b)

Figura 8 – Tempos de cifragem das curvas 256bits para Elgamal (a) e Menezes-Vanstone (b)

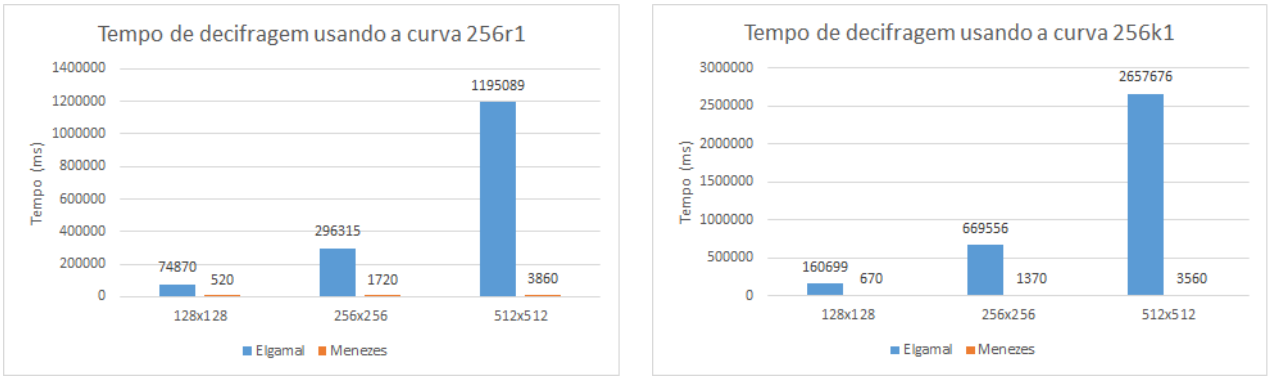
Como é possível perceber nos gráficos 7 e 8, em todas as curvas o Elgamal apresentou um tempo de cifragem muitas vezes mais alto que o do Menezes-Vanstone. Porém, é importante notar que o tempo medido para o Elgamal para encriptar uma imagem de 512x512, já é um tempo muito alto, cerca de 2.5 minutos, para um sistema interativo.

Como é comum nos dias de hoje, vermos imagens bem maiores viajando pela internet, basicamente a forma como fizemos este processo requer de melhoras. O gráfico 9 mostra que o menezes-vanstone cresce de forma linear e em pequenas quantidades diferentemente do Elgamal, para imagens de 512x512 o tempo medido ficou em torno de 90 segundos. Apesar desta melhora significativa, imagens maiores pode levar muito tempo.



a) b)

Figura 10 – Tempos de decifragem curvas de 160 bits para Elgamal (a) e Menezes-Vanstone (b)



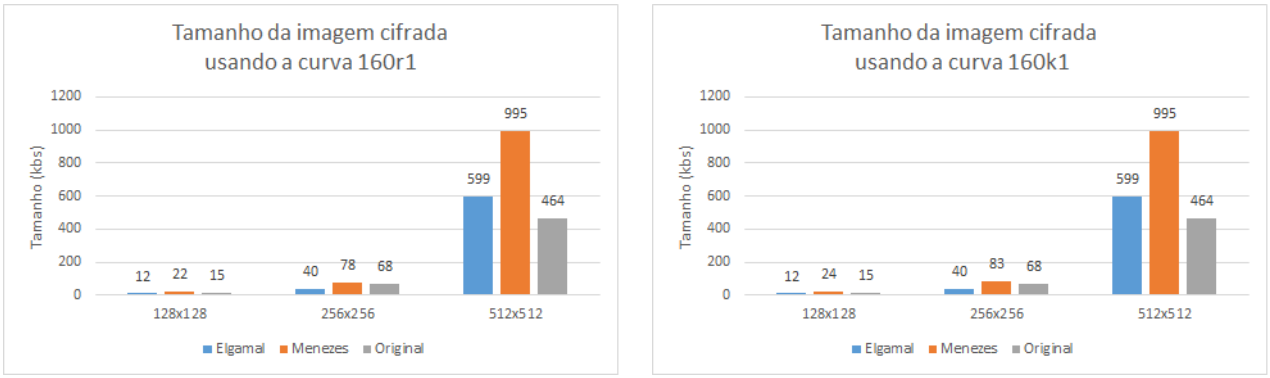
a) b)

Figura 11 – Tempos de decifragem para curvas 256bits para Elgamal (a) e Menezes-Vanstone (b)

4.2 Tempo de decifragem

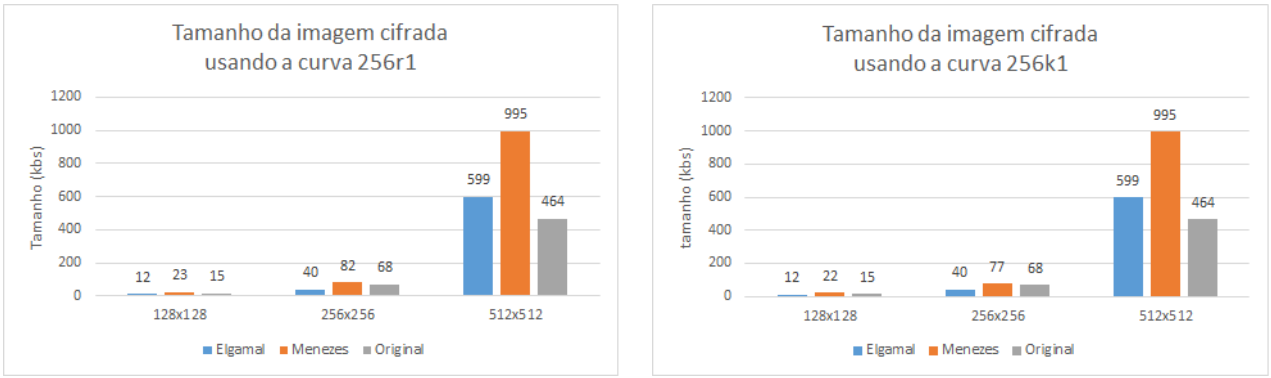
Com relação ao tempo de decifragem, os gráficos 10 e 11, nos mostram que o Elgamal apresentou um tempo ainda pior do que o da cifragem enquanto o Menezes-Vanstone melhorou, atribuímos o problema a nossa abordagem de converter cada pixel em um ponto da curva.

Também, pode se perceber que apesar dos tempos serem próximos, as curvas 160r1 e 256r1 apresentaram os melhores resultados para os dois métodos.



a) b)

Figura 12 – Tamanho da imagem cifrada em curvas 160bits para Elgamal (a) e Menezes-Vanstone (b)



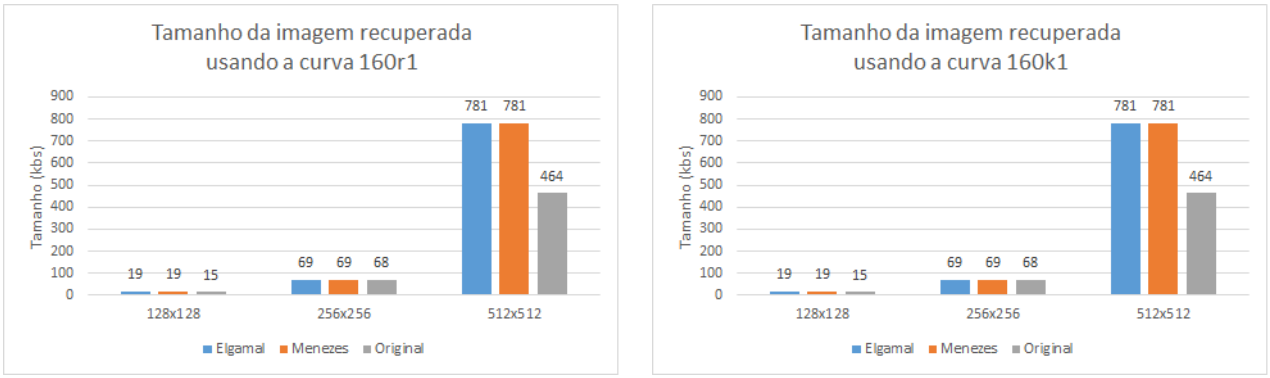
a) b)

Figura 13 – Tamanho da imagem cifrada em curvas 256bits para Elgamal (a) e Menezes-Vanstone (b)

4.3 Tamanho da imagem cifrada

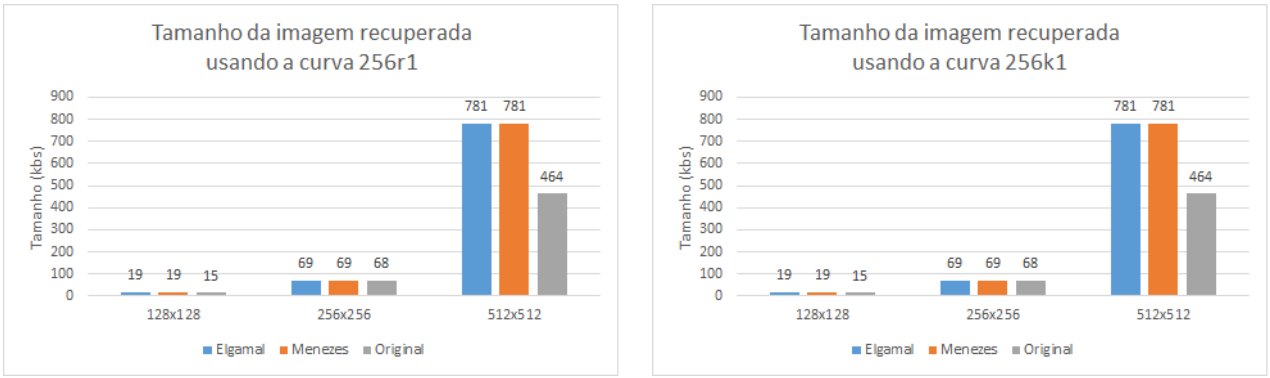
Em se tratando do tamanho da imagem cifrada gerada, o Elgamal comportou-se melhor que o Menezes-Vanstone, gerando imagens de menor tamanho em todos os casos gerando imagens menores até mesmo que a original. O que é ideal para este tipo de algoritmo tendo em vista que esses arquivos geralmente são transferidos por uma rede.

A única parte dos parâmetros que influenciou o tamanho final da imagem foi o tamanho da chave de cada curva (160 x 256) que corresponde ao módulo do grupo a ser trabalhado. Isso deve-se ao fato de um módulo maior permitir valores maiores nas operações, resultando possivelmente em resultados maiores entre uma operação com uma chave de 256 em relação a uma chave de 160 por exemplo.



a) b)

Figura 14 – Tamanho da imagem decifrada em curvas 160bits para Elgamal (a) e Menezes-Vanstone (b)



a) b)

Figura 15 – Tamanho da imagem decifrada em curvas 256bits para Elgamal (a) e Menezes-Vanstone (b)

4.4 Tamanho da imagem decifrada

Os tamanhos de imagem decifrada foram iguais para todos os casos testados, o que era esperado visto que após o tratamento todos geram um único vetor de inteiros que é aplicado à imagem, porem é importante citar que em todos os casos a imagem gerada ficou maior que a original, são necessários mais testes para comprovar se isso se deve à abordagem utilizada. É desejável que o tamanho seja o mesmo da imagem original tendo em vista que isso representaria uma reconstrução perfeita do arquivo original.

É importante mencionar que apesar de gerar tamanhos diferentes da imagem original, em todos os casos a imagem foi reconstruída perfeitamente. Para fins de transmitir a mensagem estes métodos encontram-se adequados, porém se o tamanho

da imagem for um fator essencial para digamos, uma aplicação que se utilize destes processos de cifragem. Este fator pode ser decisivo para a não utilização destes métodos da maneira que estão sendo abordados aqui.

5 CONCLUSÃO

Imagens vem se tornando cada vez mais uma parte fundamental no compartilhamento de informações do mundo conectado. Desde imagens irrelevantes até informações sigilosas podem ser transferidas por meio de imagens, logo faz-se necessário garantir a segurança dessa transferência por meio de criptografia. O trabalho atual apresentou uma análise de dois algoritmos de criptografia baseada em curvas quando aplicados ao contexto de imagens com o objetivo de auxiliar na escolha do mais adequado para este contexto . Os resultados foram apresentados por meio de gráficos contendo o valor médio das execuções. Os estudos de caso avaliaram os algoritmos em três fatores diferentes e usaram quatro variáveis de resposta para realizar as métricas.

Por meio da análise dos resultados foi possível observar que nenhum dos dois algoritmos atingiu um desempenho satisfatório em todos os aspectos. O método de Menezes-Vanstone apresentou tempos de cifragem e decifragem satisfatório para imagens pequenas, mas aumentou o tamanho do arquivo criptografado gerado. Já o Elgamal aplicado a curvas apresentou tempos de cifragem e decifragem muito elevados, tornando inviável sua aplicação na vida real envolvendo este contexto.

Porém dentro do contexto caso fosse necessário recomendar uma configuração a ser utilizada, a preferencia seria dada a utilizar o método de Menezes-Vanstone com a curva 106r1 devido ao tempo de execução dos processos.

O trabalho atual deu um primeiro passo no sentido de avaliar aplicabilidade destes métodos para imagens, mas é necessário buscar mais estratégias alternativas e criar novos métodos específicos para encriptação de imagens.

5.1 Dificuldades encontradas

Ao longo do desenvolvimento desta pesquisa algumas dificuldades foram encontradas. A primeira delas refere-se à informações gerais sobre criptografia no contexto de imagem. A maioria da literatura aborda os métodos mas não trata a questão no geral, comprovando que ainda há bastante espaço de pesquisa nesta área.

Outra dificuldade encontrada foi na obtenção de implementações de criptografia de curva elíptica que já estivessem validadas de forma que pudessem ser aplicada a este caso de estudo. Como não foram encontradas bibliotecas que se adequassem às necessidades os algoritmos tiveram de ser desenvolvidos durante o estudo. O que nos leva a outra dificuldade encontrada que foi, à medida que existem várias implementações e explicações referentes ao Elgamal, grande parte da literatura referente ao Menezes-Vanstone só trata o método de forma matemática, o que tornou necessária a implementação do método partindo praticamente do zero.

Uma última dificuldade encontrada a medição dos tempos de execução dos algoritmos. O método de Elgamal apresentou tempos de execução extremamente elevados, o que dificultou a execução dos testes a fim de obter a média para o método fatorial completo que foi adotado no trabalho. Infelizmente por conta do tempo ocupado pelos testes não foi possível realizar muitos testes pontuais a fim de detectar exatamente o que ocasionou esta situação, sabendo-se apenas que a maior parte do tempo de execução estava nas funções de cifragem e decifragem.

Como os resultados foram bem distantes um do outro, houveram alguns problemas na hora de escolher a melhor forma de apresentá-los. Após tentar vários gráficos diferentes como linha, progressão e barra composta optou-se por permanecer no de barras que visualmente apresentou melhor os dados.

5.2 Trabalhos futuros

O trabalho atual permite muitas extensões tendo em vista que o tema de criptografia de curvas elípticas é fruto de pesquisa contínua, algumas possibilidades de trabalho futuro são:

- Buscar outras abordagens do Elgamal para imagens a fim de torná-lo viável neste contexto.
- Incluir outros algoritmos criptográficos no escopo para ampliar a pesquisa, tais como o ECIES.
- Testar outras curvas recomendadas para buscar a mais eficiente, mesmo que marginalmente.

REFERÊNCIAS

BELAZI, A.; EL-LATIF, A. A. A.; BELGHITH, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, v. 128, p. 155 – 170, 2016. ISSN 0165-1684. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0165168416300147>. Citado na página 14.

DIFFIE W.; HELLMAN, M. New directions in cryptography. *Transactions on Information Theory*, IEEE, v. 7, n. 13, p. 85, 2013. Citado na página 19.

FRERY, T. P. *Introduction to Image Processing Using R*. [S.l.]: Springer, 2013. ISBN 9781447149507. Citado na página 28.

GAMAL, T. E. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, v. 31, n. 4, p. 469–472, 1985. Disponível em: <http://dx.doi.org/10.1109/TIT.1985.1057074>. Citado na página 14.

HANKERSON, D.; MENEZES, A. J.; VANSTONE, S. *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN 038795273X. Citado na página 20.

JAIN, R. *Art of Computer Systems Performance Analysis: Techniques for Experimental Design, measurement, simulation and modeling*. [S.l.]: Wyley Professional Computing, 1991. ISBN 0471503363. Citado 2 vezes nas páginas 30 e 31.

JUST, M. *Cryptography III:Symmetric Cyphers*. [S.l.: s.n.], 2012. Disponível em<http://www.inf.ed.ac.uk/teaching/courses/cs/0910/lecs/symmetric-6up.pdf>. Citado na página 18.

MENEZES, A. J.; VANSTONE, S. A. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, v. 6, n. 4, p. 209–224, 1993. ISSN 1432-1378. Disponível em: <http://dx.doi.org/10.1007/BF00203817>. Citado na página 14.

SILVA, B. da et al. Aplicação de técnicas de criptografia de chaves assimétricas em imagens. Citado na página 14.

SMART, N. *Introduction to Cryptography*. [S.l.]: Mcgraw-Hill College, 2004. ISBN 9780077099879. Citado 2 vezes nas páginas 17 e 19.

SOLEYMANI, A.; NORDIN, M. J.; ALI, Z. M. A novel public key image encryption based on elliptic curves over prime group field. *Journal of Image and Graphics*, v. 1, n. 1, 2013. Citado na página 14.

SOLEYMANI, A. et al. An image encryption scheme based on elliptic curve and a novel mapping method. *International Journal of Digital Content Technology and its Applications*, Advanced Institutes of Convergence Information Technology, v. 7, n. 13, p. 85, 2013. Citado na página 14.

TANENBAUM, A. *Redes de computadores*. CAMPUS - RJ, 2003. ISBN 9788535211856. Disponível em: <https://books.google.com.br/books?id=0tjB8FbV590C>. Citado na página 17.

ZEGHID, M. et al. A modified aes based algorithm for image encryption. *International Journal of Computer Science and Engineering*, Citeseer, v. 1, n. 1, p. 70–75, 2007. Citado na página 14.