PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Universidade Federal do Rio de Janeiro

DISSERTAÇÃO DE MESTRADO

REDE DE CONFIANÇA: UMA POLÍTICA DE SEGURANÇA PARA O ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS

Humberto Ferreira Ramos Junior

2011

Instituto de Matemática

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Humberto Ferreira Ramos Junior

REDE DE CONFIANÇA: UMA POLÍTICA DE SEGURANÇA PARA O ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Instituto de Matemática e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Mestre em Informática.

Orientadora:

Claudia Lage Rebello da Motta

RIO DE JANEIRO

2011

R175 Ramos Jr, Humberto Ferreira

Rede de Confiança: Uma Política de Segurança para o Armazenamento de Informações Sensíveis / Humberto Ferreira Ramos Junior. -- 2011.
109 f.: il.

Dissertação (Mestrado em Informática) – Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, 2011.

Orientadora: Claudia Lage Rebello da Motta

1. Segurança da Informação (Teses). -- 2. Compartilhamento de Recursos (Teses). -- 3. Computação Distribuída (Teses). – I. Claudia Lage Rebello da Motta (Orient.). II. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais III. Título.

CDD

REDE DE CONFIANÇA: UMA POLÍTICA DE SEGURANÇA PARA O ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Instituto de Matemática e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Mestre em Informática.

Aprovada em 31 de outubro de 2011.

Claudia Lage Rebello da Motta, D.Sc., PPGI e iNCE/UFRJ (Orientadora)

Marcos da Fonseca Elia, Ph.D., PPGI e iNCE/UFRJ

Paulo Henrique de Aguiar Rodrigues, Ph.D., DCC/UFRJ

Paulo Sergio Pagliusi, Ph.D., ESAF

Aos meus grandes amores: Margareth e Hosana.

AGRADECIMENTOS

A Deus pela maravilhosa luz que me guiou durante esta caminhada.

À minha esposa Margareth pelo apoio e compreensão neste longo período de dedicação aos estudos. Você é a fonte de energia inesgotável que me faz levantar e caminhar com alegria todos os dias.

À minha mãe Hosana, origem da minha vida. Agradeço pela preocupação e palavras de incentivo, embora separados pela distância.

À Profª Claudia Motta, minha atual Orientadora, sempre atenciosa e zelosa pelo correto caminhar durante o desenvolvimento desta obra. Sua dedicação deve ser um exemplo a ser seguido por todos nesta instituição. Deixo aqui registrada a minha admiração e reconhecimento.

Ao Prof. Carlo Emmanoel, pelas diversas palavras de incentivo. Nossas conversas e decorrentes idéias foram fontes inspiradoras para a materialização desta dissertação. Agradeço profundamente, além dos seus ensinamentos, pelas palavras de incentivo neste período acadêmico.

À Profª Luci Pirmez pela inicial orientação no curso de Mestrado.

Ao Prof. Marcos Elia por ter aceitado o convite de estar compondo tão distinta banca de Mestrado. Não saberia como retribuir esta gratidão.

Ao Prof. Paulo Aguiar pelas várias pelas conversas e orientações. Apesar de muito atarefado, sempre conseguiu tempo em sua agenda na tentativa de direcionar minhas pesquisas.

Ao Comandante Paulo Sergio Pagliusi pela cordialidade e pela honra ter um Oficial de Marinha de tão alto gabarito presente em minha banca de Mestrado.

Aos Comandantes Alexandre Souto de Melo Aquino e Nilson Rocha Vianna, ambos da Diretoria de Comunicações e Tecnologia da Informação da Marinha, pelas diversas orientações tanto na vida acadêmica quanto na vida militar. Com certeza, a Marinha saberá reconhecer sua dedicação à carreira naval.

Ao Comandante Rogério Corrêa Manso e à Comandante Cláudia de Abreu Silva pelo grande apoio, principalmente, por tolerarem minhas ausências no trabalho, o que tornou possível a conclusão desta obra.

Aos amigos Hélio Salmon, Tiago Cruz, André Sion, Claudio Miceli, Henrique Ribeiro, Paola Garcia, Gustavo Santos, Thomaz Barros e demais colegas do LabNet,

LabVoip, etc, pelos momentos de descontração e conversas acadêmicas que me foram de grande valia. Aprendi muito com vocês.

Por fim, agradeço a todos aqueles que direta ou indiretamente contribuíram para a conclusão desta obra.

RESUMO

RAMOS JUNIOR, Humberto Ferreira. **REDE DE CONFIANÇA: UMA POLÍTICA DE SEGURANÇA PARA O ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS**. Rio de Janeiro, 2011. Dissertação (Mestrado em Informática) – Departamento de Ciência da Computação, Instituto de Matemática e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2011.

O potencial do compartilhamento de recursos em redes de computadores vem sendo cada vez mais explorado. Entretanto, devido à natureza dos assuntos abordados, certas instituições ainda relutam quanto ao uso da tecnologia no armazenamento de dados sensíveis. Este trabalho apresenta uma política voltada à proteção e sobrevivência de informações sigilosas que leva em consideração dois parâmetros: o grau de confidencialidade da informação e a reputação do usuário que solicita acesso ao dado armazenado. A sobrevivência é caracterizada pela distribuição das informações por uma Rede de Confiança formada por instituições localizadas em pontos geograficamente distintos.

Palavras-chave: Segurança da Informação, Compartilhamento de Recursos, Computação Distribuída, Redes *peer-to-peer*.

ABSTRACT

RAMOS JUNIOR, Humberto Ferreira. **REDE DE CONFIANÇA: UMA POLÍTICA DE SEGURANÇA PARA O ARMAZENAMENTO DE INFORMAÇÕES SENSÍVEIS.** Rio de Janeiro, 2011. Dissertação (Mestrado em Informática) – Departamento de Ciência da Computação, Instituto de Matemática e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2011.

The potential of resource sharing in computer networks is being increasingly adopted. However, due to the nature of issues, certain institutions are still reluctant about the use of technology in the storage of sensitive data. This work presents a policy aimed at the protection and the survival of sensitive information that takes into account two parameters: the degree of confidentiality of information and the reputation of the user requesting access to stored data. Survival is characterized by the distribution of information on a Network of Trust formed by institutions located in different geographical places.

Keywords: Information Security, Resource Sharing, Distributed Computing, Per-to-peer Network.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AES	*Advanced Encryption Standard*
ARPA	*Advanced Research Projects Agency*
CFS	*Cooperative File System*
DES	*Data Encription Standard*
GUID	*Global Unique Identifier*
IDEA	*International Data Encryption Algorithm*
IP	*Internet Protocol*
MD	*Message Digest*
MTTR	*Mean Time to Repair*
P2P	*Peer-to-peer*
TCP	*Transmission Control Protocol*
TR	Tempo de Recuperação

SUMÁRIO

Capítulo 1 – Introdução

Neste capítulo é apresentada a pesquisa documentada nesta dissertação, abordando a motivação, o problema, o cenário, as hipóteses de pesquisa, os objetivos, a metodologia utilizada, a contribuição da dissertação e a organização do texto.

1.1 A MOTIVAÇÃO DA PESQUISA

Em certos setores comerciais, industriais e do governo, tais como as Forças Armadas e Organizações de Inteligência, há informações armazenadas que vão de segredos mercantis a assuntos que podem colocar em risco inclusive a segurança nacional. Dados sobre o desenvolvimento de um novo projeto comercial, segredos de Estado, conhecimento sobre sistemas de armas, identidades de agentes e informantes podem estar digitalmente arquivados de forma segura em uma construção destinada à salvaguarda deste conhecimento, entretanto danos às suas instalações físicas onde estas informações estão guardadas podem levar à perda destes dados sigilosos.

As informações devem ser salvaguardadas de forma segura a fim de evitar sua perda ou comprometimento, seja em caso de acidente, por motivo de força maior (acontecimentos da natureza, por exemplo) ou pela incidência de vírus ou *hackers*. Dependendo do tamanho dos dados a serem guardados, uma opção é realizar cópias de segurança em mídias removíveis ou dispositivos externos, entretanto isto deve ser feito de forma sistemática e não há garantias contra eventuais acidentes que possam destruir os dispositivos utilizados. Outra opção à salvaguarda da informação é a utilização de serviços na Internet contratados para armazenar os dados coletados, contudo é muito difícil comprovar se os dados não estão sendo analisados por outros indivíduos, além de não termos a plena garantia de que eles estarão sempre disponíveis.

Aplicações em número cada vez mais crescentes permitem o armazenamento de informações e o compartilhamento de recursos em estações de trabalho e computadores pessoais. No atendimento a esta tendência, as redes *peer-to-peer* (P2P) surgiram com a característica de serem altamente escaláveis, além de permitirem a troca direta e em tempo real de serviços e informações entre usuários localizados em plataformas geograficamente distribuídas e potencialmente heterogêneas [Kalogeraki *et al.* 2002].

1.2 O PROBLEMA

A internet oferece várias oportunidades para o compartilhamento de recursos e informações, bem como para a formação de grupos de indivíduos com interesses afins através das redes sociais. Entretanto, o armazenamento de informações sigilosas por intermédio da utilização de sistemas cujo gerenciamento dos recursos em um ambiente altamente distribuído é feita por terceiros, leva o membro da rede a duvidar se seus dados podem estar sendo analisados pelo administrador da aplicação.

Armazenar os dados na Internet, também leva o usuário a preocupar-se quanto à disponibilidade dos dados. Uma empresa pode terceirizar o serviço de armazenamento dos dados para outra organização sem que este fato seja participado ao usuário e, deste modo, o proprietário das informações desconhecerá a localização real dos seus arquivos. Além disso, em caso de falência da organização, seria necessário haver a garantia de que suas informações serão recuperadas [Devine 2008].

Além dos riscos já abordados, existem requisitos a serem satisfeitos pela infra-estrutura do sistema [Barcellos e Gaspary 2006], tais como:

- Confidencialidade: Os dados armazenados na rede devem ser acessíveis apenas pelo grupo de indivíduos que possuam este direito;
- Autenticação e Autorização: Apenas usuários cadastrados possam participar da rede;
- Disponibilidade: As informações devem estar acessíveis quando solicitadas; e
- Reputação: Grau de confiabilidade depositado nos demais participantes do sistema. Um usuário com comportamento malicioso deve deixar ou ter seus direitos penalizados à medida que apresenta uma conduta indesejada.

1.3 O CENÁRIO

O presente trabalho tem sua aplicabilidade voltada a uma rede de grande área (WAN - *Wide Area Network*), composta pelas estações de trabalho de uma organização, ou conjunto de organizações, com sedes em distintos lugares geográficos. Esta rede de caráter predominantemente corporativo, sempre que possível, deve ser constituída por recursos próprios, evitando a dependências das prestadoras de serviços de telecomunicações.

Adicionalmente, esta rede corporativa com endereços IP (*Internet Protocol*) privados deve possuir dispositivos de segurança, tais como *firewalls*, que possibilitam sua interligação de maneira segura com a Internet. Os sítios externos acessados são monitorados e filtrados em função de seu conteúdo com o intuito de minimizar a entrada de programas maliciosos na rede.

Outra característica importante é o fato de que os membros dessas organizações, por trabalharem com assuntos sigilosos, devem ser previamente investigados com o objetivo de minimizar as chances de que indivíduos com comportamentos maliciosos passem a constar de seus quadros e venham a expor assuntos confidenciais a terceiros.

Partindo-se da premissa que os usuários da rede são confiáveis, é de se esperar que suas estações de trabalho sejam utilizadas com correção e de maneira adequada, passando a serem consideradas estações seguras para o armazenamento de informações confidenciais.

1.4 HIPÓTESES

Informações sigilosas devem ser armazenadas de forma segura e de maneira restrita aos seus usuários. Ou seja, deve ser imprescindível que um atacante não consiga obter acesso às informações guardadas. Em prol dessa necessidade, trabalhamos na construção de uma infra-estrutura capaz de satisfazer duas hipóteses:

- Hipótese 1: A fragmentação de arquivos em rede impede o acesso a um dado armazenado, além de possibilitar a sobrevivência das informações, caso a sede de uma organização seja alvo de um ataque ou vítima de uma calamidade natural; e

- Hipótese 2: Um esquema de criptografia híbrida, que combina a segurança da criptografia assimétrica com a rapidez de processamento da simétrica, garante o sigilo das informações armazenadas na rede.

As condições acima devem ser satisfeitas, levando-se em consideração o impacto no tempo de resposta da aplicação. Por isso, neste trabalho, procuramos adotar as seguintes questões de pesquisa:

- Analisar o impacto da fragmentação dos arquivos, nos processos de armazenamento e recuperação, a partir da infra-estrutura de segurança proposta; e

- Analisar os tempos de armazenamento e recuperação dos arquivos. A principal preocupação recai sobre a recuperação, pois o usuário não deve ter uma espera excessiva quando solicita acesso a um dado armazenado.

Além disso, contemplamos a utilização de um mecanismo capaz de analisar a reputação das estações de trabalho. Como os arquivos armazenados na rede possuem diferentes graus de sigilo, o intuito é garantir que os arquivos sejam acessados por máquinas cujo atual *status* de reputação seja compatível com o sigilo atribuído às informações. Ou seja,

quanto maior o sigilo do arquivo, mais confiável deve ser a estação de trabalho. Assim, diminuímos as chances de que uma estação maliciosa consiga acesso aos dados sigilosos.

1.5 OBJETIVO

Com o intuito de prover a salvaguarda das informações digitais, usufruindo do potencial apresentado pelos sistemas *peer-to-peer*, o objetivo principal desta obra é apresentar uma política de segurança a ser empregada em organizações que trabalham com informações sensíveis que visa garantir a disponibilidade e o sigilo das informações em uma rede P2P denominada *Rede de Confiança*. Tal política leva em consideração dois parâmetros: o grau de confidencialidade da informação e a reputação do usuário *(peer)* que solicita acesso ao dado armazenado.

A *Rede de Confiança* sugerida é constituída pelos membros de uma organização, onde suas estações de trabalho cedem espaço ocioso em disco rígido para o armazenamento coletivo de arquivos. Tais arquivos antes de serem gravados na rede são divididos em *n* partes criptografadas e armazenadas em máquinas distintas. Adicionalmente, as máquinas são monitoradas e recebem *status* de reputação em virtude de suas interações com os demais pontos da rede. A reputação é levada em consideração por ocasião da solicitação de acesso a um dado armazenado, de tal maneira que quanto maior o sigilo de um arquivo, maior deve ser a reputação do *peer* solicitante.

1.6 METODOLOGIA

Este trabalho realiza uma pesquisa exploratória de maneira que seus resultados contribuam para a segurança da informação em questões relacionadas ao compartilhamento de arquivos em rede. O desenvolvimento da obra abrange cinco etapas: a descrição das características utilizadas na concepção da *Rede de Confiança*; o levantamento de trabalhos relacionados; a exposição da macro-arquitetuta desta Rede; a descrição da política de controle de acesso entre os agentes do sistema utilizando o sistema de reputação; e a análise dos resultados gerados a partir de experimentos envolvendo os processos de fragmentação, criptografia e armazenamento de dados espalhados na rede.

Na primeira etapa, são descritos os conceitos básicos e as características utilizadas para a concepção da uma *Rede de Confiança* que provê a segurança da informação através do arquivamento distribuído de informações sigilosas. Em seguida, na segunda etapa, o levantamento de trabalhos relacionados tem como foco encontrar na literatura questões e

soluções relacionadas ao compartilhamento de arquivos e segurança da informação que sirvam como alicerces para a construção da proposta.

A terceira fase envolve a descrição de uma macro-arquitetura cujo foco é a segurança de dados sigilosos. Sua concepção prevê o uso de técnicas de criptografia e a existência de um mecanismo de reputação que julga a confiabilidade das estações de trabalho (*peers*) dos usuários da rede.

Na quarta fase, são apresentadas políticas de controle de acesso a que estão subjugados os agentes desse sistema, de forma que as informações sejam tratadas e protegidas em função de duas variáveis: o grau de confidencialidade da informação e a reputação do usuário que solicita acesso ao dado armazenado.

Na quinta fase, apresentamos os resultados dos experimentos envolvendo a fragmentação, a criptografia, o armazenamento e a recuperação de dados na rede. Foram feitas avaliações do impacto da divisão do arquivo em blocos, variando o número de divisões utilizadas no processo de fragmentação. Além disso, avaliamos o impacto da variação do tamanho das chaves empregadas nos processos de criptografia.

1.7 A CONTRIBUIÇÃO DA DISSERTAÇÃO

Este trabalho almeja colaborar na demonstração da aplicabilidade do uso de redes *peer-to-peer* para a salvaguarda de informações sensíveis. Como contribuição, é proposta uma infra-estrutura que conjuga: o armazenamento distribuído de arquivos, o compartilhamento de informações entre usuários de forma segura e a utilização de um mecanismo de reputação para a avaliação da confiabilidade entre os *peers*.

É apresentada uma solução prática de um sistema voltado à sobrevivência das informações que permite a colaboração de organizações voltadas à salvaguarda de dados sigilosos. Esta sobrevivência é caracterizada pela distribuição das informações por uma *Rede de Confiança* formada por instituições localizadas em pontos geograficamente distintos, permitindo que os dados sigilosos não sejam perdidos, caso uma das sedes das organizações seja comprometida de alguma forma, quer seja por desastre natural ou em função de alguma ofensiva por forças inimigas, por exemplo.

A proposta está alinhada com tendência à proteção a dados confidenciais, uma necessidade apontada por algumas nações em virtude de possíveis ofensivas as suas instalações. Uma prova disso é o desenvolvimento, por parte da Marinha dos Estados Unidos, de uma rede *Onion Routin* para o compartilhamento de informações politicamente sensíveis e

proteção a funcionários públicos do setor de inteligência norte-americano [Global Oneness 2010].

Ao final deste trabalho, ainda como contribuição, apresentamos um conjunto de apêndices com dados reais, relativos aos processos de armazenamento e recuperação de dados em dois ambientes: uma rede local e via Internet.

1.8 ORGANIZAÇÃO DA DISSERTAÇÃO

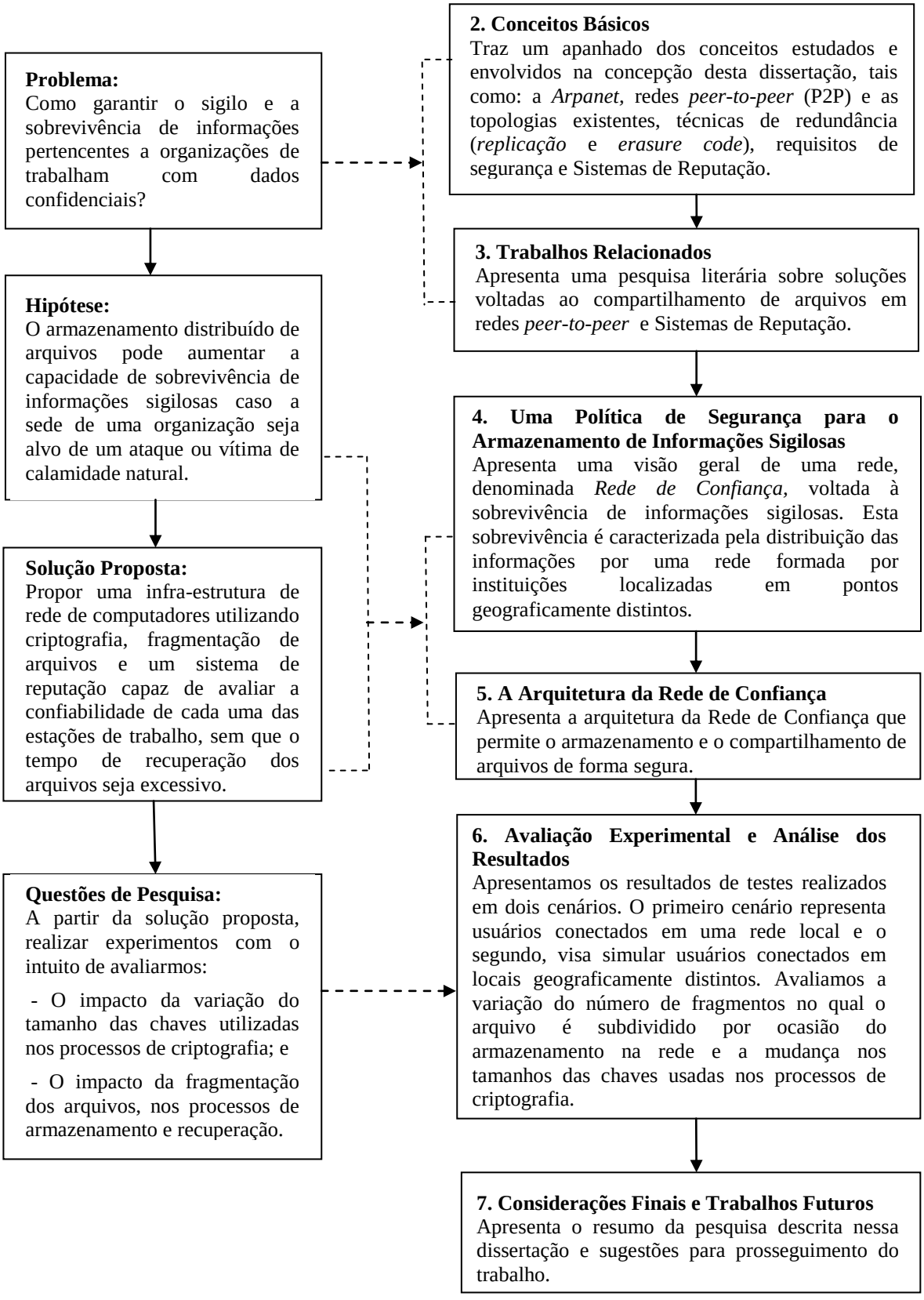

Figura 1. 1. Apresentação da dissertação

Capítulo 2 – Conceitos Básicos e Considerações sobre o Modelo Adotado

Este capítulo traz um apanhado dos conceitos estudados e envolvidos na concepção desta dissertação. De início, apresentamos a *Arpanet* com o intuito de demonstrar que não é de agora o interesse em pesquisas voltadas à utilização de redes de computadores na proteção de informações sigilosas, integrando pessoas geograficamente distantes.

Abordaremos também o conceito de redes *peer-to-peer* (P2P) e as topologias existentes, juntamente com as técnicas de redundância utilizadas em sistemas P2P de *backups*. São analisadas as técnicas de *replicação* e *erasure code* com o intuito de demonstrar sua aplicabilidade, analisando-as em função de dois fatores: a confiabilidade e a recuperabilidade dos arquivos. Introduzimos também os requisitos necessários para que a *Rede de Confiança* possa desempenhar seu papel garantindo a salvaguarda das informações nela armazenadas.

Apresentamos uma subseção sobre Sistemas de Reputação, mecanismos que nasceram sob a concepção de prevenção contra comportamentos maliciosos da rede. Além disso, faremos uma breve introdução sobre criptografia e seus tipos em função do uso de chaves. Por fim, elencamos as características empregadas no modelo proposto nesta dissertação.

2.1 ARPANET: A PRIMEIRA REDE PARA ASSUNTOS SIGILOSOS

A rede mundial de computadores surgiu da idéia de se utilizar uma rede que propiciasse proteção a um conjunto de informações. No ápice da Guerra Fria, final dos anos 50, os Estados Unidos da América tinham o objetivo de construir uma rede de Comando e Controle capaz de sobreviver a possíveis ataques da União Soviética. A ARPANET, criada pela ARPA, sigla para *Advanced Research Projects Agency*, surgiu com o propósito de descentralizar a guarda de dados sigilosos através do compartilhamento e troca de informações. A principal preocupação era a possibilidade da perda de milhares de informações sigilosas, caso um ataque nuclear fosse realizado ao *Pentágono*, sede do Departamento de Defesa dos Estados Unidos.

Naquela época, as trocas de subsídios entre as Forças Armadas e órgãos de Inteligência eram realizadas utilizando a rede pública de telefonia. Uma das preocupações era a fragmentação do sistema de informações, caso algumas de suas centrais interurbanas fossem atingidas, conforme pode ser observado na Figura 2.1(a). A fim de suprir esta falha, surgiu a ARPANET, um sistema distribuído formado por uma rede comutada de pacotes em forma de malha, trazendo a robustez considerada necessária (ver Figura 2.1(b)) [Tanenbaum 2003].

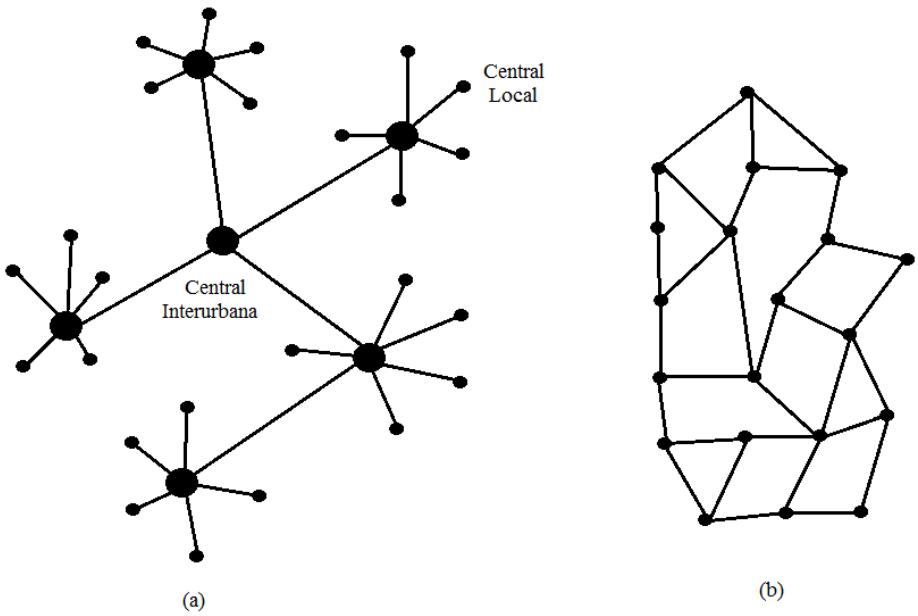

Figura 2.1. (a) Sistema de Telefonia (b) ARPANET [Tanenbaum 2003].

Ao passar dos anos, a ARPANET difundiu-se e foi aberta às universidades. Com isso, o número de máquinas e usuários cresceu vertiginosamente, principalmente após o desenvolvimento do TCP/IP (*Transmission Control Protocol/ Internet Protocol*), uma

arquitetura de protocolos de comunicação criada para manipular a comunicação entre computadores em rede.

O modelo de computação mais amplamente utilizado na Internet passou a ser denominado *cliente/servidor*, onde um usuário (*cliente*) passou a ter acesso à rede utilizando seu computador pessoal por intermédio de um provedor de serviços (*servidor*). Entretanto, à medida que as pesquisas avançaram nesta área, outras tecnologias surgiram, entre elas, a de compartilhamento de recursos *peer-to-peer*.

2.2 REDES *PEER-TO-PEER*

O grande crescimento da Internet possibilitou o surgimento de novas tecnologias aplicáveis às redes de computadores. O modelo *peer-to-peer* (P2P) quebrou o paradigma da computação cliente/servidor, pois em vez de os arquivos ficarem confinados a servidores, agora o conteúdo passou a ser distribuído e compartilhado entre membros de uma rede, sem que houvesse a dependência de uma organização central ou hierárquica [Parameswaran *et al.* 2001].

As aplicações P2P passaram a fazer parte dos ambientes domésticos, corporativos e acadêmicos. O modelo P2P tem em sua essência o compartilhamento de recursos computacionais e a troca de informação direta entre usuários. Sua característica mais distinta é a comunicação simétrica entre os *peers*, onde cada um destes pode exercer tanto o papel de cliente quanto o de servidor.

Como vantagens dos sistemas P2P podem ser citadas: a melhoria da escalabilidade, permitindo a troca direta e em tempo real de serviços e informações entre usuários; a colaboração no compartilhamento de conhecimento, agregando informações e recursos a partir dos nós que estão localizados em plataformas geograficamente distribuídas e potencialmente heterogêneas; e o aumento da disponibilidade dos serviços, eliminando a necessidade de um componente único e centralizado [Kalogeraki *et al.* 2002]. Como não possuem um ponto central de falhas, os sistemas P2P são mais resistentes a ataques de negação de serviço e oferecem maior autonomia a seus participantes, permitindo que entrem e saiam da rede de acordo com seu interesse e disponibilidade [Barcellos e Gaspary 2006].

Uma das aplicações das redes P2P é o armazenamento colaborativo de dados, onde podemos citar como exemplo: OceanStore [Kubiatowicz *et al*. 2000], FreeNet [Clarke *et al.* 2001], PAST [Druschel e Rowstron 2001] e CFS [Dabek *et al.* 2001]. Sistemas como esses devem garantir uma alta confiabilidade quanto à recuperação dos dados armazenados na rede,

devendo assim, ser toleráveis às falhas que, por ventura, poderiam comprometer permanentemente os dados de seus usuários.

É bastante oneroso tornar um sistema P2P tolerante a falhas, porém quando aplicados às redes sociais e/ou corporativas, as possíveis falhas e a complexidade são minimizadas facilitando a sua aplicabilidade [Carchiolo *et al*. 2008 e Huang *et al*. 2008]. Oliveira (2007) enumera alguns eventos que poderiam comprometer um sistema P2P de armazenamento de dados em rede, dentre elas:

- Desastres naturais: os componentes de um computador são extremamente vulneráveis à ocorrência de incidentes tais como incêndios, alagamentos, inundações e demais eventos da natureza;
- Vírus e *Worms*: Como todos os membros de uma rede P2P fazem parte de uma rede, códigos maliciosos podem ser disseminados entre os usuários, podendo causas danos tais como: consumir memória e largura de banda, danificar hardware, software ou informações armazenadas.
- Erro humano: Além do próprio usuário, pessoas próximas que utilizem sua máquina podem apagar involuntariamente dados armazenados.
- Falhas de disco: nenhuma máquina está livre de alguma falha mecânica ou elétrica que comprometa o funcionamento de seu disco rígido.
- Presença de *free riders*: o comportamento do *free-riding* é caracterizado por nós que tentam usurpar mais recursos do sistema do que efetivamente contribuem. Além disso, o *peer* pode descartar, de tempos em tempos, *backups* nele armazenados.

Os fatores acima combinados determinam a probabilidade de que uma falha ocorra durante a operacionalidade de um sistema *peer-to-peer*, entretanto esquemas de redundância de arquivos são empregados, permitindo a aplicabilidade de um sistema de armazenamento de dados em rede, como será explanado mais adiante na seção 2.3.

2.2.1 Topologias Peer-to-peer

Uma questão bastante relevante nas redes *peer-to-peer* é a escolha da topologia a ser utilizada, ou seja, o modo como os pontos comunicam-se entre si. As principais topologias utilizadas em redes *peer-to-peer* são: a Pura ou Descentralizada, a Híbrida ou Parcialmente Centralizada e a Super-peer (ver Figura 2.2), as duas primeiras apresentadas em Schollmeier

(2002) e a terceira, em Yang e Garcia-Molina (2003). A Descentralizada pode ainda ser subdividia em Não-estruturada e Estruturada.

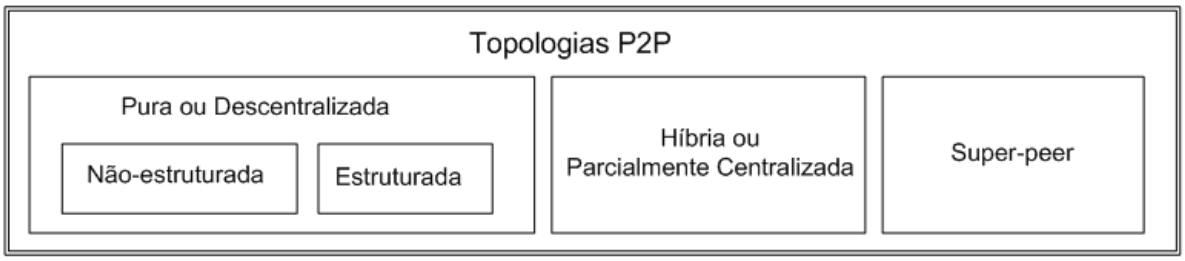

Figura 2.2. Classificação das Topologias

A topologia Pura consiste de um grande número de nós distribuídos em rede sem que haja a figura de um elemento central [Steinmetz e Wehrle 2005]. Esta topologia possui alta escalabilidade, pois qualquer nó pode adentrar e iniciar a troca de dados com os demais nós. Além disso, é mais tolerante a falhas, uma vez que a saída temporária ou permanente de um participante não causa nenhum impacto considerável ao sistema. Os sistemas de topologia Pura são classificados em Não-estruturados e Estruturados.

No modelo Não-estruturado, nenhum nó possui qualquer informação sobre a localização dos recursos que os outros pontos compartilham, por isso, normalmente, é utilizado o *flooding* como técnica de consulta de informações, acarretando no congestionamento da rede, uma vez que cada consulta recebida é repassada a todos os vizinhos. Um exemplo deste modelo de rede é o *Freenet* [Freenet 2007].

As soluções Não-estruturadas possibilitam a conexão entre nós bem estabelecidos (*super Nós*) com o intuito de obter um maior desempenho na consulta. Cabe salientar que, pela sua característica não determinística, não é possível garantir a recuperação de uma informação, uma vez que ela tenha sido publicada na rede. Isso traz grandes implicações, por exemplo, não é possível fazer a autenticação de usuário nesse tipo de rede, porque não existe garantia nenhuma de que o *login* e senha poderão ser recuperados a qualquer momento.

Por sua vez, na topologia Estruturada, os *peers* mantêm informações sobre os recursos compartilhados com os demais nós, com isso as buscas são direcionadas, empregando uma menor quantidade de mensagens, o que corrobora para um melhor desempenho.

Nos sistemas p2p Híbridos, as transferências de dados ocorrem de forma *peer-to-peer*, entretanto existe a figura de um servidor central utilizado para a troca de informações de controle, com isso, problemas de gerenciamento de sistemas são amenizados quanto comparados aos sistemas P2P com topologia pura. Na eventual indisponibilidade do servidor

central, os aplicativos existentes não são afetados e o fluxo de dados entre os nós continua independentemente de seu funcionamento, até que o servidor seja restabelecido.

Por fim, na topologia *Super-peer*, a rede existente é dividida em *clusters* gerenciados por nós com maiores capacidades computacionais (*super-peers*), conforme pode ser observado na Figura 2.3(c). No instante inicial de sua participação no sistema, cada nó é direcionado a um *super-peer* que é responsável por armazenar todo o conjunto de informações indexadas dos seus *peers* subalternos, com isso, as pesquisas realizadas são mais rápidas, pois o sistema realiza suas buscas de informações a partir de um conjunto menor de *super-peers*.

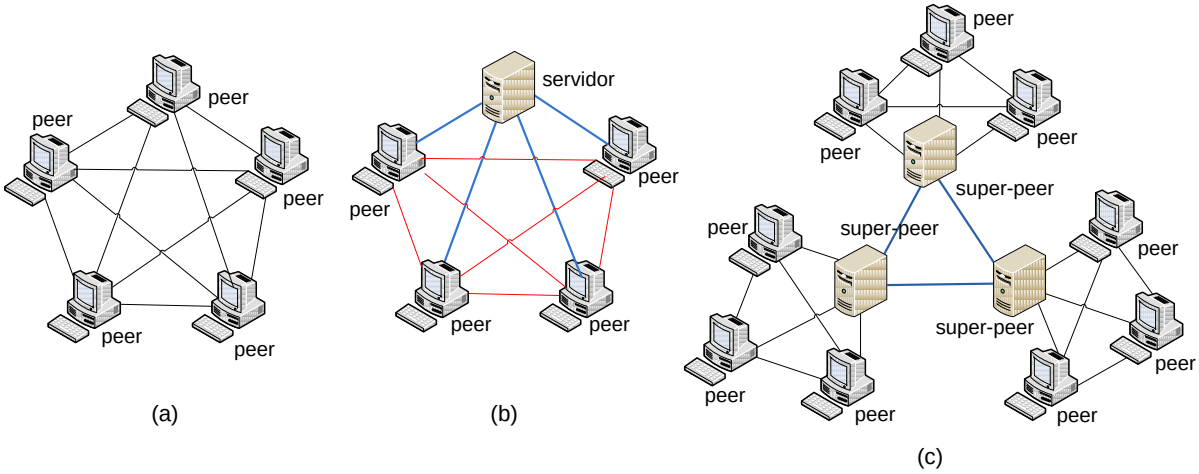

Figura 2.3. Topologias P2P. (a) Pura. (b) Híbrida. (c) Super-peer.

2.3 TÉCNICAS DE REDUNDÂNCIA DE ARQUIVOS PARA REDES P2P DE BACKUP

O arquivamento de dados em redes de computadores depende de técnicas que garantam a recuperação das informações armazenadas. Caso apenas uma cópia seja efetuada em uma máquina distinta e esta, por acaso, esteja inacessível, a recuperação do arquivo não poderá ser realizada. No desenvolvimento de sistemas de backups para redes *peer-to-peer*, um dos grandes desafios a serem vencidos é o desenvolvimento de mecanismos eficazes de controle das replicas geradas em virtude do comportamento autônomo dos *peers*, pois estes podem deixar a rede a qualquer momento, sem aviso prévio.

Em ferramentas voltadas ao compartilhamento de arquivos em redes sociais via Internet, um dos fatores mais levados em consideração é o comportamento autônomo de cada *peer*. Um nó pode deixar momentaneamente ou permanentemente a rede a qualquer momento, influenciando diretamente na recuperação de um arquivo. As saídas momentâneas podem ser frutos de uma ação voluntária do utilizador ou meramente em virtude de problemas temporários de comunicação. Além disso, há também a existência dos *free riders*, usuários

que disponibilizam inicialmente espaço livre em seu disco rígido para o armazenamento de dados de outros nós, descartando-os *a posteriori.*

A fim de contornar estes obstáculos, técnicas de redundância foram desenvolvidas para que o armazenamento dos dados em sistemas distribuídos de *backups* possa ser realizado com a confiabilidade de seus usuários. As duas principais técnicas atualmente empregadas são a *Replicação* e o *Erasure Code*, utilizados nos sistemas P2P de armazenamento.

Na *Replicação*, várias cópias de um arquivo são publicadas em diferentes pontos da rede. Esta técnica é utilizada pelos sistemas PAST [Druschel and Rowstron 2001], CFS [Dabek *et al.* 2001] e FreeNet [Clarke *et al.* 2001]. Um fator de replicação *r* determina o número de cópias e a quantidade de falhas suportadas pelo sistema. No caso do *Erasure code*, utilizado pelo OceanStore [Kubiatowicz *et al.* 2000], cada arquivo de tamanho B é fragmentado em *b* blocos e então recodificado em k·b blocos, que são disseminados em diferentes pontos da rede, onde k é o fator de expansão usado na codificação. A principal propriedade do *Erasure code* é que o arquivo original pode ser reconstruído com quaisquer b blocos dos k·b blocos codificados [Oliveira 2007].

Oliveira (2007) avaliou e constatou a viabilidade do emprego de sistemas P2P em sistemas de backup de arquivos baseando-se em dois requisitos necessários: a *confiabilidade* e a *recuperabilidade* do backup. Enquanto, a *confiabilidade* assegura a recuperação de um arquivo armazenado na rede, onde pequenos atrasos são aceitáveis caso o arquivo não possa ser acessado imediatamente, a *recuperabilidade* está relacionada à velocidade de recuperação do dado armazenado.

2.3.1 A Confiabilidade

Um sistema de armazenamento de arquivos deve garantir uma Confiabilidade (C) de recuperação dos dados armazenados. À medida que a confiabilidade no sistema aumenta, maiores são as probabilidades de que um arquivo seja recuperado quando necessário.

A avaliação de um sistema P2P de armazenamento em rede considera dois fatores: a sobrecarga de armazenamento (*k*) e a probabilidade de falhas (*f*). No caso da replicação, *k* é o número de réplicas de cada arquivo armazenado. Por sua vez, quando utilizamos o *Erasure Code*, *k* assume um valor denominado fator de expansão e surge um novo fator *b* que nada mais é do que a quantidade de blocos resultante da fragmentação do arquivo original, antes de ser armazenado na rede.

No caso da *Replicação*, a confiabilidade (C) é traduzida na expectativa de que ao menos uma das réplicas possa ser recuperada. Ou seja, seu valor é obtido através do somatório

das probabilidades de que ao menos uma cópia não falhe, de que pelo menos duas cópias não falhem, e assim por diante, até o ultimo fator, onde não haveria falha em nenhum das cópias.

Por sua vez, no *Erasure Code* para que um arquivo possa ser restaurado, devemos recuperar os *b* blocos, nos quais o dado original foi fragmentado. Cabe lembrar que é aplicado o fator de expansão *k,* determinando o número de vezes que cada bloco é replicado. Do processo de codificação existente no *Erasure Code*, a confiabilidade (*C*) na recuperação do arquivo resume-se à probabilidade de que pelo menos *b* blocos sejam recuperados. Ou seja, seu valor de *C* é obtido através do somatório das probabilidades de que ao menos *b* blocos não falhem, de que pelo menos *b+1* blocos não falhem, e assim por diante, até o ultimo fator, onde não haveria falha em nenhum dos *k*b* blocos [Oliveira 2007].

Para a análise da confiabilidade de ambas as técnicas, foram colhidas informações junto à *Ontrack Data Recovery* (2011), cujos estudos mostraram que as perdas de dados estão relacionadas a problemas de hardware ou sistema (56%), erro humano (26%), software corrompido ou problemas de programação (9%), vírus (4%) e desastres naturais (2%). Outro fator que poderia influenciar na confiabilidade do sistema é a ação dos *free riders*, entretanto em organizações que trabalham com informações sensíveis, não haveria presença de usuários que estariam entrando e saindo repentinamente da rede apenas com o intuito de prejudicar o bom funcionamento do sistema. Em simulações que levaram em consideração as falhas em virtude de problemas de hardware ou sistema, por serem consideradas os principais motivos de erros em sistemas P2P de armazenamento de dados, foram obtidos os resultados apresentados na Figura 2.4. Podemos constatar que ambas as técnicas de redundância apresentam confiabilidade aceitável para $k > 2$.

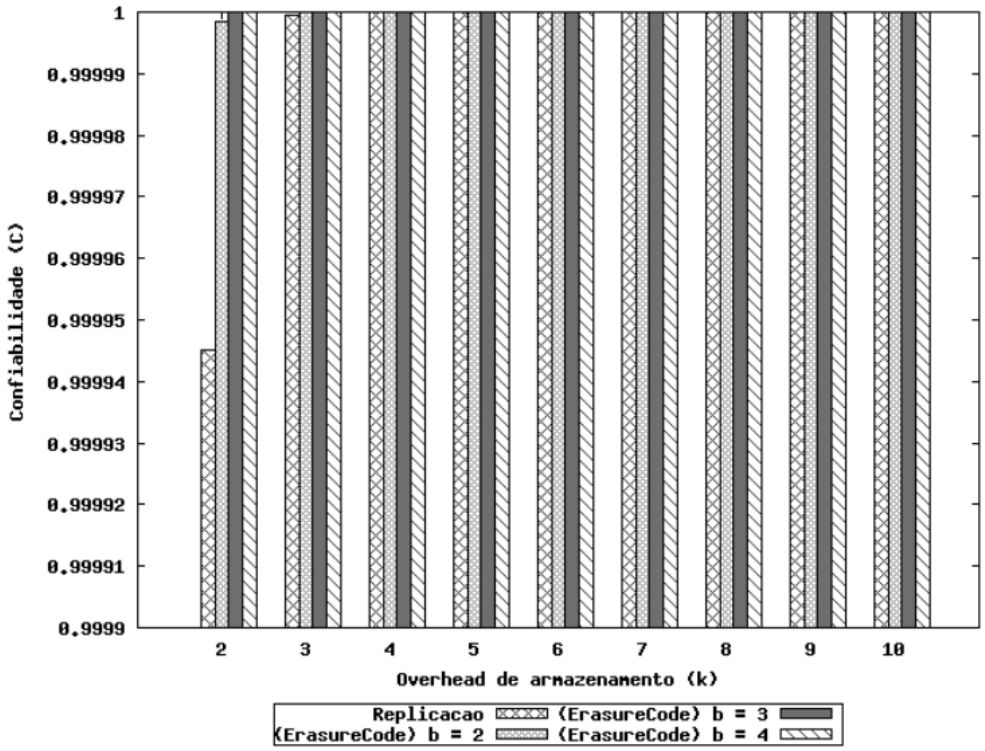

Figura 2.4. Comparação entre a confiabilidade obtida usando Replicação e *Erasure codes* diante de ocorrência de falhas de disco (f =0,0074) [Oliveiva 2007.]

2.3.2 A Recuperabilidade

A Recuperabilidade (*R*) está relacionada à velocidade de restauração de um arquivo armazenado após o surgimento de uma falha, permitindo avaliar a eficiência desse processo. O indicador mais usado nesta análise é o MTTR (*Mean Time to Repair*) ou tempo médio para reparo, cujo valor é utilizado na estimativa de tempo em que o sistema não está operacional, refletindo diretamente na sua disponibilidade [Oliveira 2007]. Nas redes *peer-to-peer* de *backup*, o MTTR é denominado como tempo de recuperação (TR) de arquivos.

O melhor tempo possível para a recuperação de um arquivo seria o resultado da divisão do seu tamanho *S* pela capacidade de *download* do *peer* que está recuperando o dado *d*. Entretanto, fatores como a quantidade de tráfego na rede e a qualidade da conexão contribuem para que o tempo de *download* de um arquivo não seja simplesmente (*S/d*). Por isso, a Recuperabilidade de um arquivo passa a ser definida como a relação entre o tempo real gasto recuperando um *backup* (TR) e o tempo ótimo de recuperação (*S/d*), refletindo assim, o quanto um sistema aproxima-se do tempo ótimo de recuperação de um arquivo (ver Eq. 2.1) [Oliveira 2007]:

$$R = \frac{(\frac{S}{d})}{TR} = \frac{s}{(TR)(d)} \quad (2.1)$$

Levando-se em consideração o fato acima exposto, simulações foram realizadas em redes P2P com intervalo de confiança de 95%, com o intuito de analisar a recuperabilidade de um sistema baseado em redes sociais. A Figura 2.5 expõe os resultados das análises de utilização das técnicas de redundância Replicação e *Erasure Code*. O valor de *R* representa a recuperabilidade obtida para diferentes valores de sobrecarga de armazenamento (*k*).

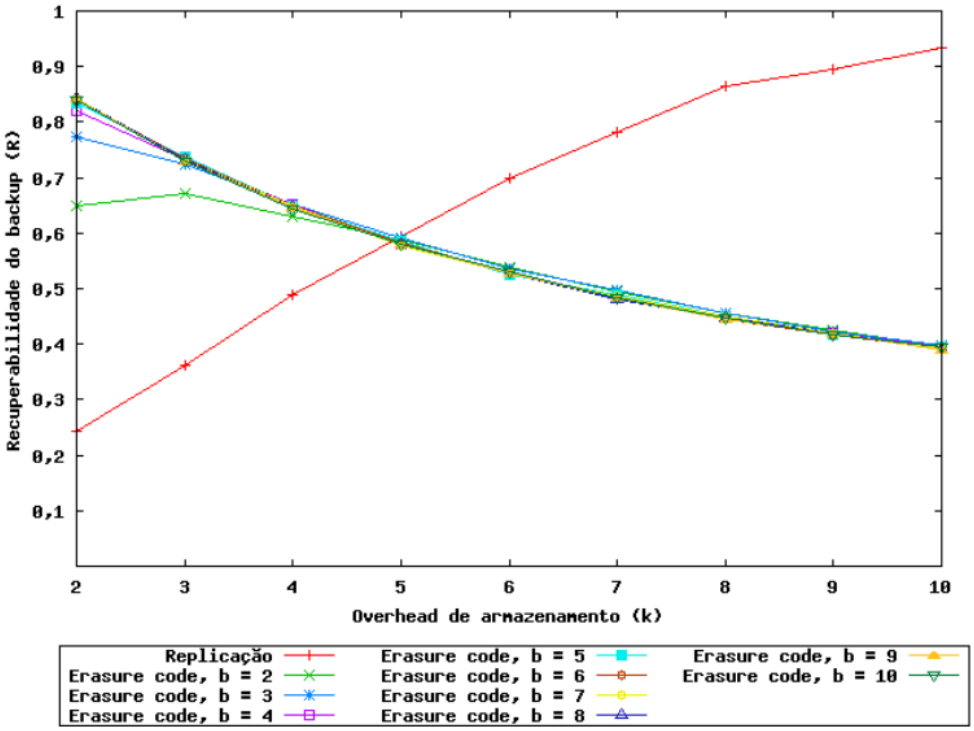

Figura 2.5. Replicação vs. *Erasure Code* [Oliveira 2007].

Na literatura, muitos estudos e comparações ente Replicação e *Erasure Code* foram realizados. Rodrigues e Liskov (2005) fizeram esta análise e concluíram que a replicação exerce melhor papel em aplicações onde a disponibilidade dos *peers* é alta, enquanto o *Erasure Code* é aplicável nos demais casos.

A escolha da técnica de redundância a ser aplicada deve levar em consideração o *tradeoff* existente entre complexidade e espaço de armazenamento utilizado, pois a replicação consome mais espaço. Os resultados demonstram que esta técnica apresenta melhor recuperabilidade para valores de k > 5.

2.4 REQUISITOS DE SEGURANÇA

Nas redes P2P, uma grande preocupação está voltada ao comportamento malicioso de algum nó. P*eers* mal-intencionados podem, por exemplo: inundar a rede com pacotes falsos, impedindo o tráfego de dados; escutar passivamente a comunicação entre dois *peers*; corromper ou simplesmente negar o acesso aos dados armazenados pelos demais usuários; ou apresentar múltiplas identidades e, assim, passar a controlar parte da rede [Chen e Jiang 2010]. Quando utilizamos uma rede P2P para o compartilhamento seguro de arquivos, devemos atender certos requisitos de segurança: confidencialidade, autenticidade, integridade, disponibilidade, autorização, reputação, negabilidade e o não-repúdio. Além disso, os aspectos explorados quanto a esses itens dependem do tipo de aplicação e do grau de segurança exigido [Barcellos e Gaspary 2006].

A Confidencialidade visa à proteção das informações armazenadas contra a divulgação a indivíduos não autorizados; a Autenticação é a comprovação da identidade de um usuário que procura acesso à rede; a Integridade tem como objetivo a garantia de que as informações armazenadas ou em trânsito não sejam modificadas por um indivíduo não autorizado; a Disponibilidade tem o intuito de que as informações, quando solicitadas, estejam disponíveis aos usuários devidamente autorizados; a Autorização consiste no fato de restringir, a partir de direitos estabelecidos, o acesso aos recursos; a Reputação é uma estimativa do grau de confiança depositado em um usuário pelos demais participantes da rede; a Negabilidade consiste em negar conhecimento sobre os arquivos guardados por uma entidade, isentando-o de responsabilidades sobre o seu armazenamento; e o *Não-repúdio* impede que uma entidade negue sua participação, ou não, em uma dada operação [Barcellos e Gaspary 2006].

Como as estações de trabalho utilizadas para o armazenamento dos fragmentos estão sob o controle dos demais membros da rede, faz-se necessário que cada bloco de um objeto, além de armazenado, também seja replicado em outras máquinas, a fim de garantir sua disponibilidade. Sem estas réplicas, a indisponibilidade de um *peer* comprometeria a recuperação do arquivo original, pois uma de suas partes estaria inacessível.

2.5 SISTEMAS DE REPUTAÇÃO

As redes *peer-to-peer* (P2P) são utilizadas em aplicações voltadas ao compartilhamento de arquivos, computação distribuída, gerenciamento de informações e *e-market*. Normalmente, o termo *peer-to-peer* está associado ao compartilhamento público de

arquivos de mídia na internet, mas outras aplicações podem fazer uso de uma infra-estrutura P2P, como por exemplo, a associação de bibliotecas para o compartilhamento do conhecimento e a realização de *backups* de seus conteúdos contra possíveis perdas.

Como característica dessas redes, cada *peer* pode adentrar e sair freqüentemente sem causar nenhum dano ao funcionamento de sua infra-estrutura. Por esta razão, um dos grandes desafios em sistemas P2P é a capacidade de gerenciar os riscos envolvidos na interação e colaboração entre os seus participantes, muitas das vezes desconhecidos e potencialmente danosos [Wu e Wu 2009]. A fim de avaliar o quão confiável pode ser um ponto na rede, nasceu a concepção dos Sistemas de Reputação como tentativa de prevenção a comportamentos maliciosos e com o intuito de estimular a colaboração entre usuários confiáveis.

À medida que os *peers* relacionam-se entre si, suas interações são constantemente avaliadas por alguma entidade e/ou pelos demais nós. Este conhecimento colhido e compartilhado com os demais pontos da rede serve de embasamento para a construção da reputação de um *peer*. Segundo Marti e Garcia-Molina (2006), os mecanismos de reputação têm três fases principais: a *Coleta de Informações* desde o momento em que um nó passa a pertencer à rede; *Pontuação e Ranqueamento*, baseado nas experiências e comportamentos observados pelos demais *peers*; e *a Resposta* da rede que pode, por exemplo, selecionar um conjunto de nós confiáveis para a execução de um dado serviço ou levar à exclusão de nós considerados maliciosos.

A principal estratégia utilizada em sistemas P2P é a cooperação dos recursos disponíveis em cada nó. Individualmente, não há benefício algum para um *peer* colaborar com outros nós que não cooperam. Quando um nó A recebe uma solicitação por um nó B, pode haver uma maior predisposição em sua colaboração, se há algum indício de que B atenda a um futuro pedido de A. Ou seja, os pontos da rede tendem a cooperar à medida que a confiança entre eles aumenta. Este grau de confiabilidade apresentado por um *peer* é denominado Reputação.

A Reputação de cada *peer* é realizada a partir de suas interações com os demais. Para isso, tornam-se necessárias duas ações: armazenar as informações relativas à reputação e compartilhá-las com os demais pontos da rede, pois semelhante a uma sociedade, os *peers* individualmente podem tomar decisões sobre a confiabilidade dos outros membros da comunidade com base em suas próprias experiências passadas ou nas recomendações de colegas confiáveis [Novotny e Zavoral 2008].

Quanto ao armazenamento das informações relativas à reputação, existem quatro principais abordagens: (i) No *armazenamento centralizado*, as informações sobre a reputação são armazenadas em um servidor central. Apesar de facilitar o gerenciamento das informações, esta abordagem apresenta um ponto central suscetível a falhas; (ii) No *armazenamento distribuído*, as informações sobre a reputação são armazenadas em certos pontos da rede. Entretanto, a maioria dos modelos não considera a possível heterogeneidade dos *peers* de armazenamento e o fato de que informações sobre *peers* com alta reputação podem estar armazenadas em *peers* com baixa reputação ou com comportamento mal-intencionado ainda não detectado. Além disso, em operações de grande escala, esta abordagem pode sobrecarregar a rede; (iii) No *Rater-Based Storage*, os *peers* apenas armazenam as informações de reputação de outros nós com quem interagem. Esta abordagem diminui a possibilidade de adulterações das avaliações realizadas, pois os *peers* não trocam informações sobre reputação e as avaliam individualmente; e (iv) No *Ratee-Based Storage*, cada *peer* armazena sua própria reputação resultante de suas ações. Os demais nós consultam a reputação de cada *peer*, entretanto é notório que um *peer* mal-intencionado pode manipular sua própria reputação [Wu e Wu 2009].

Quanto ao compartilhamento das informações e cálculo final da reputação dos *peers*, podem ser seguidas as seguintes abordagens: (i) Na Ação Local (*local share*), cada nó individualmente gerencia as informações coletadas por si. A sobrecarga na rede é reduzida, mas aumenta a probabilidade de falha de interações com novos *peers*; (ii) No Compartilhamento Parcial (*Part Share*), cada *peer* compartilha informações sobre reputação com alguns *peers* específicos, tais como conhecidos e vizinhos. Estes *peers* podem periodicamente realizar o intercâmbio de informações numa freqüência que pode ser ajustada, a fim de controlar a sobrecarga de troca de mensagens da rede; e (iii) Na Participação Global (*Global Share*), pressupõe-se a existência de um mecanismo de coleta de informações, com o intuito de compartilhá-las com todos os integrantes da rede. As informações sobre reputação são calculadas, atualizadas e armazenadas em alguns *peers* (*storage peers*). Entretanto, à medida que a rede cresce, as trocas de mensagens aumentam, podendo sobrecarregar o sistema [Wu e Wu 2009].

2.6 A CRIPTOGRAFIA

A criptografia é uma das técnicas de codificação mais utilizadas em aplicações voltadas à garantia do sigilo de informações e à comunicação segura entre dois indivíduos.

Com o seu uso, dados podem ser armazenados, enviados e recuperados sem que haja exposição ou alteração do seu conteúdo. O termo Criptografia tem origem grega como resultado da união das palavras *Kruptós* que significa “escondido” e *grápho* que significa “escrita”.

A criptografia consiste em transformar um *texto claro* (conjunto de informações coerentes) em um *texto cifrado* (conjunto de caracteres relacionados de forma totalmente desconexa), ocultando suas informações originais. Esta transformação pode ser realizada utilizando *códigos* ou *cifras*. No uso de *códigos*, a mensagem a ser compartilhada entre duas partes é modificada através de termos pré-definidos. A técnica do uso de *cifras* envolve a codificação da informação por intermédio de um algoritmo associado a uma *chave* (conjunto de bits).

Em relação ao uso de chaves, quando a mesma chave é utilizada tanto para a cifragem quanto para a decifragem da mensagem, está sendo empregada a *criptografia por chave simétrica ou secreta*. Quando chaves diferentes são empregadas nos processos, está sendo empregada a *criptografia por chaves assimétricas ou de chave pública*.

2.6.1 Criptografia por Chave Simétrica ou Secreta

Como dito anteriormente, nesta técnica, o Remetente e o Destinatário devem compartilhar e manter em segredo a mesma chave que é utilizada nos processos de cifragem e decifragem. Esta sistemática é exemplificada na Figura 2.6.

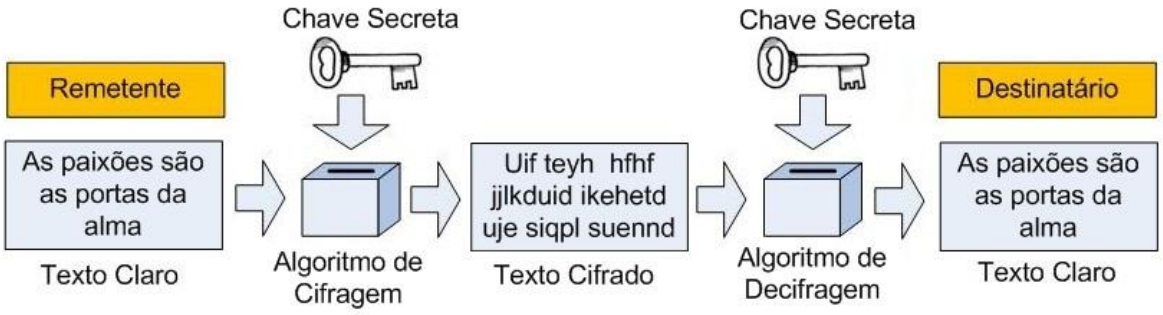

Figura 2.6. Esquema de Criptografia por Chave Simétrica.

Como exemplo de algoritmos de chave simétrica, podemos citar: o *DES, o 3-DES, o IDEA (International Data Encryption Algorithm) e o AES (Advanced Encryption Standard). O DES* (*Data Encription Standard)* baseado no algoritmo *Lucifer* desenvolvido pela IBM, é utilizado pelo governo americano desde 1978. O DES utiliza cifras de blocos de 64 bits com uma chave de 56 bits. Tem como variação o *triplo-DES* (3-DES) que faz três aplicações seguidas do DES. O *IDEA* é um algoritmo de origem suíça, publicado em 1960, cuja chave de

128 bits impossibilita a sua quebra computacional por ataques de força bruta [Trinta e Macêdo 2008]. Este tipo de ataque consiste em percorrer a lista das possíveis chaves utilizando um algoritmo de busca com o objetivo de encontra a chave secreta. Por último, o AES é um dos algoritmos mais utilizados, em função de sua rapidez de execução tanto em *software* quanto em *hardware*. Atualmente, é o padrão de criptografia adotado pelo governo dos Estados Unidos.

2.6.2 Criptografia por Chaves Assimétricas ou Chave Pública

No caso da criptografia por chaves assimétricas, é utilizado um par de chaves denominadas chave pública (Pub_A) e chave privada (Pri_A) nos processos de cifragem e decifragem da informação. A chave pública de um indivíduo deve ser amplamente divulgada, pois esta chave é a utilizada pelo remetente no processo de cifragem e apenas o destinatário, por possuir sua chave privada correspondente, é capaz de decifrar o conteúdo da mensagem. A chave privada deve ser mantida em sigilo e de posse do destinatário a fim de evitar que outro indivíduo possa ter acesso às mensagens enviadas. Este processo é exemplificado na Figura 2.7.

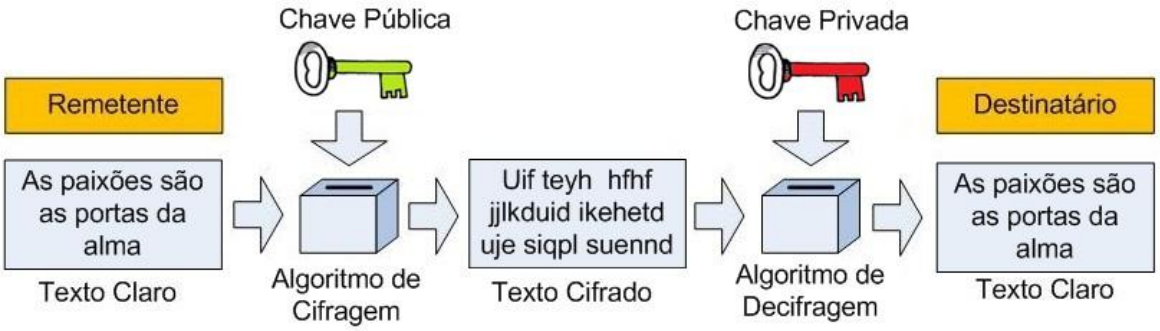

Figura 2.7. Esquema de Criptografia por Chave Assimétrica.

Como exemplo de algoritmos de chaves assimétricas, podemos citar: o *Diffie-Hellman* [Diffie e Hellman 1976], ponto de partida para a criptografia por chave pública, é um algoritmo onde cada participante inicia com sua chave secreta e através da troca de informações é derivada outra chave denominada chave de sessão, que será usada para futuras comunicações. O algoritmo *RSA* que deve seu nome aos professores Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman (*Massachusetts Institute of Technology*) é um dos mais seguros e seu princípio baseia-se na complexidade da manipulação de números primos extensos, sendo o primeiro algoritmo a possibilitar a assinatura digital [Trinta e Macêdo 2008].

2.6.3 Assinaturas Digitais

No processo de assinatura digital de um arquivo, inicialmente aplicamos uma função matemática, denominada *função Message Digest*, que mapeia a seqüência de bits de todo o documento digital produzindo um *hash*, uma seqüência de bits de tamanho fixo e menor. É praticamente impossível dois arquivos com conteúdo distintos produzirem o mesmo *hash*. Dessa forma, o remetente (R) ao produzir um *hash* possibilita ao destinatário (D) verificar a integridade do conteúdo enviado aplicando a mesma *função Message Digest (MD)* ao arquivo recebido e fazendo uma comparação com o *hash* recebido.

Para o envio de um arquivo assinado digitalmente, primeiramente o remetente aplica uma função *Message Digest* extraindo o *hash* do arquivo e o criptografa utilizando sua chave privada. O *hash* permite a verificação da integridade, enquanto a criptografia do arquivo com a sua chave privada garante a autenticidade do remetente.

Na recepção, o destinatário gera outro *hash* do arquivo recebido e procede a comparação com o *hash* enviado R decifrado com a chave pública do remetente. Este esquema pode ser observado na Figura 2. 8, onde é utilizado algoritmo de chave pública RSA, como exemplo.

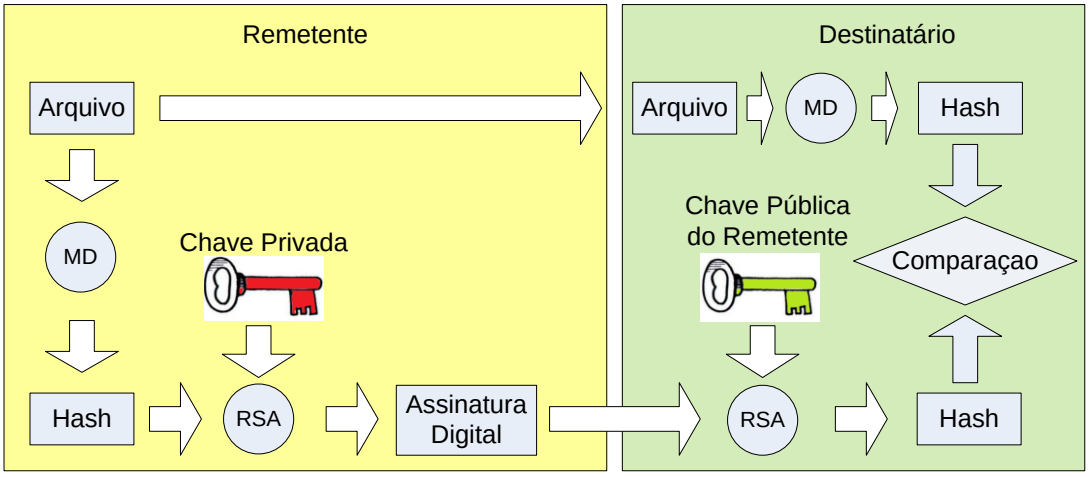

Figura 2. 8. Esquema de Assinatura Digital.

Quanto à criptografia, os algoritmos simétricos são mais simples do que os de chave assimétrica, pelo fato dos simétricos utilizarem a mesma chave para criptografar e descriptografar dados. Em virtude disso, o processo simétrico é mais rápido, apresentando melhor desempenho quando é necessária a criptografia de um grande volume de dados. Entretanto, apesar da criptografia simétrica ser mais rápida, o uso da mesma chave por todos os indivíduos que enviam e recebem cria um problema de segurança envolvendo a geração, a distribuição, o backup e ciclo de vida da chave.

Na criptografia assimétrica, uma chave privada é mantida de posse de cada usuário e a outra chave é pública. As informações criptografadas com uma chave só pode ser descriptografada pela outra, pois ambas são matematicamente relacionadas. Por isso, os algoritmos assimétricos são mais lentos. Entretanto, o uso de um par de chaves garante o não-repúdio, ou seja, o emissor de uma mensagem não poderá posteriormente negar sua autoria.

2.7 CONSIDERAÇÕES SOBRE O MODELO ADOTADO

Os conceitos básicos estudados neste capítulo serviram para encontrar as soluções existentes mais adequadas relacionadas à topologia, à técnica de redundância e ao esquema de criptografia para uma futura concretização desta proposta.

Um dos propósitos desta dissertação é demonstrar a aplicabilidade de um sistema seguro de armazenamento de arquivos em uma rede organizacional denominada *Rede de Confiança*. A rede construída por integrantes de uma organização é, na verdade, um caso particular de uma rede social onde a taxa de abandono é muito baixa, uma vez que os *peers* apenas deixam de pertencer à rede ao saírem definitivamente da organização. Além disso, a grande maioria normalmente está conectada no mesmo horário de trabalho, o que aumenta ainda mais as chances de recuperabilidade dos dados armazenados.

Quanto à topologia, uma estrutura P2P Híbrida mostrou-se mais adequada no propósito de minimizarmos os problemas de gerenciamento dos usuários. Além disso, esta proposta pode ser utilizada em organizações cuja estrutura já possui a figura de um servidor central, cabendo apenas a implantação de um servidor redundante a fim de evitar a existência de um ponto único de falhas em cada organização.

Outro ponto importante foi o estudo de mecanismos de redundância, cujo objetivo era encontrar a técnica mais adequada em função de sua implementação. Assim, com o intuito de simplificarmos esta etapa, decidimos por optar pela técnica de replicação. Cada arquivo é fragmentado ao ser armazenado na rede e esses fragmentos são replicados a fim de aumentar as chances de recuperação das informações.

A fim de manter a confidencialidade dos dados, será utilizada uma sistemática de criptografia híbrida utilizando algoritmos de chave simétrica e assimétrica. Para a codificação de cada arquivo, a aplicação cria uma chave simétrica e única, por ser uma criptografia mais rápida. O emprego da criptografia assimétrica é voltado apenas à codificação da chave simétrica gerada anteriormente. Além disso, nos algoritmos de chave assimétrica, um arquivo

apenas pode ser decifrado pelo indivíduo que divulgou sua chave pública, uma vez que somente ele possui a *chave privada* necessária para a decodificação.

Por fim, com o intuito de analisarmos a confiabilidade das estações de trabalho dos usuários, avaliando se o *peer* que solicita acesso ao dado armazenado na rede possui reputação compatível com o grau de sigilo atribuído à informação, propomos, no capítulo 5, a utilização de um mecanismo de reputação. O armazenamento da reputação é distribuído, pois cada *peer* armazena o resultado de suas interações com cada um dos nós com quem interagiu anteriormente. Além disso, quando um nó A interage com outro nó B e a reputação B é modificada, este novo valor pode ser distribuído por A aos demais nós com quem A já interagiu no passado. Dessa forma, os *peers* constroem uma reputação global dos demais pontos da rede, mesmo que não haja nenhum histórico de interação direta. Detalhes do mecanismo de reputação proposto serão expostos na Seção 5.3.

Capítulo 3 – Trabalhos Relacionados

Neste capítulo é apresentada a pesquisa literária sobre soluções voltadas ao compartilhamento de recursos em redes *peer-to-peer*. Além disso, é introduzido o conceito de sistemas de reputação, mecanismos utilizados para avaliar a confiabilidade das entidades presentes em uma rede.

Ao final do capítulo, são feitas considerações com a apresentação de uma infra-estrutura para o compartilhamento seguro de informações sigilosas.

3.1 COMPARTILHAMENTO DE RECURSOS EM REDES P2P

Vários trabalhos propõem soluções voltadas à segurança em questões relacionadas ao compartilhamento de recursos e arquivos em redes. Por exemplo, o *Freenet* é um aplicativo que funciona como uma rede *peer-to-peer* adaptativa onde a publicação, replicação e recuperação de arquivos protegem o anonimato de seus autores e leitores. Sua implementação visa à disponibilidade e à confiabilidade no armazenamento dos dados e roteamento de mensagens. Outra característica presente, é tornar inviável a descoberta da origem e destino de um pacote que transita na rede, além de isentar um nó sobre a responsabilidade do conteúdo por ele armazenado [Clarke *et al.* 2001 apud Barcellos e Gaspary 2006]. Entretanto, o *FreeNet* não garante a preservação de todos os documentos, pois os mesmos são armazenados em função do número de acessos recentes, podendo ser eventualmente descartados em razão de sua obsolescência.

O TOR [Dingledine *et al.* 2004] também é um sistema de armazenamento de arquivos voltado ao anonimato do emissor e do receptor, além de não permitir a vinculação entre esses dois agentes. Após uma primeira versão em Goldschlag *et al.* (1999), a segunda trouxe uma série de melhorias. Seu princípio de funcionamento está na aplicação de criptografia em camadas nos pacotes que trafegam na rede. Por ocasião do envio de dados entre dois *peers*, é feita uma consulta a um servidor de diretórios onde um circuito é escolhido com base em uma lista de roteadores (*Onion Routers*).

O *Free Haven* [Free Haven 2010] é uma rede de armazenamento distribuído de dados que provê o anonimato de todos os agentes envolvidos. Os servidores pertencentes à rede estabelecem relações de confiança entre si, em virtude da observação, ou não, de comportamentos considerados maliciosos. A partir disso, objetos passam a ser transferidos dinamicamente entre eles com o intuito de ocultar a identidade do nó que publicou um arquivo.

O *OceanStore* [OceanStore 2010] é um sistema de armazenamento de dados que possibilita a presença de milhões de participantes. O usuário inscreve-se em um único provedor *OceanStore* e passa a usufruir da capacidade de armazenamento e largura de banda dos demais provedores pertencentes à rede. Cada versão de um objeto é armazenada de forma permanente, acessível somente para leitura, sendo espalhada por um grande número de servidores utilizando o esquema de redundância *erasure code*. Nesta técnica, cada arquivo de tamanho B é fragmentado em *b* blocos e então recodificado em k·b blocos, que são

disseminados em diferentes pontos da rede, onde k é o fator de expansão usado na codificação.

O *OurBackup* [Oliveira 2007] aborda uma proposta que utiliza o espaço disponível no disco rígido de computadores pertencentes a uma rede *peer-to-peer* (P2P) para realizar *backups*. Como nos sistemas P2P tradicionais a taxa de abandono exige uma grande quantidade de banda necessária para manter a redundância dos backups, o autor propõe um sistema P2P baseado em redes sociais, pois a grande maioria dos participantes tende a permanecer na rede.

Filho (2010) desenvolveu o SAS-P2P como um serviço a ser oferecido à rede GigaNatal [GigaNatal 2010] que disponibiliza serviços básicos das redes Metro-ethernet, interligando instituições de ensino e pesquisa da cidade. O SAS-P2P disponibiliza uma área de armazenamento compartilhada, onde os dados são guardados em arquivos padronizados no formato XML.

3.2 SISTEMAS DE REPUTAÇÃO

Nos sistemas P2P, muitas vezes, usuários mal-intencionados tentam desobedecer às políticas e normas de conduta estabelecidas, por exemplo, não compartilhando recursos sobre sua responsabilidade, ou recusando-se a avaliar interações com os demais participantes. Por isso, surgiu a necessidade da criação de Sistemas de Reputação capazes de avaliar a confiabilidade dos *peers* com objetivo de diminuir a incidência de comportamentos maliciosos que poderiam levar ao colapso da rede.

Essa preocupação existe há mais tempo, por exemplo, o EigenTrust [Kamvar et al. 2003] é um sistema voltado para redes de compartilhamento de arquivos P2P cujo objetivo é calcular a reputação de um *peer* com base em seu histórico de interações, atribuindo uma reputação global e única em função do seu histórico de *uploads*. Os *peers* usam os valores de reputação global para escolher quais os pares mais confiáveis para realizar o *download* de um arquivo. Além disso, os valores globais de reputação são usados com o intuito de identificar e prover o isolamento de nós que não contribuem com a rede. Este valor global atribuído a um peer *i* é ponderado pelo peso da reputação de cada um dos *peers* que fazem sua avaliação.

Conforme Barcellos e Gaspary (2006), o *PeerTrust* é um framework que inclui um modelo de confiança adaptativa com o objetivo de quantificar e comparar a confiabilidade dos *peers*, com base em um sistema de transações com *feedbacks*. O modelo define três parâmetros básicos de confiança, dois fatores adaptativos usados no cômputo do grau de

confiança em um *peer* e a definição de uma métrica geral de confiança para combinar esses parâmetros. O modelo de reputação usa a avaliação das interações mais recentes para cálculo da confiança. Os dados necessários para o cálculo da confiança entre os *peers* são armazenados de maneira distribuída. Cada nó possui *um gerenciador de confiança*, que é responsável pela submissão de *feedback* e avaliação da confiança através de um banco de dados com um segmento da base global, e um *localizador* para a alocação e localização dos dados de confiança na rede.

Por sua vez, o PowerTrust [Zhou e Hwang 2007] é um mecanismo de reputação escalável para redes P2P baseado no sistema de *feedbacks* dos usuários. Os autores fizeram vários experimentos sobre um conjunto de dados extraídos das transações no site de comércio eletrônico *eBay* e concluíram que as avaliações realizadas seguem uma lei de potência. Ainda mais, eles demonstram que esta lei de potência é aplicável a qualquer sistema de reputação P2P. A lei de potência rege que é comum haver *peers* com alguns *feedbacks*, entretanto *peers* com um grande número de *feedbacks* são extremamente raros. A partir dessa característica, através do uso de um mecanismo distribuído de pontuação, os *peers* mais confiáveis são dinamicamente selecionados.

O trabalho de Tran *et al*. (2005) apresenta um *framework* para o compartilhamento de arquivos P2P que integra um modelo de confiança, onde *peers* classificam os demais usuários e atribuem diferentes direitos de acessos aos documentos armazenados na rede em função de sua atual reputação. A reputação é um cálculo global do histórico das interações baseadas em dois aspectos: velocidade de download e a qualidade de arquivo. Uma interação é considerada satisfatória e, conseqüentemente, a reputação do *peer* é incrementada se a velocidade de download é maior que um *threshold* estipulado e o arquivo é avaliado positivamente pelo usuário que o requisitou.

3.3 CONSIDERAÇÕES FINAIS

Podemos observar que há, na literatura, várias soluções distintas voltadas ao compartilhamento e/ou armazenamento seguro de dados e na análise da reputação das entidades existentes em uma rede. A pesquisa realizada serviu para encontrar os alicerces necessários à fundamentação da proposta da dissertação. A seguir destacamos algumas comparações com os trabalhos anteriormente citados neste capítulo.

Diferente do *FreeNet*, onde os arquivos poder ser eventualmente descartados devido a sua obsolescência, na Rede de Confiança a garantia da preservação de um arquivo é fundamental, uma vez que documentos sigilosos não podem ser simplesmente perdidos.

Com relação à técnica de redundância de arquivos, enquanto o *OceanStore* emprega o *erasure code*, a Rede de Confiança utiliza a *replicação* para fazer cópias dos fragmentos pertencentes a um arquivo. Ou seja, se um arquivo é dividido em cinco partes, cada uma delas será replicada *k* vezes e distribuídas em diferentes locais da rede.

Semelhante ao *OurBackup*, o espaço ocioso nos discos rígidos das máquinas pertencentes à rede também compartilhado, entretanto os objetos não são integralmente gravados em um local. Por ocasião do armazenamento, cada arquivo é divido em vários blocos que são criptografados e distribuídos pela rede. Quando há a necessidade de obter acesso ao arquivo original, os fragmentos são reagrupados.

A abordagem presente na Rede de Confiança criptografa os arquivos antes de armazená-lo na rede, de maneira análoga ao SAS-PSP, entretanto aplicamos uma segunda "camada" de segurança, fragmentando e armazenando as partes constituintes de um mesmo arquivo em diferentes locais geográficos, de tal maneira que nenhum dos computadores da rede possua uma versão integral de um arquivo.

Com relação ao sistema de reputação, de maneira semelhante ao *Free Haven*, o presente trabalho também prevê a utilização de uma sistemática capaz atribuir *status* de reputação às estações de trabalho (*peers*), de modo que os arquivos apenas sejam acessados por *peers* considerados confiáveis. Além disso, em nossa abordagem não há a troca dinâmica de objetos entre os pontos da rede, diminuído assim o tráfego de mensagens.

A principal diferença em relação ao trabalho de Tran *et al*. (2005) é o fato de que enquanto sua metodologia incrementa a reputação à medida que as interações bem sucedidas acontecem, nessa dissertação, partindo-se da premissa que os usuários são considerados confiáveis ao serem autorizados a participarem da Rede de Confiança, sua reputação é penalizada à medida que comportamentos maliciosos são detectados.

A partir do exposto até aqui, será apresentada uma infra-estrutura P2P denominada *Rede de Confiança*, capaz de permitir o compartilhamento e sobrevivência de informações sigilosas de uma organização. Um esquema híbrido, utilizando a criptografia simétrica e a assimétrica, permite o controle de acesso aos arquivos. Além disso, os arquivos são fragmentados e armazenados em máquinas distintas, de tal modo que nenhuma delas possua uma cópia integral de um documento. E por fim, propomos a utilização de um sistema de

reputação que verifica a compatibilidade entre a reputação do *peer* que solicita acesso ao dado armazenado e o grau de sigilo atribuído à informação.

Capítulo 4 – Uma Política de Segurança para o Armazenamento de Informações Sigilosas

Neste capítulo, apresentamos uma visão geral do funcionamento de uma rede voltada à sobrevivência de informações sigilosas. Esta sobrevivência é caracterizada pela distribuição das informações por uma *Rede de Confiança* formada por instituições localizadas em pontos geograficamente distintos, permitindo que os dados confidenciais não sejam perdidos, caso uma das sedes das organizações seja comprometida de alguma forma, quer seja por desastre natural ou em função de alguma ofensiva por forças inimigas, por exemplo.

Instituições que tratam de informações sigilosas tendem a criar fortes defesas físicas e digitais aos dados sob a sua guarda. Normalmente, este modelo traz o benefício de, ao concentrarmos as informações em um só lugar, podermos empregar nossos esforços na implantação de barreiras que vedem o acesso por indivíduos estranhos. Por outro lado, ao ser descoberta a localização desses dados, o adversário pode concentrar suas forças em ataques cada vez mais poderosos, a fim vencer os obstáculos e obter acesso aos dados ou simplesmente torná-los inacessíveis aos seus devidos utilizadores.

Outra questão a ser abordada é o fato de que, caso algum dano seja causado às instalações em virtude de uma ofensiva adversária ou em razão de algum desastre natural, os dados armazenados neste local serão perdidos ou danificados com uma remota chance de recuperação. Se as informações estiverem guardadas em mais de um local, a chance de que os dados sobrevivam às medidas ofensivas e catástrofes aumentam consideravelmente.

Em alguns setores, tais como as Forças Armadas, Órgão do Governo e Organizações de Inteligência, há informações armazenadas que podem colocar em risco inclusive a segurança nacional. Segredos de Estado, conhecimento sobre sistemas de armas, identidades de agentes e informantes podem estar digitalmente arquivados de forma segura em uma construção destinada à salvaguarda deste conhecimento, entretanto danos às suas instalações poderiam levar à perda destes dados sigilosos.

A utilização da Computação em Nuvem [Armbrust *et al.* 2009] seria uma boa alternativa para o arquivamento dos dados de uma empresa. Entretanto, organizações que trabalham com informações sigilosas não podem arquivá-las em *Data Centers* (locais onde estão localizadas as infra-estruturas dos provedores de serviços), onde a única garantia de que os dados não são acessados por terceiros são os *Acordos de Nível de Serviço* celebrados entre as partes. A quebra do sigilo é inaceitável.

Até agora, abordamos apenas o comprometimento em massa das informações de uma organização. Entretanto, cada usuário está passível de ter sua estação de trabalho violada, quer seja pela instalação de algum software, quer pela utilização indevida de sua máquina por outro indivíduo. Caso haja um acesso mal-intencionado ao seu computador, seus dados e documentos podem ser copiados na integra e o conteúdo do arquivo sigiloso seria revelado, algo que não aconteceria se nenhuma máquina possuísse uma versão completa de um documento sensível.

Uma solução que dificulta o acesso a dados sigiloso é a construção de uma *Rede de Confiança* formada pelos membros de uma organização. Antes de ser armazenado nesta rede, o arquivo é dividido em partes criptografadas, a serem guardadas em usuários diferentes.

Quando houver a necessidade de acesso ao documento, as partes são novamente reunidas e o arquivo original é recomposto (ver Figura 4.1).

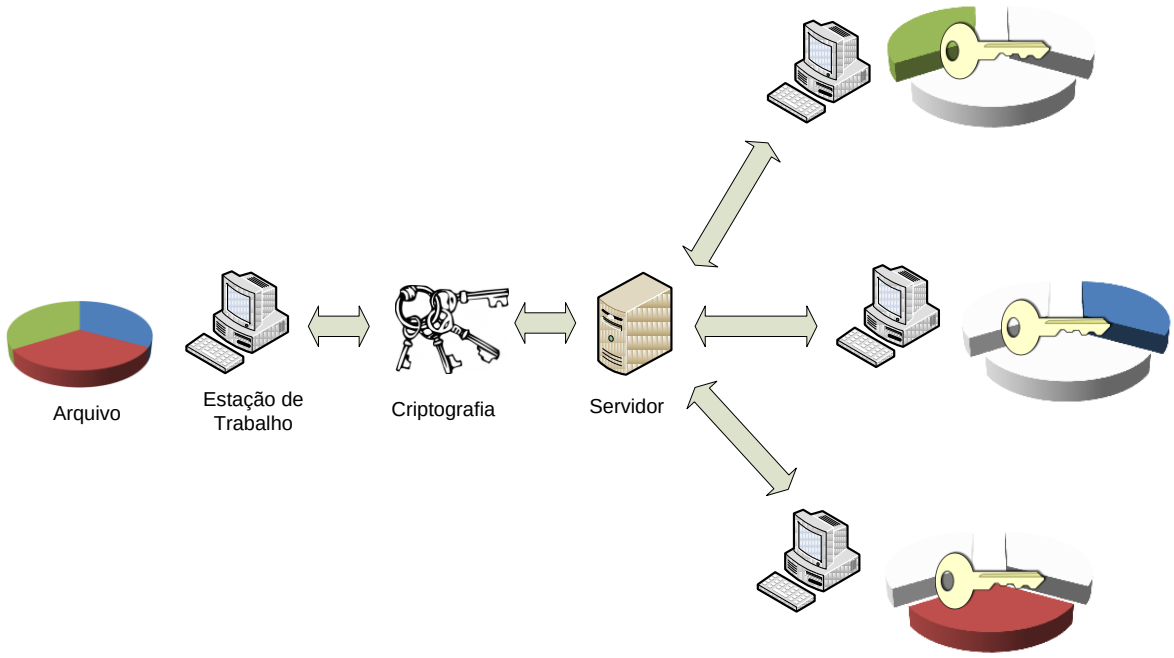

Figura 4.1. Fragmentação do arquivo.

4.1 SERVIDORES E AGENTES

A arquitetura envolvida na política de segurança utiliza os recursos disponíveis em uma rede *peer-to-peer* e traz alguns traços do protocolo *BitTorrent* [BitTorrent 2010]. Por adequação, este trabalho descartou algumas de suas características originais. O *BitTorrent* permite que várias cópias integrais de um mesmo arquivo sejam arquivadas por diferentes usuários, entretanto, a presente proposta desmembra um arquivo em várias partes, espalhando-as pela rede para que sejam utilizadas apenas quando uma versão integral do documento for solicitada. Diferente do *BitTorrent*, nenhum usuário possuirá uma versão integral do documento.

A macro-arquitetura é composta por servidores e usuários (*peers*), como pode ser visto na Figura 4.2. Os servidores são responsáveis por gerenciar os usuários, sendo utilizados nos processos de criação, atualização, remoção e consultas de usuários.

Cada terminal *peer* pode exercer dois distintos papéis: o *Leech* (sanguessuga) é o terminal que está executando uma tarefa de recuperação ou armazenamento de um arquivo na rede e o *Seed* (semente) é a denominação dada a cada terminal onde estão armazenadas as partes integrantes de um mesmo arquivo. O conjunto de máquinas que compartilham os

fragmentos de um mesmo arquivo recebe a denominação *Swarm*. Cada *peer* aloca espaço do seu disco rígido para que seja utilizado no armazenamento de dados dos demais usuários.

Além disso, há também a existência dos *trackers*, armazenados nos servidores, que são os elementos gerenciadores de conexões, que contém as informações necessárias sobre a localização das partes integrantes de um arquivo armazenado na rede.

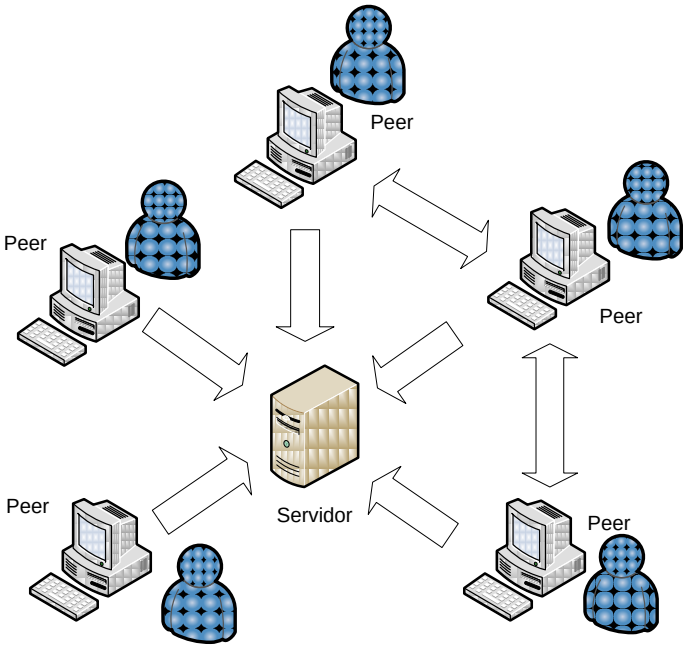

Figura 4.2 Macro-arquitetura da Rede de Confiança.

4.2 A FRAGMENTAÇÃO DOS ARQUIVOS SIGILOSOS

A Rede de Confiança é composta pelas máquinas dos usuários pertencentes ao sistema. Dentro de uma organização podem existir assuntos diferentes com níveis de segurança distintos; por exemplo, há instituições onde os assuntos são classificados, de acordo com o seu grau de sigilo, em ostensivos, reservados, confidenciais, secretos e ultra-secretos.

Os assuntos *ostensivos* são aqueles a que qualquer indivíduo pode ter acesso. Os *reservados* são aqueles que não devem ser de conhecimento geral. Os *confidenciais* são assuntos cuja divulgação não autorizada afeta a segurança da instituição. Os *secretos*, normalmente, são arquivos que contêm informações sensíveis da própria organização ou cuja divulgação pode colocar em perigo a ordem pública. E por fim, os *ultra-secretos* estão destinados a proteger informações de grande importância nacional. Dessa forma, teríamos cinco níveis de sigilo: *ostensivo, reservado, confidencial, secreto e ultra-secreto*.

Guardar documentos em uma máquina pode ocasionar a divulgação de informações importantes, caso este computador seja violado por algum indivíduo malicioso. Para proporcionarmos maior segurança, um arquivo sigiloso é criptografado e dividido em fragmentos armazenados em usuários (*peers*) distintos. Ou seja, para que o conteúdo de um arquivo seja copiado e acessado indevidamente, seria necessária a invasão de várias máquinas para reunir os fragmentos do arquivo, além do conhecimento das chaves utilizadas no processo de criptografia, algo extremamente trabalhoso.

A presente proposta visa demonstrar a aplicabilidade da *Rede de Confiança* formada pelos indivíduos de uma organização. Seu funcionamento parte da premissa de que seus arquivos são classificados em função do sigilo em cinco níveis sigilosos ou restritos, a saber: *ostensivo, reservado, confidencial, secreto e ultra-secreto*.

As estações de trabalho cedem um espaço definido em seus discos para o armazenamento dos arquivos dos demais membros da rede. Além disso, as máquinas são monitoradas por um sistema de reputação com o intuito de permitir, ou não, o acesso a um determinado documento em função do grau de sigilo atribuído a um arquivo e do nível de confiança apresentado pelo usuário (*peer*).

Os documentos com grau de sigilo ostensivo, como seu conteúdo pode ser conhecido por todos, podem ser armazenados integralmente na máquina do próprio usuário. Entretanto, de acordo com o exposto anteriormente, arquivos com grau de sigilo igual ou superior ao de *reservado* cujo usuário opte por guardá-lo na *Rede de Confiança*, são desmembrados em várias partes criptografadas enviadas a usuários diferentes. Para garantir a disponibilidade do documento, cada parte é replicada utilizando a técnica de redundância denominada Replicação, apresentada na seção 2.3. O armazenamento em locais distintos satisfaz três aspectos de segurança:

(i) O espalhamento de um arquivo pela rede impede o acesso indevido, pois o comprometimento de uma máquina não expõe integralmente um documento sigiloso. Nenhuma estação de trabalho possui uma versão integral do arquivo;

(ii) Caso a máquina do usuário seja danificada, o documento não é perdido, pois está a salvo na rede; e

(iii) Se uma sede da instituição é totalmente comprometida devido a um ataque ou em virtude de problemas de calamidade pública, os documentos podem ser recuperados de outro lugar geográfico.

4.3 A REPUTAÇÃO DOS USUÁRIOS

Quanto maior o nível de sigilo atribuído a um arquivo, mais confiáveis devem ser os usuários que solicitam acesso ao conteúdo armazenado (ver Figura 4.3). A confiabilidade de um usuário é medida em função do seu *status* de reputação, conforme será explanado na seção 5.3. Para que um usuário comece a fazer parte de uma rede de assuntos sigilosos, há uma investigação anterior, de tal modo que o indivíduo seja considerado confiável. Partindo-se dessa premissa, sua estação de trabalho é considerada confiável e a partir da análise das interações com outros *peer*, seu *status* de reputação começa a ser penalizado, caso seja detectada alguma ação maliciosa. À medida que tais observações passam a ser rotineiras, sua reputação é diminuída e a estação de trabalho perde o acesso a determinados graus de sigilo.

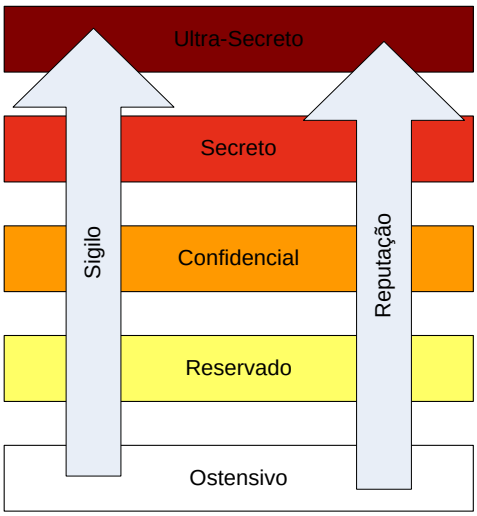

Figura 4.3. Relação entre Sigilo e Reputação.

Por fim, cabe salientar que a Rede de Confiança pode ser formada por membros (*peers*) de uma mesma instituição, ou pela junção de organizações diferentes que tratem de assuntos correlacionados interligadas através de seus servidores, fazendo o papel de *super-peers*, como exemplificado na Figura 4.4.

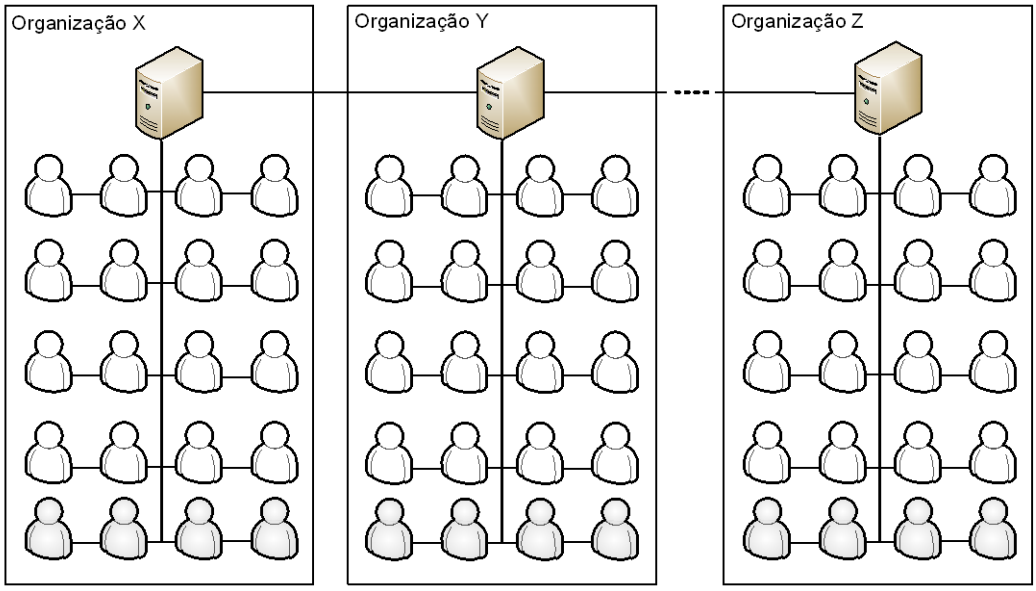

Figura 4.4. Rede de Confiança composta por *n* organizações.

4.4 CONSIDERAÇÕES FINAIS

A Rede de Confiança proposta assemelha-se a uma rede social privada que apresenta uma alta disponibilidade dos usuários em função dos mesmos estarem praticamente conectados durante todo o horário do expediente de trabalho. Além da criptografia, aplicamos uma segunda camada de segurança, a fragmentação dos arquivos, com o objetivo de tornar extremamente trabalhoso a um atacante obter acesso ao seu conteúdo, pois, para conseguir realizar a leitura de um arquivo, além das chaves necessárias para a decodificação, o atacante deverá reunir todos os fragmentos espalhados na rede do arquivo de seu interesse.

A utilização do sistema de reputação visa contribuir para a manutenção do sigilo das informações. À medida que as estações de trabalhos apresentam um comportamento considerado malicioso, seu *status* de reputação é penalizado e as máquinas deixam de ter acesso a certos arquivos, em função do grau de sigilo atribuído à informação existente.

Capítulo 5 – A Arquitetura da Rede de Confiança

A *Rede de Confiança* proposta neste trabalho é uma rede social privada onde as informações trocadas, compartilhadas e armazenadas requerem um alto grau de confidencialidade, em virtude do conteúdo dos arquivos. Os problemas de segurança são objetos constantes de preocupação para desenvolvedores de plataformas P2P utilizadas nas redes sociais. Neste capítulo, apresentaremos uma solução para uma infra-estrutura denominada *Rede de Confiança*, que permite o armazenamento e o compartilhamento de arquivos de forma segura. A intenção de um mecanismo de reputação é identificar comportamentos maliciosos dos *peers* participantes, auxiliando na prevenção do comprometimento das informações.

5.1 A INFRA-ESTRUTURA DE SEGURANÇA

Inicialmente, algumas medidas de segurança são necessárias para que, a partir delas, seja efetuado o correto gerenciamento do controle de acesso aos dados armazenados, corroborando para a garantia da confidencialidade.

5.1.1 Registro

Cada usuário deve ser registrado na Rede de Confiança. Este processo é necessário para garantir a adesão de novos participantes e permitir sua identificação pelo sistema de reputação. O usuário fará seu registro a partir de sua estação de trabalho. Após o processo de registro, cada usuário possuirá um único *UserID* e uma senha que servirão para o processo de *login* e autenticação na rede. Efetuado o processo de *login*, o status de conexão do usuário é anunciado aos demais integrantes, permitindo a troca de mensagens *online*.

5.1.2 Controle de acesso

Um arquivo pode ser armazenado e seu conteúdo compartilhado entre os integrantes da organização, entretanto nem todos os arquivos devem ser amplamente compartilhados, sendo restritos a grupos específicos. Este gerenciamento é realizado pelo Controle de Acesso.

O autor ou o indivíduo que possui a guarda de um documento sigiloso deve ter a possibilidade de gerenciar os indivíduos que possuem acesso ao arquivo. O Controle de acesso tem o objetivo de contribuir para a garantia da confidencialidade dos arquivos compartilhados dentro da instituição.

5.1.3 Comunicação segura de mensagens (*chat*)

A Rede de Confiança também provê um canal seguro de troca de mensagens entre os usuários que, por ventura, estejam conectados online. As mensagens enviadas devem chegar ao seu destinatário com garantias de confidencialidade e integridade. Para isso, os pacotes trocados são criptografados, de tal maneira que o seu conteúdo apenas possa ser decodificado pelos participantes do *chat*.

5.1.4 Reputação dos *peers*

Um sistema de reputação em redes P2P exerce um importante papel no provimento da segurança da rede. Normalmente, a partir das interações entre os nós, é possível qualificá-

los em termos de confiança, com o intuito de utilizar os *peers* mais confiáveis nas atribuições dos serviços e rotinas mais importantes para o bom desempenho da rede. Nesta proposta, a reputação dos *peers* é levada em consideração no processo de recuperação de um arquivo, pois o *peer* que solicita acesso ao dado armazenado deve possuir reputação compatível com o grau de sigilo atribuído à informação.

5.2 A ARQUITETURA

O projeto arquitetônico da *Rede de Confiança* é baseado em uma rede social privada sob uma plataforma P2P [Graffi 2009]. Com o intuito de garantir a confidencialidade e autenticidade dos dados armazenados e das mensagens trocadas entre os integrantes da Rede de Confiança, é utilizada a técnica da criptografia assimétrica, cuja fácil utilização é uma dos principais motivos do seu emprego em várias aplicações nos sistemas distribuídos.

Na criptografia assimétrica, cada usuário possui um par de chaves, sendo uma pública (Pub_A) e uma chave privada (Pri_A) criadas a partir do seu *UserId* e da sua senha. A chave pública de um usuário é armazenada em um chaveiro público e acessível a todos os demais nós da rede, enquanto sua chave privada é de conhecimento apenas do seu proprietário.

Na troca de mensagens entre usuários, quando um usuário R (remetente) deseja enviar uma mensagem M para um usuário D (destinatário), esta mensagem M é enviada para D após ser cifrada por R utilizando a chave pública de D. Por ocasião de sua chegada ao destino, o usuário D decodifica a mensagem M utilizando sua chave privada. Este processo é descrito na seção 2.6.2.

Para o armazenamento e compartilhamento de arquivos em rede e controle de acesso, utilizamos uma abordagem híbrida, utilizando criptografia simetria e assimétrica. Cada um dos arquivos sigilosos é criptografado com uma chave simétrica e única que, por sua vez, é criptografada com as chaves públicas dos usuários que possuem algum privilégio sobre o arquivo em questão (ver seção 5.2.2). Após isso, os dados são fragmentados, replicados e armazenados em pontos aleatórios da rede, entretanto seu conteúdo só pode ser acessado pelo conjunto inicialmente definido usuários.

Descreveremos agora como são realizados os passos necessários e os serviços providos pela rede de Confiança.

5.2.1 O Registro dos usuários

O primeiro passo é cadastrar o endereço da máquina do usuário no servidor de sua organização como integrante da Rede de Confiança. Após isso, o usuário escolhe seu *userID* e uma frase secreta, para que sejam geradas uma chave pública (Pub_A) e outra privada (Pri_A). Estas chaves são cruciais para os processos de criptografia e assinatura digital de documentos, nos processos de garantia da confidencialidade a autenticidade dos arquivos.

No processo de *login* do usuário, além do seu *userID* e senha, também é verificada a identificação do nó através do seu endereço IP (*IPAadress*). No servidor, há um objeto para cada usuário denominado *LoginSec*, que contém os dados necessário para a identificação de um nó. O *IPAdress* do usuário é utilizado para o encaminhamento de mensagens criptografadas provenientes dos demais nós da rede.

5.2.2 O Controle de Acesso

Um usuário pode criar, ler e apagar um arquivo compartilhado (*SharedFile*), desde que possua algum desses direitos. Uma lista de controle de acesso é necessária para garantir a disponibilidade dos dados armazenados. Cada *SharedFile* possui uma chave simétrica e única gerada de maneira pseudo-aleatória, utilizando o algoritmo AES.

O *SharedFile* é então criptografado com a sua chave simétrica que, por sua vez, é criptografada com as chaves públicas de cada um dos usuários que possuem acesso ao arquivo. O *SharedFile* é então fragmentado em blocos que são armazenados em usuários diferentes. Uma visão geral do processo acima descrito pode ser observada na Figura 5.1.

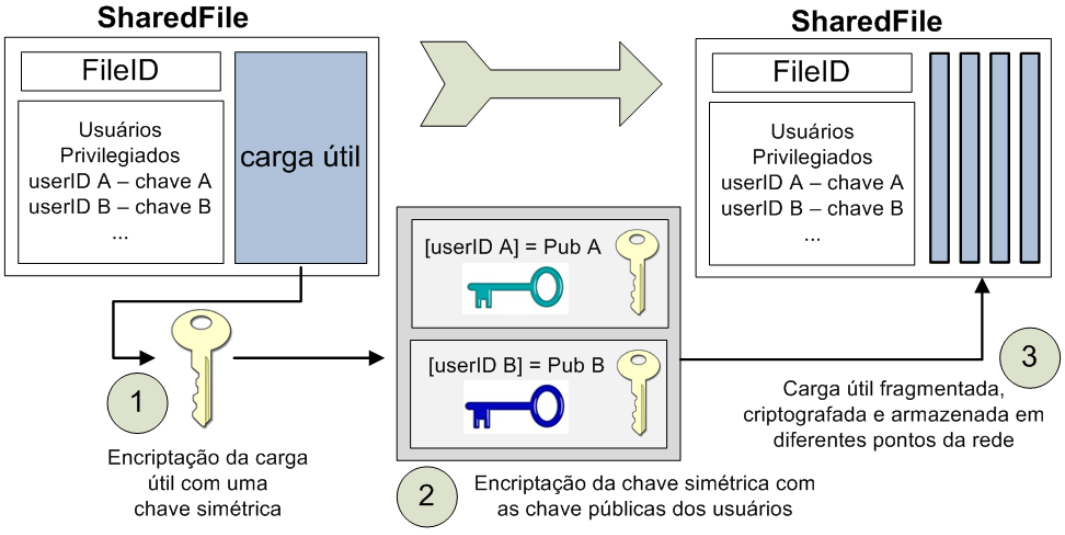

Figura 5.1. Esquema de criptografia do *SharedFile*.

Quando um arquivo é armazenado na rede, o autor pode definir um conjunto de usuários com acesso à sua leitura. Para isso, é criada uma chave simétrica, única para cada arquivo, que é utilizada para cifrar o *SharedFile* (passo 1). Essa chave simétrica é então criptografada com as chaves públicas dos usuários com acesso ao documento, criando assim um número de cópias criptografadas da chave simétrica igual ao número de usuários com acesso ao documento (passo 2) . Após criptografado, o *SharedFile* é fragmentado e arquivado na rede de tal maneira que cada bloco seja armazenado em uma máquina diferente (passo 3). O *SharedFile* possui um campo associado denominado *FileID* que é utilizado para a posterior localização das partes integrantes do arquivo.

Para modificar a relação de usuários com privilégios de um *SharedFile*, a lista de chaves deve ser alterada. Cabe salientar também que um nó malicioso não consegue acessar o teor de um fragmento nele armazenado, pois o conteúdo de um arquivo só é exposto quando todos os fragmentos são reunidos e as chaves corretas são utilizadas no processo de decifragem.

As chaves públicas dos usuários ficam armazenadas em chaveiro público, a fim de que possam ser consultadas e importadas para a máquina do indivíduo que deseja compartilhar documentos com outros membros da rede. A Figura 5.2 apresenta um modelo de interface utilizada para o gerenciamento de chaves. As chaves podem ser encontradas no chaveiro público, realizando uma pesquisa pelo nome do usuário ou por algum código individual, como por exemplo, o número de sua matrícula na organização.

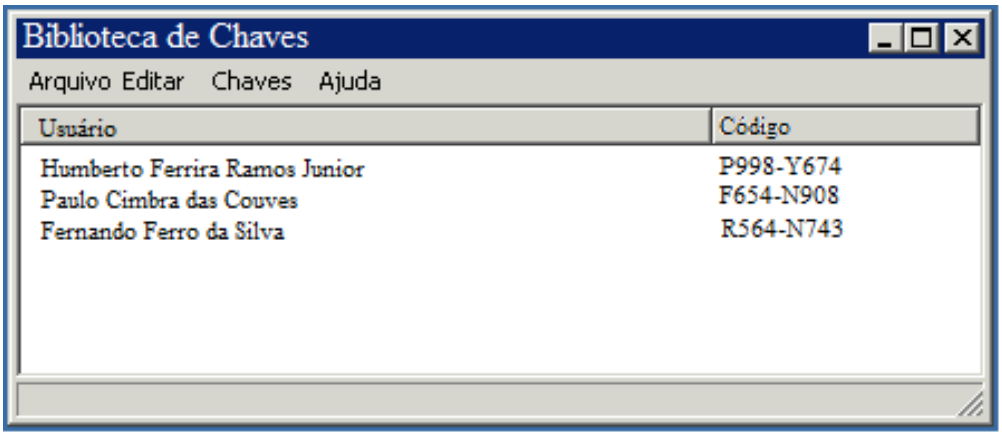

Figura 5.2. Interface de Gerenciamento de Chaves.

Feita a importação das chaves públicas de interesse para a sua máquina, elas estarão disponíveis para serem utilizadas pela interface apresentada na Figura 5.3. Após o *login* no sistema, o usuário pode selecionar um arquivo através da tecla “Procurar arquivo”, selecionar

um conjunto das chaves dos demais usuários fazendo, uso da tecla “Compartilhar arquivo” e, em seguida, teclar “Enviar arquivo”. Feito isto, o arquivo aparece no campo “Meus arquivos” com a relação dos usuários compartilhados.

Os arquivos cujos autores tenham compartilhado o acesso com outro usuário aparecerão no campo “Arquivos compartilhados comigo”, podendo ser selecionados e recuperados através da tecla “Recuperar arquivo”. Por fim, um arquivo poderá ser excluído após ser selecionado no campo “Meus arquivos” ou “Arquivos compartilhados comigo”, caso o usuário possua este direito, e apagado com o uso da tecla “Deletar arquivo”.

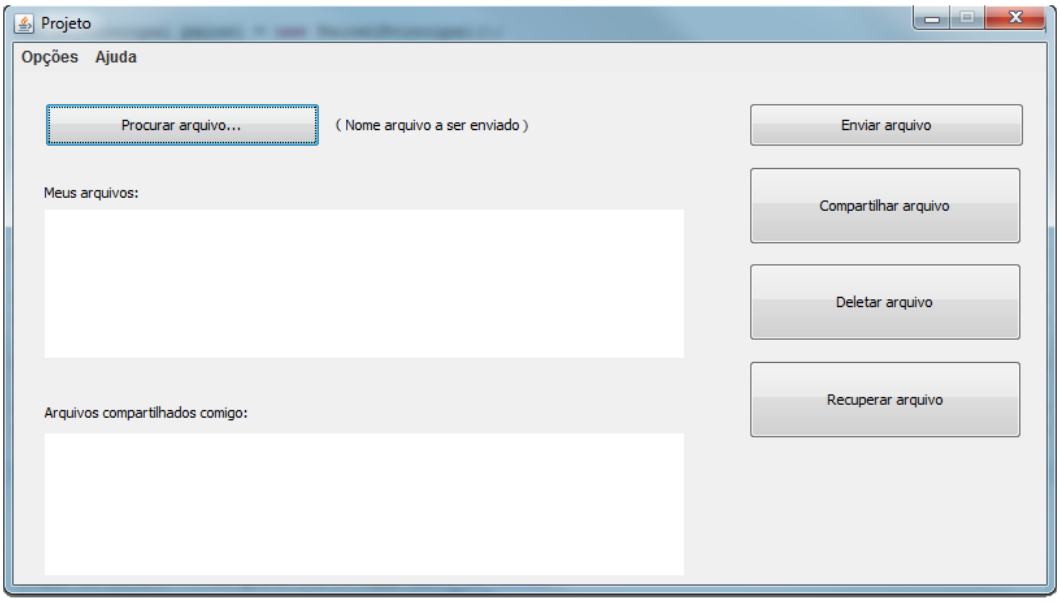

Figura 5.3. Protótipo da Interface de Compartilhamento de Arquivos.

5.2.2.1 Mensagens de Texto Online

Um serviço presente na Rede de Confiança é a troca de mensagens *online* entre seus integrantes. Quando um *usuário A* deseja estabelecer uma conexão segura com outro *usuário B*, o primeiro usuário cria uma chave de sessão simétrica para criptografar sua mensagem convite. O *usuário A* então envia a mensagem convite e a chave simétrica de sessão, ambas criptografadas com a chave pública de *B* (Pub_B) e assinadas com a chave privada de *A* (Pri_A), garantindo a autenticidade do usuário *A* e possibilitando que apenas o usuário *B* possa decifrá-la. Se *B* aceitar a solicitação de comunicação *A*, a conversação é então iniciada com a chave simétrica da sessão enviada por *A*. Esse processo é exemplificado na Figura 5.4.

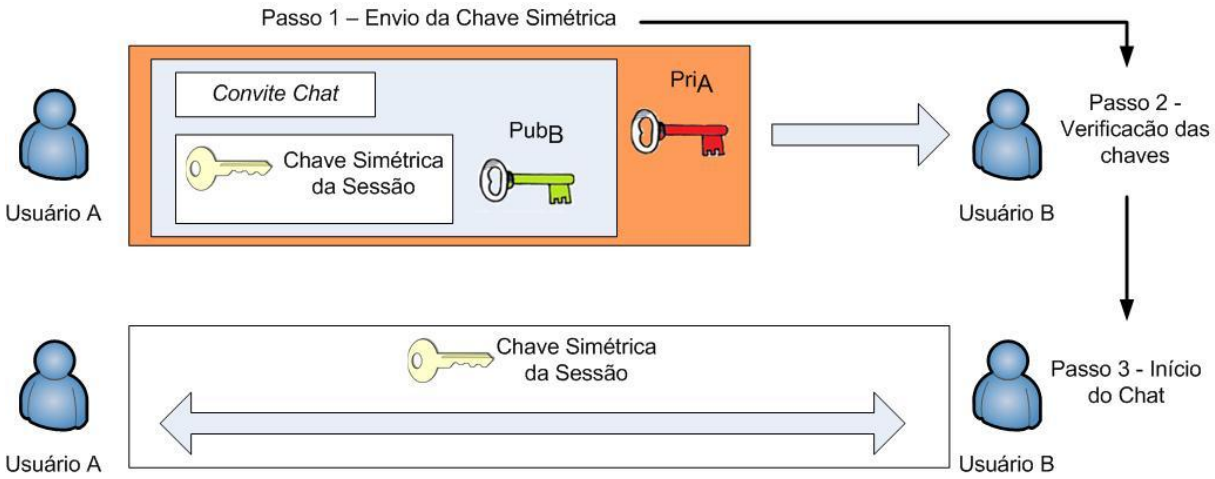

Figura 5.4 Esquema de Comunicação Segura (Chat).

5.3 O SISTEMA DE REPUTAÇÃO

O uso de sistemas P2P de compartilhamento de arquivos é um paradigma bastante aceito para o armazenamento e compartilhamento de informações. Esquemas de estímulo à cooperação entre os usuários podem ser empregados, mas *peers* mal-intencionados podem querer tirar proveito da rede por meio de comportamentos egoístas e maliciosos. Por isso, é necessária a utilização de mecanismos capazes de identificar tais *peers*, a fim de prevenir a perda de informações e/ou diminuição do desempenho da rede.

Nas aplicações P2P, um usuário pode acessar diretamente um arquivo no disco rígido de outros usuários, por isso torna-se necessária a utilização de mecanismos de controle, a fim de prevenir a perda e o acesso a dados sigilosos por usuários mal-intencionados. A utilização de um mecanismo de reputação possibilita identificar *peers* não confiáveis, permitindo que o acesso aos dados sensíveis apenas seja feito por *peers* que apresentem reputação compatível com o grau de sigilo atribuído a um arquivo.

Neste trabalho, é utilizada uma abordagem semelhante à apresentada por Tran *et al.* (2005) que provê o controle de acesso para redes P2P voltadas ao compartilhamento de arquivos, preservando a estrutura descentralizada de sua plataforma. Cabe salientar que, enquanto a metodologia de Tran *et al.* (2005) incrementa a reputação à medida que as interações bem sucedidas acontecem, nesta dissertação, partindo-se da premissa que os usuários são considerados confiáveis ao serem autorizados a participarem da Rede de Confiança, a reputação de uma estação de trabalho é decrescida quando: (i) deveria armazenar um fragmento de um arquivo e este bloco não é encontrado pelo *peer* solicitante; ou (ii) o bloco enviado por esta estação de trabalho está corrompido.

Os arquivos armazenados nos *peers* são classificados pelo autor quanto ao grau de sigilo em: ostensivo, reservado, confidencial, secreto e ultra-secreto. Para cada um desses níveis, é atribuído um valor mínimo de reputação variando entre 0 e 1. O *peer* considera que os arquivos nele armazenados precisam ser protegidos e os demais *peers* necessitam manter um nível de reputação compatível com o grau de sigilo atribuído ao arquivo solicitado.

O mecanismo de reputação deve poder classificar os *peers* e atribuir-lhes diferentes direitos de acordo com seu atual *status* de reputação, embora, por vezes, sejam contatados *peers* sem nenhuma interação anterior. O *status* de reputação ou confiabilidade de um *peer* assume um valor entre [0,1] e é calculado em função de dois fatores: *confiança direta* e *confiança indireta*.

Na *confiança direta*, em cada interação entre dois pontos da rede, no processo de tentativa de recuperação de um fragmento de arquivo, a reputação do *peer* de origem é mantida se o bloco é recebido e sua integridade é confirmada. Entretanto, se o fragmento não é encontrado no *peer* que deveria armazená-lo, ou o bloco é enviado corrompido, a interação entre ambos é considerada mal sucedida e o *peer* de origem terá sua reputação penalizada. O efeito desta penalização é melhor compreendido observando a Figura 5.5.

A sistemática proposta contempla não só a análise da reputação e o controle de acesso ponto-a-ponto isoladamente. Com o intuito de utilizar uma visão global e a impressão de outros *peers*, é empregada a *confiança indireta* conforme abordado na seção 5.3.2. Assim, o *status* de reputação faz com que os *peers* sejam interdependentes no processo de controle de acesso a um dado arquivo.

O primeiro passo para o apropriado funcionamento do sistema de reputação é a correta identificação de cada um dos pontos da rede. Como a reputação dos *peers* leva em consideração as interações passadas com os demais pontos da rede, é de suma importância que a identidade de cada um deles seja única, a fim de evitar que *peers* possam assumir diferentes identidades.

Em cada transação entre dois *peers*, um processo de autenticação mútua é iniciado pelo *peer* A que deseja estabelecer contato com o *peer* B. O *peer* A envia uma solicitação de autenticação contendo sua identificação e uma chave simétrica de sessão, ambas cifradas com a chave pública de B, e assinadas com a chave privada do peer A. Depois de recebida esta solicitação, e verificada a autenticidade da origem A, o destinatário B está pronto para começar a interagir com o remetente da mensagem. Estabelecida a conexão, os *peers* verificam se há algum registro em seus bancos de dados sobre reputação. Caso não haja, uma entrada destinada a tal fim é criada.

A reputação de um *peer* percebida pelos demais é resultado das experiências das interações diretas entre ambos e dos julgamentos enviados pelos demais sobre o *peer* a ser avaliado, ou seja, a reputação é definida através da combinação de dois valores: *confiança direta* e *confiança indireta.* A *confiança direta é a* representação de quanto um *peer* confia no outro baseado nas interações diretas entre ambos. A *confiança indireta* é calculada a partir das avaliações enviadas pelos demais *peers*.

5.3.1 Confiança direta

Há vários algoritmos presentes na literatura que calculam a *Confiança Direta* baseando-se nas experiências anteriores. Apresentamos uma abordagem semelhante à utilizada por Tran *et al.* (2005), onde o resultado dessas interações é expresso pela Eq. 5.1:

$$T_{ij} = \alpha^n, \text{ onde:} \qquad \text{(Eq. 5.1)}$$

T_{ij} representa o valor de confiança que o peer *i* atribui ao peer *j*;

n é o número de transações mal sucedidas realizadas com o *peer j*, ou seja, onde o *peer j* envia um fragmento corrompido ou, por alguma razão, não está mais de posse do fragmente que deveria nele estar armazenado; e

α é um número real entre 0 e 1 denominado taxa de aprendizagem. Quanto menor o valor de α, mais rapidamente a confiança direta decresce.

Logo, T_{ij} é um número positivo entre 0 e 1. Quanto menor for o valor de α, mais rapidamente decresce o valor da confiança, conforme pode ser observado na Figura 5.5.

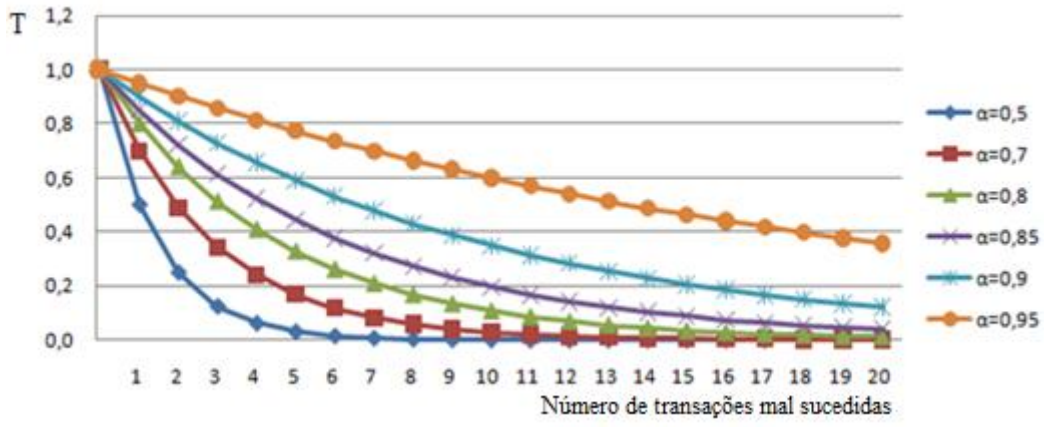

Figura 5.5 Variação da Reputação em função do número de interações comprometidas.

À medida que o número de experiências negativas entre os *peers* i e j aumenta, o valor de confiança, T_{ij} aproxima-se de 0. Como o *n* assume inicial valor zero, implica que T_{ij}

assume valor 1, refletindo a confiança positiva no começo das interações, pois normalmente o indivíduo que entra na *Rede de Confiança* é considerado inicialmente confiável.

Quando houver a necessidade de que a reputação de um *peer* específico seja restabelecida, uma mensagem em *broadcast* pode ser disseminada, a partir de um servidor, e todos os demais pontos da rede que possuírem alguma entrada para este *peer* atualizaram seu *status* de reputação para o valor 1, ou seja, passarão a considerá-lo novamente confiável.

5.3.2 Confiança Indireta

Em ambientes de compartilhamento P2P, há uma grande chance de pontos da rede nunca terem interagido anteriormente. Por isso, para estabelecermos a confiança entre dois *peers* considerados estranhos utilizamos a Confiança Indireta, conforme observado na Eq. 5.2.

$$R_{ij} = \frac{\sum_{t=1}^{k} T_{it} * T_{tj}}{k} \qquad \text{(Eq. 5.2)}$$

R_{ij} representa o valor de confiança indireta que o *peer i* deposita em *j*, sendo R_{ij} um número positivo entre 0 e 1;

k é um número inteiro utilizado para limitar o número de recomendações para o cálculo de R_{ij}. Se o número de recomendações recebidas aumenta, o *peer* analisará apenas as *k*-últimas avaliações; e

T_{it} representa a confiança direta do *peer i* em *t*. T_{tj} é a confiança direta do peer *t* em *j*. A partir disso, calculamos a confiança indireta R_{ij} entre os peers *i* e *j*. Como os valores de T_{it} *e* T_{tj} estão compreendidos entre 0 e 1, R_{ij} estará sempre entre esses dois valores (ver Figura 5.6). As recomendações indiretas envolvem um único nível de indicação, ou seja, o *peer i* apenas envia o resultado de uma interação ao conjunto de *peers* com quem já interagiu anteriormente.

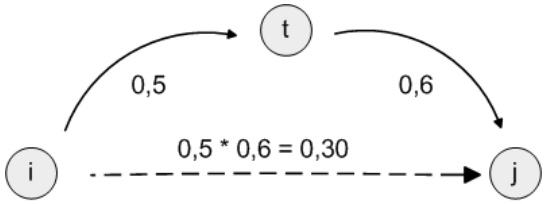

Figura 5.6. Representação da Confiança Indireta entre os *peers* i e j.

5.3.3 Permissão para *Download*

Para cada grau de sigilo (ostensivo, reservado, confidencial, secreto ou ultra-secreto) atribuído a um arquivo, existe um valor associado denominado *threshold de confiança* (A_{th}), que representa o valor mínimo de confiança requerida a um *peer i* que solicita o *download* de um fragmento armazenado no *peer j*. Quanto maior o grau de sigilo do arquivo, maior é o valor de A_{th} atribuído. O valor de A_{th} varia entre 0 e 1. Assim, um *peer* apenas pode ter acesso a um fragmento de arquivo confidencial armazenado em um ponto da rede, se possui *status* de confiança igual ou maior ao *threshold de confiança* necessário. Este limiar de acesso varia em função do grau de sigilo atribuído.

O *status* da confiança (A) que um *peer* deposita em outro é uma soma ponderada dos valores de confiança direta e indireta. Os pesos são definidos como CD para a confiança direta, CI para a confiança indireta, de tal forma que:

$$\mathrm{CD} + \mathrm{CI} = 1 \qquad \text{(Eq. 5.3)}$$

A partir da equação acima, Tran *et al.* (2005) definem o valor da confiança global (A_{ij}) entre dois *peers* como:

$$\mathrm{A_{ij}} = \mathrm{CD} * \mathrm{T_{ij}} + \mathrm{CI} * \mathrm{R_{ij}} \qquad \text{(Eq. 5.4)}$$

O valor de A_{ij} deve ser maior que os limiares A_{th} estabelecidos para cada grau de sigilo da informação a ser recuperada. Ou seja, quanto maior for o grau de sigilo, mais confiável deve ser o peer que solicita acesso a um arquivo. Assim, poderíamos ter a Tabela 5. 1 como um exemplo dos valores de A_{th} (Threshold de Confiança) estabelecidos para uma organização.

Tabela 5. 1 Exemplo de Threshold de Confiança (Ath)

Grau de Sigilo	Threshold de Confiança (A_{th})
Ultra-secretos	0,9
Secretos	0,8
Confidenciais	0,7
Reservados	0,5
Ostensivos	(não há sigilo neste nível)

A Figura 5.7 apresenta o fluxograma de interação entre um *peer Cliente* e outro *peer host*. Inicialmente, o *Cliente* obtém do servidor a lista dos *hosts* que possuem os fragmentos necessários à recomposição de um arquivo. A partir disso, iniciam-se os processos de requisição do arquivo, cálculo e distribuição de reputação.

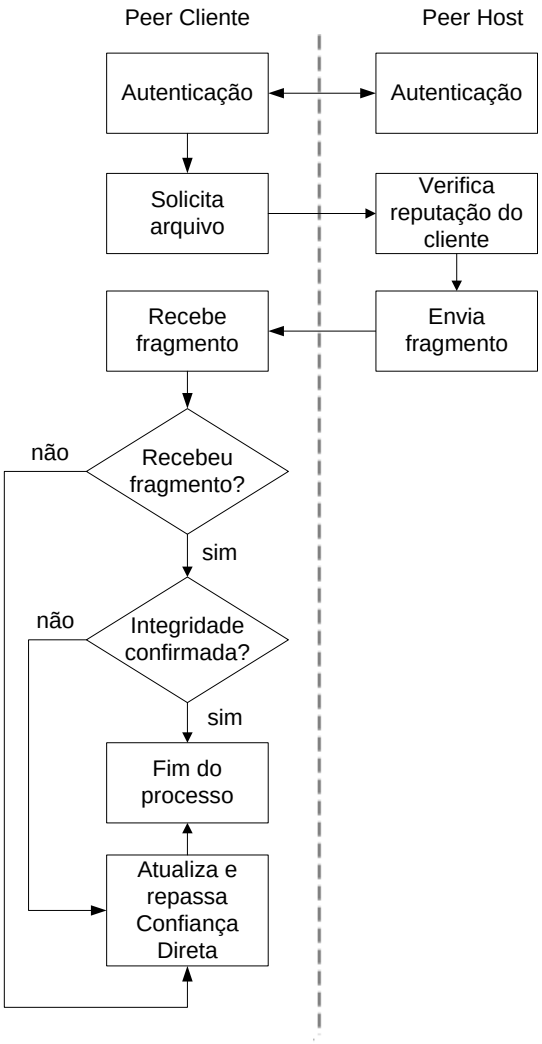

Figura 5.7. Processo de interação entre peers.

5.4 CONSIDERAÇÕES FINAIS

A infra-estrutura apresentada neste capítulo visa ao compartilhamento e à confidencialidade dos dados armazenados em uma rede formada por membros pertencentes a uma mesma organização ou a indivíduos pertencentes a instituições diferentes que tratem de assuntos afins. A idéia principal desta dissertação é o desenvolvimento de uma sistemática que permita a sobrevivência de informações sigilosas espalhando-as em locais geograficamente distintos. A fragmentação dos arquivos e a utilização da criptografia podem ser encaradas como duas barreiras a serem vencidas por um usuário mal-intencionado, tornando algo bastante trabalhoso para um atacante.

Através do registro dos indivíduos, apenas membros cadastrados podem ter acesso ao sistema. Além disso, a correta identificação de cada uma das estações de trabalho é

imprescindível em função da utilização do sistema de reputação, que atribui um status de confiabilidade à estação utilizada pelo usuário. Para que um indivíduo possa ter acesso a informações sigilosas, pressupõe-se ser confiável, assim como deve ser a sua estação de trabalho.

A sistemática do sistema de reputação utilizando as reputações direta e indireta tem o propósito de construir uma reputação global, evitando que os *peers* construam impressões isoladas, levando em consideração apenas a reputação de indivíduos com quem interagiram no passado.

Outro conceito presente é o ato de classificar os documentos em diferentes graus de sigilo em função da importância e do valor agregado à informação contida. Quanto maior o grau de sigilo do arquivo, mais restrito é o grupo de indivíduos que possuem acesso, pois a informação deve ficar cada vez mais restrita aos membros mais confiáveis da organização. Por analogia, as informações com maior grau de sigilo devem ter acesso restrito às estações de trabalho com maior grau de confiabilidade. Por isso, a idéia de utilizar um sistema de reputação, com o intuito de atribuir um *status* de confiabilidade às estações utilizadas individualmente pelos usuários.

Capítulo 6 – Avaliação Experimental e Análise dos Resultados

Neste capítulo, apresentamos os resultados de testes realizados em dois cenários. O primeiro cenário representa usuários conectados em uma rede local e o segundo, visa simular usuários conectados em locais geograficamente distintos. Analisamos os tempos de armazenamento e recuperação de arquivos, variando o número de fragmentos em que o arquivo original é fragmentado e os tamanhos das chaves empregadas nos algoritmos utilizados nos processos de criptografia. O principal intuito deste capítulo é analisar como a aplicação das duas hipóteses apresentadas na seção 1.4 influencia no tempo de recuperação dos arquivos.

6.1 A AVALIAÇÃO EXPERIMENTAL

A avaliação experimental teve como objetivo analisar o impacto sobre o tempo de armazenamento e recuperação dos arquivos em dois cenários: (i) *Rede Local*, onde utilizamos um laptop com Processador Athlon 64X2 (2.0 Ghz) com Memória de 3 GB de DDR2 e seis computadores Pentium 4 (3 Ghz) com memória de 1GB interligados; e (ii) *via Internet*, onde utilizamos cinco computadores Pentium 4 (3 Ghz) com memória de 2GB interligados com conexão de 10 Mbps de *download* e 500 Kbps para *upload*.

Foi implementado um protótipo na linguagem Java com as funcionalidades necessárias para analisar os tempos de armazenamento e recuperação de arquivos. Nos teste realizamos as variações apresentadas na Figura 6. 1:

(i) tamanho dos arquivos: de 300k a 3000K;

(ii) quantidade de blocos gerados na fragmentação do arquivo: 3, 4 e 5 blocos; e

(iii) tamanho das chaves empregadas nos algoritmos de criptografia: utilizamos as seguintes combinações (RSA 1024 e AES 128), (RSA 1024 e AES 256) e (RSA 2048 e AES 256).

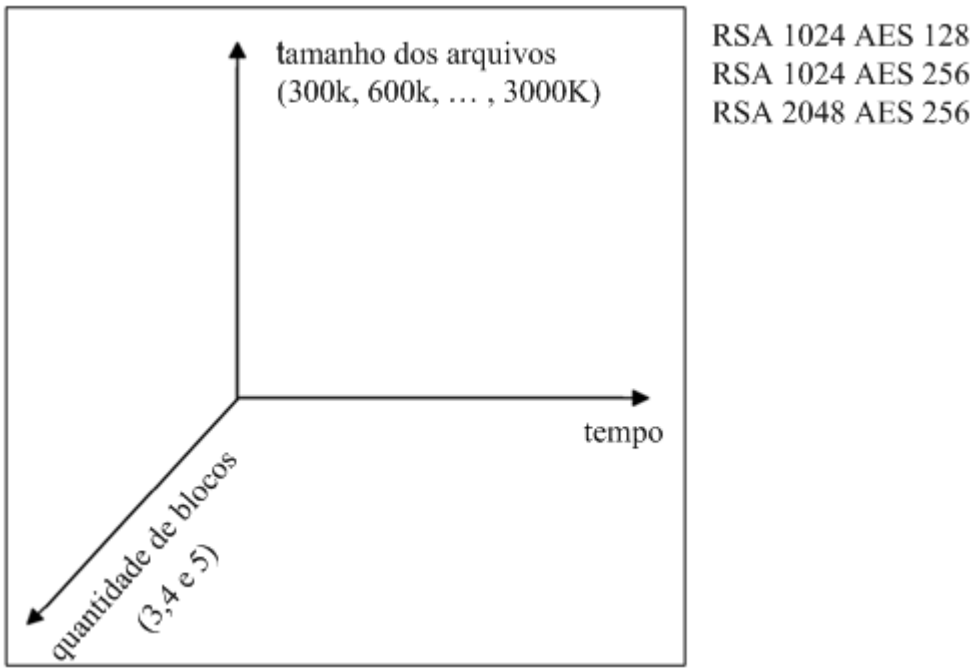

Figura 6. 1. Dimensões da avaliação experimental.

Para cada uma dessas combinações, extraímos a média de 50 experimentos realizados. Não foram empregados simuladores, os resultados foram obtidos a partir de

máquinas interligadas a redes que realmente estavam sendo utilizadas. Esta característica objetivou aproximar os resultados a valores reais.

Em cada um das máquinas empregadas nos testes, estava sendo executada uma instância do protótipo desenvolvido, excetuando-se a máquina utilizada como servidor. Para acessar o sistema é necessário o registro de cada um dos clientes no servidor, onde será anunciado seu número IP. Tendo o número IP do cliente em mãos, o servidor o incluirá na lista de *hosts* ativos. A partir deste momento, o *host* tem disponibilizadas duas funções básicas: compartilhar um arquivo e recuperar um arquivo compartilhado.

O primeiro passo para compartilhar um arquivo na rede é a obtenção de um lista de *hosts* ativos para os quais um Cliente pode enviar dados. Caso consiga obter esta lista do servidor, o Cliente criptografa o arquivo e divide a versão criptografada em um número de partes especificado pelo usuário. O Cliente então iniciará uma conexão TCP com cada um dos *hosts* presentes na lista enviada pelo servidor e enviará um fragmento para cada um destes *peers*, até que se consiga enviar o número total de pedaços em que o arquivo foi dividido. Por fim, o Cliente envia para o servidor uma lista dos *peers* escolhidos e o nome do arquivo, dados necessários para a recuperação do arquivo.

Para recuperar um arquivo, o Cliente faz uma requisição ao servidor para obter uma lista dos *hosts* que possuem os fragmentos criptografados do arquivo. A partir desta lista, o Cliente inicia uma conexão TCP com cada um dos *hosts* da lista para obter todos os pedaços do arquivo. Uma vez obtidos, os fragmentos são recombinados e o arquivo é descriptografado. As chaves assimétricas (algoritmo RSA) são geradas a partir do programa *openssl* e as chaves simétricas (algoritmo AES) são geradas por uma classe específica da aplicação. A utilização das chaves é demonstrada na seção 5.2.2.

Em cada um das máquinas empregadas para os testes, estava sendo executada uma instância do protótipo desenvolvido. Foi utilizado um diretório com arquivos de 0,3 Mb a 3Mb em formato de texto com figuras, que chegaram a atingir 1900 páginas de informações.

Analisamos basicamente os tempos de armazenamento e recuperação de arquivos. Na atividade de armazenamento, foi contabilizado: o tempo de geração da chave secreta (algoritmo simétrico) criada para o arquivo + a cifragem do arquivo com esta chave secreta + a cifragem da chave secreta do arquivo com a chave pública (algoritmo assimétrico) do autor + a fragmentação do arquivo em várias partes + o tempo de armazenamento dos fragmentos em diversos pontos da rede.

Para a recuperação, contabilizamos: o tempo de *download* dos fragmentos + o tempo de decifragem da chave secreta (algoritmo simétrico) + o tempo de decifragem do arquivo, tornando-o um texto claro.

6.2 ARMAZENAMENTO DOS ARQUIVOS

A Tabela 6.1 apresenta os resultados dos experimentos relativos à fragmentação dos arquivos no armazenamento. Utilizamos para a criptografia simétrica (AES) uma chave com 128 bits e para a assimétrica (RSA), uma chave de 1024 bits. Quando dividimos o arquivo original em 3, 4 e 5 fragmentos, verificamos tempos totais de armazenamento de aproximadamente, 4s, 5s e 6s, respectivamente. Contabilizamos desde a solicitação de arquivamento de um arquivo até a gravação dos fragmentos em diferentes pontos da rede.

A média obtida para cada um dos testes é fruto de 50 experimentos realizados. Utilizamos um Intervalo de Confiança (IC) de 95%, ou seja, 95 % das médias amostrais caíram a uma distância máxima de 1,96 desvios padrões do valor médio. Os tempos de armazenamentos para as diferentes combinações de chaves criptográficas e números de fragmentos encontram-se listados nos apêndices A a I.

Tabela 6.1. Armazenamento RSA 1024 AES 128

	3 fragmentos			4 fragmentos			5 fragmentos		
Tamanho	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**
300k	3664	84	3641 - 3687	4854	136	4816 - 4892	6005	295	5923 – 6087
600k	3685	52	3671 - 3699	4846	70	4827 - 4865	5936	36	5926 – 5946
900k	3707	47	3694 - 3720	4848	39	4837 - 4859	5935	35	5925 – 5945
1200k	3735	43	3723 - 3747	4900	185	4849 - 4951	5971	31	5962 – 5980
1500k	3744	22	3738 - 3750	4905	41	4894 - 4916	6094	370	5991 – 6197
1800k	3780	31	3772 - 3788	4954	190	4901 - 5007	6050	276	5974 – 6126
2100k	3814	31	3805 - 3823	4957	35	4947 - 4967	6064	235	5999 – 6129
2400k	3827	42	3815 - 3839	4975	61	4958 - 4992	6049	41	6038 – 6060
2700k	3933	398	3823 - 4043	5020	182	4969 - 5071	6113	299	6030 – 6196
3000k	3882	119	3849 - 3915	5017	42	5005 - 5029	6129	231	6065 – 6193

DP = Desvio Padrão. IC = Intervalo de Confiança. Tempo em (ms).

6.2.1 A Criptografia no Armazenamento

Contabilizamos os períodos afetos especificamente à operação de criptografia dos arquivos. Na Tabela 6.2, apresentamos os tempos paras os diferentes tamanhos de arquivos e diversas combinações de chaves criptográficas.

Tabela 6.2. Tempo de criptografia dos arquivos

Tamanho	3 fragmentos			4 fragmentos			5 fragmentos		
	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256
300k	47	39	61	19	39	37	18	34	35
600k	35	58	59	42	58	51	34	51	56
900k	53	73	83	50	73	71	51	71	73
1200k	65	105	114	65	105	91	66	91	92
1500k	90	130	112	84	130	116	81	107	112
1800k	96	126	142	99	126	143	113	129	128
2100k	115	144	162	114	144	162	119	141	148
2400k	130	163	193	130	163	208	134	151	167
2700k	158	192	195	145	192	191	159	191	184
3000k	166	200	226	174	200	212	185	204	212

Tempo em (ms)

Na Figura 6. 2, podemos verificar graficamente que o tempo de criptografia varia em função do tamanho dos arquivos, mas não é afetado significativamente pela mudança dos algoritmos de codificação. Ou seja, levando em consideração os tempos totais da operação de armazenamento dos arquivos na rede (ver Tabela 6.1), podemos observar que a alteração das chaves criptográficas não tem grande impacto sobre todo o processo. Por exemplo, no processo de armazenamento de um arquivo de 3000K com as chaves RSA 1024 bits e AES 128 bits, dividindo-o em 5 fragmentos, o tempo total foi de 6,1 s, com um tempo de criptografia de apenas 185 ms.

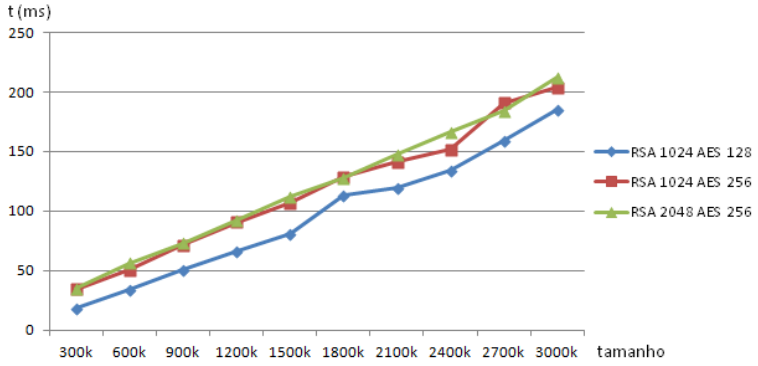

Figura 6. 2. Tempo de criptografia dos arquivos

6.3 OS TEMPOS DE RECUPERAÇÃO DOS ARQUIVOS

A Tabela 6.3 apresenta os tempos de recuperação de arquivos na *Rede de Confiança*. Analisamos duas variáveis: o número de fragmentos em que o arquivo é dividido (3, 4 e 5 partes) e os diferentes tamanhos das chaves utilizadas nos algoritmos criptográficos (RSA 1024 AES 128, RSA 1024 AES 256 e RSA 2048 AES 256.

Os experimentos foram realizados em laboratórios que estavam sendo normalmente utilizados por vários outros alunos. Este fato foi importante para aproximarmos os tempos encontrados a valores mais próximos da realidade. Os valores obtidos são reais e obtidos a partir de uma rede real, pois não foram empregados simuladores. Os valores dos experimentos realizados nesta seção encontram-se listados nos apêndices de J a R. Para cada uma das médias foram realizados 50 experimentos.

Tabela 6.3. Tempos de Recuperação de arquivos em rede local

		3 fragmentos			4 fragmentos			5 fragmentos		
RSA 1024 AES 128	**Tamanho**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**
	300k	3992	96	3965 - 4019	5037	115	5005 - 5069	6141	421	6024 - 6258
	600k	4274	158	4230 - 4318	5174	108	5144 - 5204	6171	248	6102 - 6240
	900k	4440	110	4410 - 4470	5340	112	5309 - 5371	6193	89	6168 - 6218
	1200k	4607	135	4569 - 4645	5544	119	5511 - 5577	6313	75	6292 - 6334
	1500k	4854	104	4825 - 4883	5774	235	5709 - 5839	6458	69	6439 - 6477
	1800k	5151	209	5093 - 5209	5958	166	5912 - 6004	6628	101	6600 - 6656
	2100k	5313	154	5270 - 5356	6142	139	6103 - 6181	6816	167	6770 - 6862
	2400k	5616	182	5565 - 5667	6330	259	6258 - 6402	6941	306	6856 - 7026
	2700k	5798	161	5753 - 5843	6595	223	6533 - 6657	7000	109	6970 - 7030
	3000k	6130	302	6046 - 6214	6813	495	6676 - 6950	7193	151	7151 - 7235
		3 fragmentos			**4 fragmentos**			**5 fragmentos**		
RSA 1024 AES 256	**Tamanho**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**
	300k	4037	87	4013 - 4061	5191	106	5162 - 5220	6049	167	6003 - 6095
	600k	4354	130	4318 - 4390	5282	137	5244 - 5320	6176	185	6125 - 6227
	900k	4539	129	4503 - 4575	5308	129	5272 - 5344	6126	135	6089 - 6163
	1200k	4732	79	4710 - 4754	5448	51	5434 - 5462	6191	118	6158 - 6224
	1500k	5046	189	4994 - 5098	5638	113	5607 - 5669	6222	148	6181 - 6263
	1800k	5268	35	5258 - 5278	5809	58	5793 - 5825	6351	267	6277 - 6425
	2100k	5638	127	5603 - 5673	6010	228	5947 - 6073	6904	257	6833 - 6975
	2400k	5827	77	5806 - 5848	6192	148	6151 - 6233	7018	255	6947 - 7089
	2700k	6111	52	6097 - 6125	6382	165	6336 - 6428	7159	283	7081 - 7237

	3000k	6314	172	6266 - 6362	6519	55	6504 - 6534	7337	150	7295 - 7379
RSA 2048 AES 256		**3 fragmentos**			**4 fragmentos**			**5 fragmentos**		
	Tamanho	Média (ms)	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**
	300k	4062	92	4036 - 4088	5045	103	5016 - 5074	6008	47	5995 - 6021
	600k	4161	64	4143 - 4179	5129	86	5105 - 5153	6074	57	6058 - 6090
	900k	4391	161	4346 - 4436	5288	100	5260 - 5316	6211	227	6148 - 6274
	1200k	4627	94	4601 - 4653	5429	80	5407 - 5451	6131	59	6115 - 6147
	1500k	4829	110	4799 - 4859	5685	268	5611 - 5759	6512	236	6447 - 6577
	1800k	5126	161	5081 - 5171	5841	128	5806 - 5876	6731	229	6668 - 6794
	2100k	5324	191	5271 - 5377	6066	138	6028 - 6104	6790	86	6766 - 6814
	2400k	5613	301	5530 - 5696	6262	183	6211 - 6313	6983	137	6945 - 7021
	2700k	5913	273	5837 - 5989	6406	171	6358 - 6454	7163	260	7091 - 7235
	3000k	6390	601	6223 - 6557	6659	231	6595 - 6723	7289	121	7256 - 7322

Tempo em (ms)

6.3.1 A Descriptografia na Recuperação

Contabilizamos os períodos afetos especificamente à operação de descriptografia dos arquivos. Na Tabela 6.4, apresentamos os tempos paras os diferentes tamanhos de arquivos e diversas combinações de chaves criptográficas.

Tabela 6.4. Tempo de descriptografia dos arquivos

Tamanho	**3 fragmentos**			**4 fragmentos**			**5 fragmentos**		
	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256
300k	63	51	205	42	39	88	42	41	90
600k	83	73	122	62	74	167	62	68	120
900k	80	88	224	96	102	155	84	96	175
1200k	114	141	191	112	118	250	105	116	180
1500k	144	151	425	131	195	228	135	136	223
1800k	162	254	660	142	183	269	147	156	227
2100k	168	416	506	173	194	257	173	187	224
2400k	194	506	954	219	435	310	191	222	269
2700k	212	76	954	233	231	484	238	243	357
3000k	236	243	1123	234	266	731	223	279	373

Tempo em (ms)

Na Figura 6. 3, podemos verificar graficamente que o tempo de descriptografia varia em função do tamanho dos arquivos, mas não é afetado significativamente pela variação dos algoritmos de codificação, pois todos estão na faixa dos ms (milisegundos). Ou seja, levando

em consideração os tempos totais da operação de recuperação dos arquivos na rede (ver Tabela 6.3), podemos observar que a mudança das chaves utilizadas na descriptografia não tem grande impacto, quando analisamos todo o processo de recuperação de arquivos. Por exemplo, no processo de recuperação de um arquivo de 3000K fragmentado em 5 blocos, empregando as chaves RSA 2048 bits e AES 256 bits, o tempo total foi de 7,3 s, com um tempo de criptografia de apenas 373 ms.

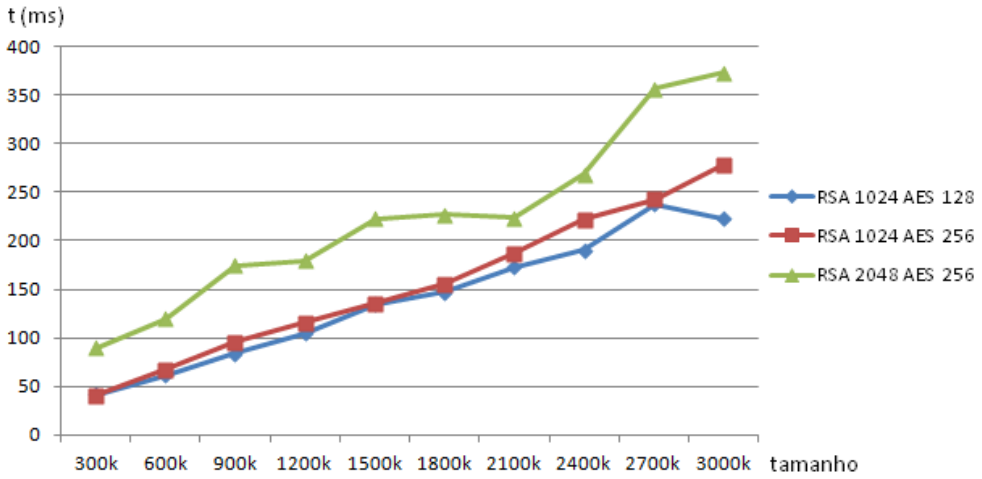

Figura 6. 3 Tempo de descriptografia dos arquivos

6.4 FATORES QUE INFLUENCIAM NO TEMPO DE RECUPERAÇÃO

Diversos fatores influenciam o tempo final de recuperação de um arquivo. Faremos uma análise do impacto do tamanho dos arquivos, da fragmentação e do tamanho das chaves empregadas nos algoritmos de criptografia. Para isso, utilizamos em alguns casos a Correlação entre estes fatores. A Correlação (ρ) é uma grandeza adimensional, com possíveis valores entre -1 e +1, que pode ser usada para comparar as relações lineares entre pares de variáveis em diferentes unidades. Duas variáveis aleatórias x e y com correlação não-zero são ditas correlacionadas. No caso de uma correlação positiva, quanto maior o valor de ρ, mais forte é a associação entre as duas variáveis, ou seja, à medida que x cresce, também cresce y [Montgomery e Runger 2009].

6.4.1 Tamanho do Arquivo

Na Tabela 6. 5 podemos constatar, por meio da correlação, que o tempo de recuperação aumenta à medida que o tamanho do arquivo também aumenta, ou seja, que o tamanho do arquivo logicamente influencia no seu tempo de recuperação, pois são valores de ρ bem próximos a 1.

Por exemplo, na tabela abaixo, a correlação entre o tamanho do arquivo e o seu tempo de recuperação é 0,997715852, quando utilizamos os algoritmos RSA e AES com chaves de 1024 e 128 bits, respectivamente, e fragmentamos o arquivo original em 3 partes. Ou seja, utilizando esta combinação de chaves e fragmentação, à medida que o tamanho dos arquivos aumenta, cresce também o seu tempo de recuperação.

Tabela 6. 5. Correlação entre tamanho do arquivo e tempo de Recuperação

Chaves	3 fragmentos	4 fragmentos	5 fragmentos
RSA 1024 AES 128	0,997715852	0,998318078	0,985319659
RSA 1024 AES 256	0,998396487	0,989692191	0,939318876
RSA 2048 AES 256	0,991259902	0,996482112	0,982045432

6.4.2 Fragmentação dos Arquivos

Para avaliarmos o impacto da fragmentação dos arquivos, mostramos as figuras abaixo (Figura 6. 4, Figura 6. 5 e Figura 6. 6), onde podemos verificar a apresentação gráfica dos tempos de recuperação utilizando a mesma combinação de chaves criptográficas, mas variando o número de partes nas quais os arquivos são fragmentados.

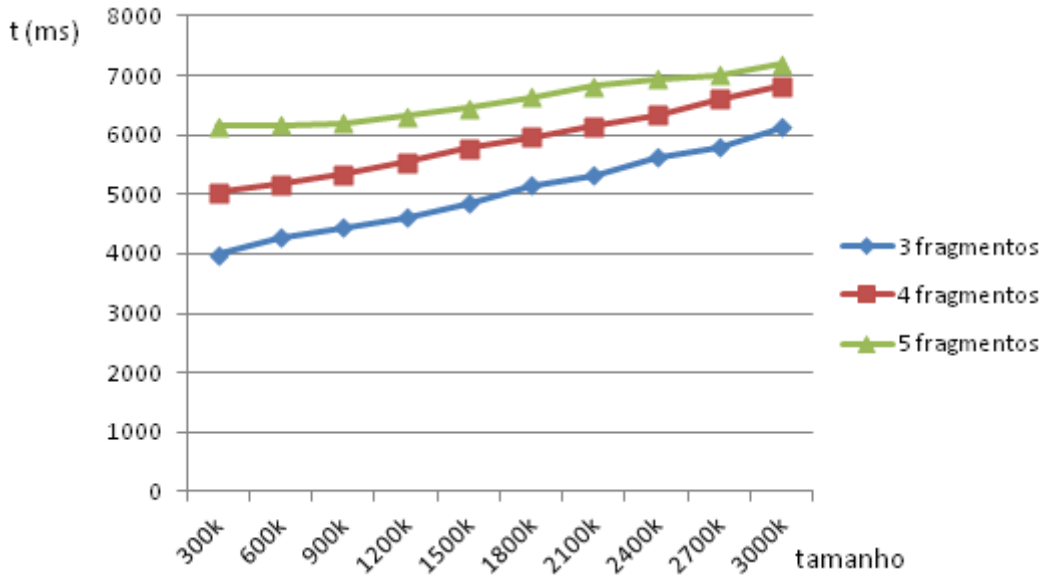

Figura 6. 4. Tempos de recuperação em rede local com RSA 1024 AES 128.

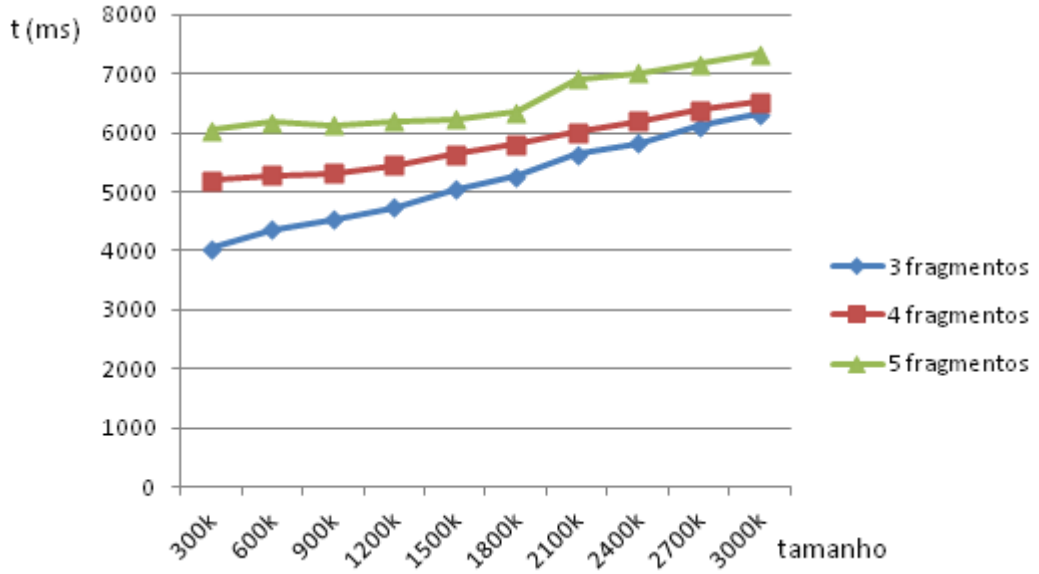

Figura 6. 5. Tempos de recuperação em rede local com RSA 1024 AES 256.

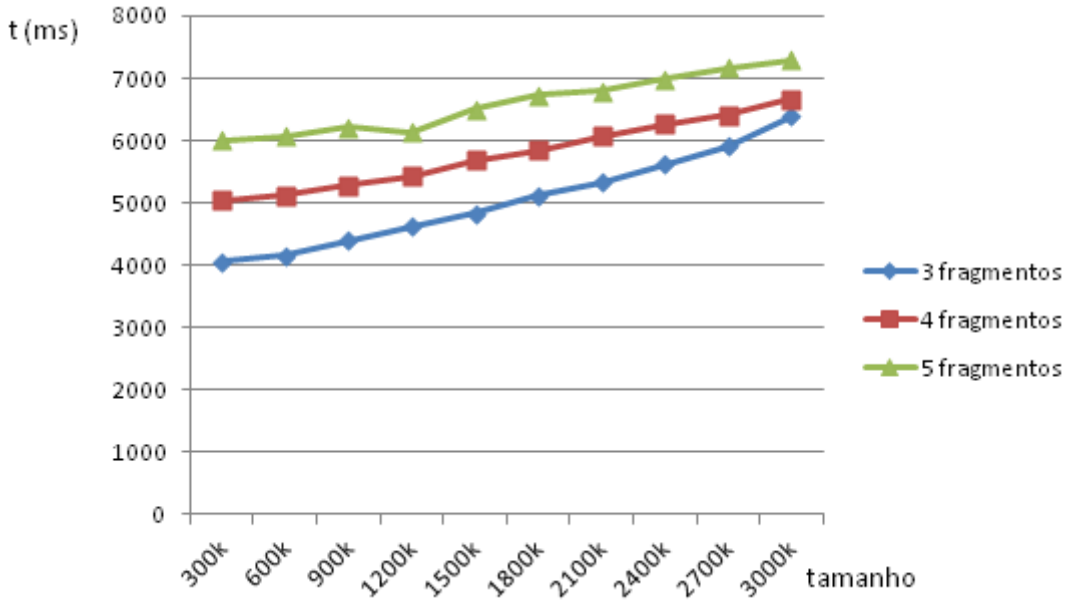

Figura 6. 6. Tempos de recuperação em rede local com RSA 2048 AES 256.

Além da apresentação gráfica acima, analisamos também a correlação (ρ) entre a fragmentação dos arquivos e seu tempo de recuperação (ver Tabela 6. 6). Por exemplo, a correlação entre a fragmentação do arquivo e o seu tempo de recuperação é 0,999874398, quando utilizamos os algoritmos RSA e AES com chaves de 1024 e 128 bits, respectivamente, e variamos a fragmentação de um arquivo de 300K em 4, 5 e 6 partes. Ou seja, como este valor é bem próximo a 1, podemos afirmar que a mudança na fragmentação dos arquivos está intrinsecamente ligada ao seu tempo de recuperação.

Tabela 6. 6. Correlação entre fragmentação do arquivo e tempo de recuperação

Tamanho	RSA 1024 AES 128	RSA 1024 AES 256	RSA 2048 AES 256
300K	0,999874	0,996412152	0,999982396
600K	0,999565	0,999941967	0,999975909
900K	0,99988	0,999841151	0,999965988
1200K	0,998388	0,999942927	0,999264007
1500K	0,996411	0,999992287	0,999950518
1800K	0,998569	0,999999858	0,998024458
2100K	0,998232	0,972815171	0,999974875
2400K	0,998994	0,975927501	0,999539984
2700K	0,982732	0,963273812	0,992647648
3000K	0,986727	0,945043077	0,974162317

De uma maneira geral, de acordo com a Figura 6. 7, verificamos que a correlação entre a fragmentação e o tempo de recuperação tende a diminuir à medida que tamanho dos arquivos aumentam. Para arquivos muito grandes, o impacto no tempo de recuperação quando variamos o número de partes em que o arquivo é fragmentação tende a ser reduzido.

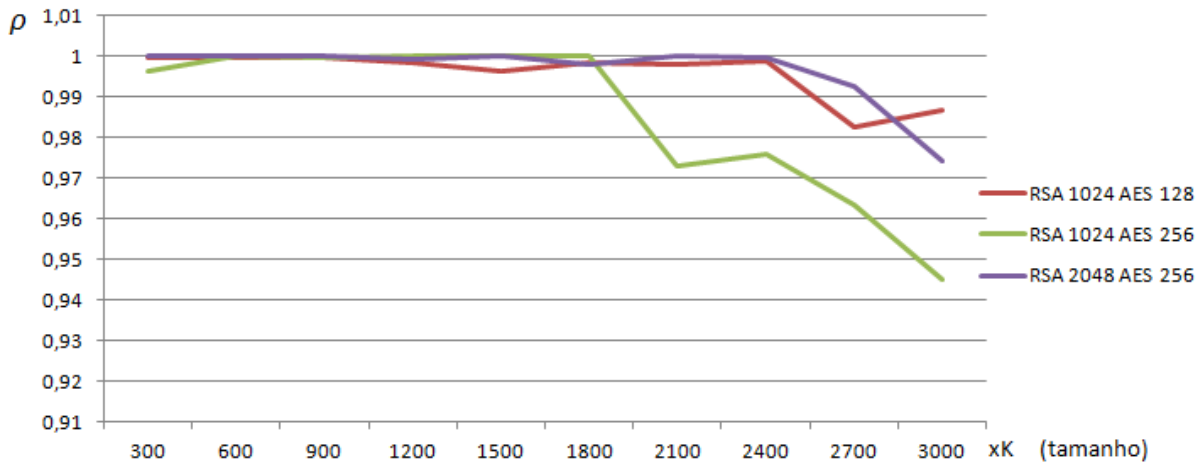

Figura 6. 7. Correlação entre fragmentação do arquivo e tempo de recuperação.

6.4.3 Tamanho das Chaves

Para avaliarmos o quanto os tamanhos das chaves criptográficas influenciam no processo de recuperação, apresentamos abaixo a Figura 6. 8, onde tomamos como exemplo a recuperação de arquivos fragmentados em 4 blocos. Podemos observar que depois de aplicadas as variações de chaves dos algoritmos RSA e AES, os tempos permaneceram bem próximos, não alterando significativamente os tempos de resposta da aplicação.

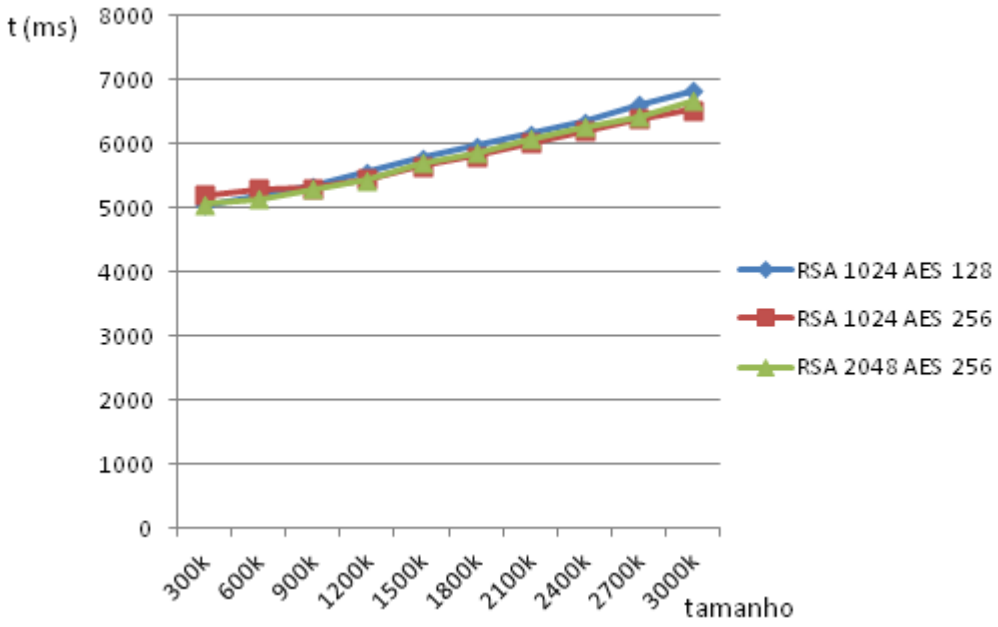

Figura 6. 8. Tempo de recuperação de arquivos (4 fragmentos).

6.5 ARMAZENAMENTO E RECUPERAÇÃO DE ARQUIVOS VIA INTERNET

A Tabela 6.7 apresenta os resultados de testes realizados via Internet (ver apêndice S), pois a idéia principal é a de que a rede seja utilizada para a proteção e salvaguarda de arquivos sigilosos, de tal maneira que os fragmentos dos arquivos sejam replicados e armazenados em pontos geograficamente distintos, garantindo a sua recuperação, caso uma das sedes da organização seja comprometida. Utilizamos o algoritmo RSA com chave 2048 bits e o AES com chave 256 bits, dividindo o arquivo original em três fragmentos.

Tabela 6.7. Tempos de recuperação de arquivos via Internet

RSA 2048 AES 256 (3 fragmentos)						
Tamanho	**Armazenamento**			**Recuperação**		
	Média (ms)	**DP**	**IC (95%)**	**Média (ms)**	**DP**	**IC (95%)**
300k	7778	1608	7280 - 8277	5101	234	5028 - 5174
900k	8951	2476	8183 - 9718	6004	1666	5488 - 6520
1500k	8583	1212	8208 - 8959	6685	1736	6147 - 7223
2400k	9613	1782	9061 - 10165	6451	1266	6059 – 6843
3000k	8959	1661	8444 - 9473	7512	664	7306 – 7718

Tempo em (ms)

Por fim, a Figura 6. 9 apresenta uma comparação gráfica entre os resultados dos testes obtidos em uma rede local e via Internet. Tanto em rede local quanto via Internet, do ponto de vista do usuário que solicita acesso a um documento, o tempo de espera não foi superior a 8s. Cabe salientar que, quando a aplicação está sendo executada em modo autônomo, não há influência significativa no tráfego da rede.

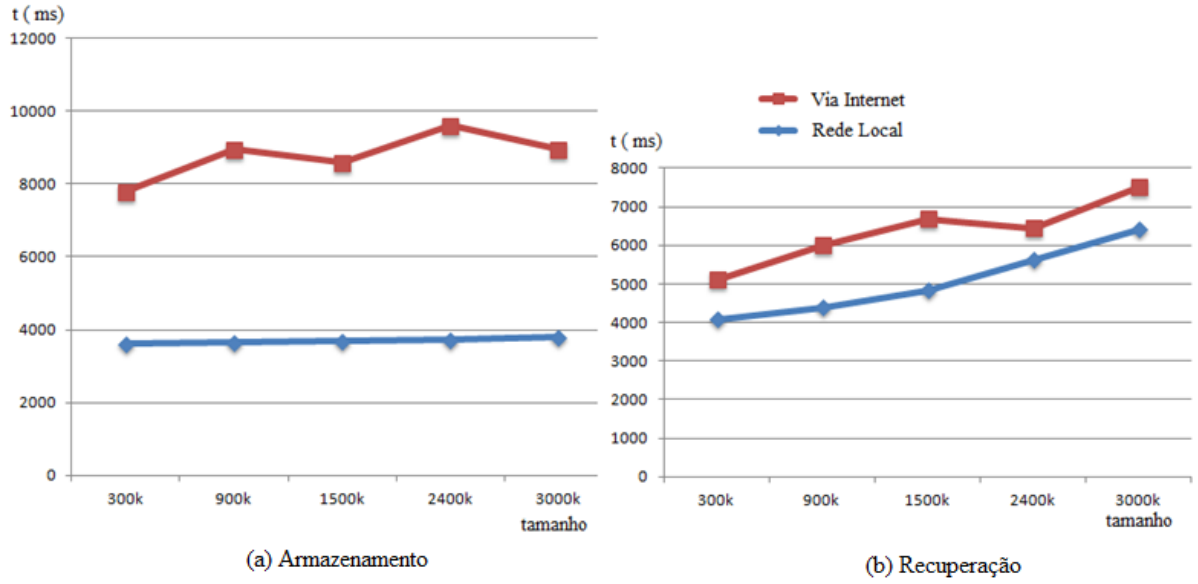

Figura 6. 9. Armazenamento e recuperação em rede local e via Internet.

6.6 CONSIDERAÇÕES FINAIS

Esta seção teve o objetivo de avaliar se a fragmentação dos arquivos em rede (Hipótese 1) e a utilização de um sistema de criptografia híbrida (Hipótese 2) podem ser simultaneamente empregados. Visamos encontrar correlações que indicassem o impacto da

fragmentação e dos tamanhos das chaves criptográficas envolvidas no processo de recuperação da informação.

Os testes realizados serviram para demonstrar a viabilidade da infra-estrutura proposta, em função do tempo de armazenamento e recuperação de arquivos. O tempo de recuperação era o fator mais crítico, pois reflete o intervalo de espera desde a requisição do arquivo até a sua efetiva disponibilidade da máquina do usuário.

Constatamos que o número de blocos no qual o arquivo é fragmentado tem influência significativa no tempo de recuperação dos arquivos. À medida que aumenta o número de fragmentos, cresce também o tempo de espera. O tamanho das chaves criptográficas não tem um peso tão relevante ao levarmos em conta todo o tempo de armazenamento e recuperação. Chaves com tamanhos cada vez maiores tendem a tornar os arquivos mais protegidos, pois inviabilizam o processo de quebra da cifra por parte de um atacante.

A implementação do sistema de reputação proposto e sua aplicabilidade não foram avaliados neste capítulo, pois o tráfego de dados envolvido neste processo é transparente ao usuário, não influenciando significativamente nos tempos de armazenamento e recuperação dos arquivos.

Capítulo 7 – Considerações Finais e Trabalhos Futuros

Neste capítulo é apresentado o resumo da pesquisa descrita nessa dissertação, problemas encontrados e sugestões para prosseguimento do trabalho.

7.1 RESUMO DO TRABALHO

Apresentamos um sistema a ser utilizado por instituições que trabalham com arquivos sigilosos. Sua utilização está voltada para a sobrevivência de informações sensíveis que ficam sujeitas a serem comprometidas quando armazenadas em uma só instituição, caso haja algum dano a esta sede, por isso propomos o modelo de armazenamento em rede denominado *Rede de Confiança*.

A metodologia utilizada vislumbra que o autor de um arquivo possa armazená-lo de uma forma segura, permitindo o seu compartilhamento com um grupo de indivíduos. Além disso, um mecanismo verifica se a reputação de um *peer* que deseja recuperar um arquivo é compatível com o grau de sigilo atribuído ao documento.

De início, realizamos uma pesquisa exploratória com o objetivo de encontrarmos soluções P2P voltadas á segurança da informação. Buscamos trabalhos que apresentassem características que pudessem ser empregadas na concepção desta proposta. Surgiu então o embrião da Rede de Confiança.

A Rede de Confiança utiliza um esquema de criptografia híbrida que combina a segurança da criptografia assimétrica, que utiliza um par de chaves (pública e privada), com a rapidez de processamento da criptografia simétrica. Adicionalmente, os arquivos são arquivados na rede de forma fragmentada, de tal modo que nenhuma máquina possua uma versão integral do arquivo, este procedimento visa minimizar as chances de acesso por um atacante a um arquivo confidencial armazenado na rede.

Descrevemos também a metodologia de um sistema de reputação a ser empregado onde a reputação é levada em consideração por ocasião da solicitação de acesso a um dado armazenado, de tal maneira que quanto maior o sigilo de um arquivo, maior deve ser a reputação do *peer* solicitante.

No decorrer do trabalho, desenvolvemos um protótipo com o intuito de realizar alguns experimentos iniciais que apresentassem indícios da exeqüibilidade da proposta. Realizamos experimentos variando o tamanho das chaves das chaves dos algoritmos utilizados na criptografia e o número de fragmentos no qual um arquivo é dividido por ocasião do seu armazenamento na rede. Para cada uma das possíveis combinações, realizamos 50 rodadas, de onde extraímos as médias desses resultados.

De uma maneira geral, o desempenho da aplicação e o resultado dos testes realizados ficaram dentro de valores considerados satisfatórios, avaliando principalmente a operação de

recuperação dos arquivos, situação mais crítica para os usuários que devem aguardar a recomposição do arquivo solicitado.

Um exemplo da tendência ao uso de redes P2P para o compartilhamento de assuntos sigilosos é o fato da Marinha dos Estados Unidos está financiando o desenvolvimento de uma rede *Onion Routin* para a troca de informações politicamente sensíveis e proteção aos funcionários públicos do setor de inteligência [Global Oneness 2010].

7.2 TRABALHOS FUTUROS

Como trabalhos futuros, planejamos incrementar a idéia proposta nessa dissertação em diferentes fases, até que realmente uma versão final possa ser empregada em uma Organização da esfera federal. Uma das próximas etapas é o aprofundamento no estudo de sistemas de reputação a fim de analisar a alternativa mais viável a ser usada, pois a metodologia aqui exposta serviu apenas didaticamente para apresentar o paradigma do acesso a arquivos com diferentes níveis de sigilo, em função do *status* de reputação apresentado pelos *peers*.

A idéia inicial era realizar testes em uma organização de âmbito nacional que possui várias sedes espalhadas pelo país, entretanto a carga burocrática envolvida no processo de autorização da utilização do protótipo e a dificuldade de envolver participantes para a pesquisa, dentro do prazo atribuído ao Mestrado, impactaram na necessidade de que esta fase seja realizada futuramente.

Vislumbramos também o emprego do sistema de reputação em conjunto como o recurso Honeypot [Huang *et al*. 2009]. A tarefa é utilizar esta solução distribuindo "arquivos-iscas" (arquivos com alto grau de sigilo atribuído) a fim de sondar e coletar informações que levem à identificação de estações de trabalho que apresentem comportamentos maliciosos.

Outra linha de pesquisa é tornar o sistema cada vez mais distribuído. Nesta obra, com o intuito de simplificar a implementação do protótipo usado, utilizamos um servidor para desempenhar dois papéis: o *login* dos usuários e o armazenamento dos *trackers*. O *tracker* armazena os *logs* e o número da porta utilizada pelos usuários que possuem os fragmentos necessários à recomposição de um arquivo. Entretanto, como tendência à total descentralização do sistema, a comunidade BitTorrent é convergente ao emprego de um *hiperlink* conhecido como *link magnético* (*magnet link*), em vez de utilizar um *tracker* tradicional *.torrent*. O link magnético permite que a estação de trabalho obtenha todas as

informações necessárias para o *download* a partir de indexadores espalhados na rede, dispensando a necessidade de servidores [Wolchok e Halderman 2010].

REFERÊNCIAS

ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A.D., KATZ, R.H., KONWINSKI, A., LEE, G., PATTERSON, D.A., RABKIN, A., STOICA, I. e ZAHARIA, M. (2009). "Above the Clouds: A Berkeley View of Cloud Computing". Tech. Rep. UCB/EECS-2009-28, EECS Department, Universidade da Califórnia, Berkeley.

BARCELLOS, M. E GASPARY, L. (2006). "Segurança em Redes P2P: Princípios, Tecnologias e Desafios". In: XXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, p. 211-260, 2006.

BITTORRENT (2010). Disponível em http://www.bittorrent.com. Acessado em 10 de dezembro de 2010.

CARCHIOLO, V., M. MALGERI, G. MANGIONI, e V. NICOSIA (2008). "Emerging structures of P2P networks induced by social relationships". In: Computer Communications Vol. 31,pág. 620-628.

CHEN, J. e JIANG, X. (2010). "Trust-based Robust Mechanism in Peer-to-peer Computing". In: International Conference on E-Business and E-Government (ICEE). pág. 1687 – 1690.

CLARKE, I., SANDBERG, O, WILEY, B. e HONG, T.W. (2001). "Freenet: A Distributed Anonymous Information Storage and Retrieval System". Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability, LNCS 2001.

DABEK, F., KAASHOEK, M. F., KARGER, D., MORRIS, R., E STOICA, I. (2001). "Wide-area cooperative storage with CFS". In: 18th ACM Symposium on Operating Systems Principles, pág. 202-215.

DEVINE, S. (2008) "Danger in the clouds". In: Network Security, Vol.12, p. 9-10. Outubro/2008.

DIFFIE, W. e HELLMAN, M. E. (1976). "Multiuser cryptographic techniques". In: Proc. AFIPS 1976 National Computer Conference, AFIPS Press, pág. 109–112.

DINGLEDINE, R., MATHEWSON, N., e SYVERSON, P. (2004). "Tor: The Second-generation Onion Router". In: Proceedings of the 13th conference on USENIX Security Symposium. Vol. 13, pág. 303–320.

DRUSCHEL, P. e ROWSTRON, A. (2001). “PAST: A large-scale, persistent peer-to-peerstorage utility”. In 8th IEEE Workshop on Hot Topics in Operating Systems, pág. 75–80.

FILHO, F.S.L. (2010). “Mecanismos de segurança para um sistema cooperativo de armazenamento de arquivos baseado em P2P”. Dissertação de Mestrado. Universidade Federal do Rio Grande do Norte.

FREE HAVEN (2010). “The Free Haven Project”. Disponível em http://www.freehaven.net/overview.html. Acessado em 07 de dezembro de 2010.

FREENET (2011). “Freenet. The Free Network Project”. http://freenetproject.org/. Acessado em 27 de janeiro de 2011.

GLOBAL ONENESS (2010) “Uses of anonymous P2P”. Disponível em: http://www.experiencefestival.com/a/Anonymous_P2P_- _Uses_of_anonymous_P2P/id/609575. Acesso em 11 de novembro de 2010.

GOLDSCHLAG, D., REED, M. e SYVERSON, P. (1999). “Onion Routing for Anonymous and Private Internet Connections". In: Communications of the ACM 42(2), pág. 39–41.

GRAFFI, K., MUKHERJEE, P., MENGES, B., HARTUNG, D., KOVACEVIC, A. e STEINMETZ, R. (2009). “Practical security in p2p-based social networks”. In: 34th Annual IEEE Conference on Local Computer Networks (LCN 2009), pág. 269–272.

HUANG, J.-J. , CHANG, S.-C. E HU, S.-Y. (2008). “Searching for Answers Via Social Networks”. In Proc. CCNC, 2008. pág. 289–293.

HUANG, P.S.; YANG, C.H. e AHN, T.N. (2009). “Design and implementation of a distributed early warning system combined with intrusion detection system and honeypot.” In: ICHIT '09 - International Conference on Hybrid Information Technology, pág. 232–238.

KALOGERAKI, V., GUNOPULOS, D. e ZEINALIPOUR-YAZTI, D. (2002). “A local search mechanism for peer-to-peer networks”. In Proc. of the 11th International Conference on Information Knowledge Management, 2002. pág. 300–307.

KAMVAR, S. D., SCHLOSSER, M. T. e GARCIA-MOLINA, H. (2003). “The eigentrust algorithm for reputation management in p2p networks”. In: Proceedings of the 12th international conference on World Wide Web (WWW ’03), pág. 640–651

KUBIATOWICZ, J., BINDEL, D., CHEN, Y., EATON, P., GEELS, D., GUMMADI, R., RHEA, S., WEATHERSPOON, H., WEIMER, W., WELLS, C., e ZHAO, B. (2000). "Oceanstore: An architecture for global-scale persistent storage". In Proceeedings of 9th ACM Architectural Support forProgramming Languages and Operating Systems (ASPLOS), pág 190–201.

MARTI, S. e GARCIA-MOLINA, H. (2006). "Taxonomy of trust: Categorizing p2p reputation systems". In: Computer Networks, 50(4). pág. 472–484.

MONTGOMERY, D. e RUNGER, G. (2009). "Estatística Aplicada e Probabilidade para Engenheiros". Rio de Janeiro: LTC - Livros Técnicos e Científicos Editora S.A., 4ª Ed. p. 109.

NOVOTNY, M. E ZAVORAL, F. (2008). "Reputation-based Methods for Building Secure P2P Networks". In: 1st. International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2008). pág: 403–408.

OCEANSTORE (2010). "The OceanStore Project - Project Overview". Disponível em http://oceanstore.cs.berkeley.edu/info/overview.html. Acessado em 07 de dezembro de 2010.

OLIVEIRA, M. I. S. (2007) "Ourbackup: Uma Solução P2P de Backup Baseada em Redes Sociais". Dissertação de Mestrado. Universidade Federal de Campina Grande.

OLIVEIRA, M., CIRNE, W., BRASILEIRO, F. e GUERRERO, D. (2008). "On the impact of the data redundancy strategy on the recoverability of friend-to-friend backup systems". In: Proceedings of the 26th Brazilian Symposium on Computer Networks and Distributed Systems.

ONTRACK DATA RECOVERY (2011). "Understanding data loss". Disponível em http://www.ontrackdatarecovery.com.au/understandingdataloss/. Acessado em janeiro de 2011.

PARAMESWARAN, M., SUSARLA e A., WHINSTON, A. (2001). "P2P Networking: An Information-Sharing Alternative". In: IEEE Computer, julho 2001, páginas 31–38.

RODRIGUES, R. e B. LISKOV. (2005) "High availability in DHTs: Erasure coding vs. replication". In Proc. of the 4th International Workshop on Peer-to-Peer Systems. Ithaca, NY, páginas 225–239.

SCHOLLMEIER, R. (2001). “A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications”. In Proc. of the 1st International Conference on Peer-to-Peer Computing (P2P '01), Lingkoping, Suécia, pág.101-102.

STEINMETZ, R. E WEHRLE, K. (2005). "Peer-to-Peer Systems and Applications". Ed. Springer, 2005. p. 42

TANENBAUM, A.S. (2003) "Redes de Computadores” 4ª. Ed.”, Editora Campus, pág 54-55.

TRAN, H., HITCHENS, M., VARADHARAJAN, V. e WATTERS, P. (2005). “A trust based access control framework for P2P file-sharing systems”. In: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS’05). IEEE Computer Society, 2005.

TRINTA, F.A.M. e MACÊDO. R.C. (2008). “Um Estudo sobre Criptografia e Assinatura Digital”. Departamento de Informática, universidade Federal de Pernambuco. Disponível em: http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm. Acesso em: 11 de fevereiro de 2011.

WOLCHOK, S. e HALDERMAN, J. A. (2010). “Crawling BitTorrent DHTs for Fun and Profit”. In: Proc. 4th USENIX Workshop on Offensive Technologies.

WU, P e WU, G (2009). “Reputation Mechanism in Peer-to-Peer Network”. In: 1st International Conference on Information Science and Engineering (ICISE 2009). pág: 1793-1796.

YANG, B. e GARCIA-MOLINA, H. (2003). “Designing a Super-Peer Network”. In Proc. of International Conference on Data Engineering (ICDE'03), Bangalore, India.

ZHOU, R. e HWANG, K. (2007). “PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing”. In: IEEE Transactions on Parallel and Distributed Systems, 2007.

Apêndice A – Tempo de Armazenamento RSA 1024 AES 128 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	3666	3744	3729	3759	3807	3837	3807	3853	3853	3853
2	3666	3666	3697	3760	3713	3760	3744	3822	3822	3853
3	3651	3729	3713	3759	3697	3791	3853	3775	3838	3869
4	3650	3666	3728	3713	3697	3697	3806	3869	3900	3916
5	3651	3713	3713	3729	3713	3791	3822	3853	3837	3822
6	3650	3681	3682	4009	3791	3775	3807	3838	3822	3853
7	3650	3682	3728	3713	3728	3759	3790	3807	3807	3838
8	3651	3666	3728	3744	3713	3729	3822	3790	3869	3853
9	3650	3666	3698	3744	3744	3806	3854	3932	3853	3931
10	3651	3697	3712	3759	3744	3775	3790	3822	3806	3822
11	3650	3666	3698	3713	3759	3776	3854	3822	3838	3853
12	3650	3682	3712	3728	3760	3790	3775	3806	3806	3854
13	3651	3681	3713	3729	3744	3822	3884	3853	5866	3884
14	3650	3635	3729	3713	3775	3791	3791	3869	5616	3884
15	3682	3682	3697	3681	3744	3791	3806	3853	3853	3869
16	3635	3993	3728	3729	3729	3760	3791	3775	4774	3869
17	3650	3635	3713	3744	3759	3666	3807	3869	3837	3962
18	3651	3713	3682	3713	3744	3822	3806	3822	3838	3885
19	3650	3682	3713	3712	3729	3775	3775	3791	3775	3900
20	3666	3666	3697	3713	3744	3791	3807	3822	3791	3869
21	3650	3650	3681	3729	3744	3759	3822	3822	3837	3868
22	3666	3697	3682	3744	3728	3791	3790	3822	3854	3869
23	3651	3713	3697	3744	3744	3775	3807	3822	3853	3838
24	3650	3697	3697	3744	3713	3760	3806	3822	3837	3853
25	3651	3713	3682	3728	3760	3744	3838	3806	3838	3838
26	3666	3697	3682	3728	3744	3775	3806	3807	3994	3853
27	4243	3697	3650	3760	3744	3807	3900	3837	3853	3837
28	3650	3635	3697	3728	3759	3790	3807	3635	3806	3869
29	3651	3666	3697	3713	3744	3791	3822	3885	3807	3931
30	3666	3604	3698	3713	3744	3775	3806	3868	3837	3854
31	3650	3666	3775	3728	3760	3791	3807	3838	3807	4680
32	3666	3697	3697	3760	3759	3853	3931	3806	3837	3853
33	3604	3697	3713	3744	3760	3760	3853	3838	3838	3884
34	3634	3619	3713	3728	3728	3806	3822	3806	3806	3838
35	3666	3666	3666	3729	3713	3807	3791	3854	3791	3869
36	3635	3698	3681	3728	3729	3775	3822	3837	3822	3884
37	3666	3681	3744	3713	3712	3775	3791	3838	3900	3853
38	3651	3697	3682	3728	3776	3775	3806	3822	3791	3869
39	3650	3682	3697	3729	3759	3776	3806	3791	3806	3900
40	3650	3697	3682	3713	3760	3775	3791	3822	3854	3853
41	3620	3697	3744	3728	3744	3759	3822	3915	3853	3900
42	3650	3635	3681	3713	3728	3776	3807	3838	3791	3838
43	3650	3682	3666	3713	3760	3775	3790	3853	3853	3838
44	3651	3681	3713	3712	3744	3791	3791	3853	3822	3853
45	3650	3698	3994	3744	3759	3775	3822	3791	3931	3884
46	3651	3666	3697	3713	3729	3806	3807	3822	3853	3853
47	3666	3650	3681	3729	3744	3791	3806	3807	3807	3838
48	3666	3666	3682	3728	3744	3822	3822	3790	3868	3838
49	3650	3666	3682	3729	3759	3775	3822	3822	3932	3900
50	3666	3682	3697	3744	3760	3775	3791	3838	3790	3806
Média	3664,14	3684,74	3707,2	3734,96	3743,7	3780,18	3813,9	3827	3933,38	3881,6

Apêndice B – Tempo de Armazenamento RSA 1024 AES 128 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	5241	4868	4868	6100	4914	6193	4992	4977	5038	4992
2	4790	4820	4867	4914	4914	4961	4929	5007	4961	5055
3	4820	4852	4851	4883	4852	4914	4977	4961	4961	4992
4	4758	4867	4836	4836	4914	4914	4961	4945	4961	4976
5	4805	4820	4883	4836	4961	4945	5070	4977	5039	4821
6	4805	4836	4836	4882	4914	4961	4945	4961	5070	5007
7	4773	4821	4867	4868	4914	4898	4976	5288	4976	4992
8	5180	4804	4868	4976	4883	4930	4977	4976	5008	5008
9	5070	4805	4836	4883	4898	4945	4992	4977	5007	4961
10	4820	4789	4867	5117	4883	4930	4960	4945	5008	5039
11	4820	4836	4836	4882	4930	4914	4930	4977	5023	5023
12	4821	4821	4883	4914	4898	4929	4961	4976	4961	5039
13	4867	4774	4867	4930	4883	4930	4945	4992	5039	5101
14	4820	4976	4836	4867	4898	4898	4961	4961	4992	5007
15	4790	4883	4836	4883	4930	4711	4961	4961	4960	4992
16	4804	4820	4851	4836	4945	4961	4960	5007	4977	5008
17	4774	4852	4836	4883	4867	4992	4992	4930	5007	5008
18	4805	4836	4836	4883	4930	4961	4946	5007	5024	5038
19	4758	4820	4852	4867	4883	4945	4882	4977	4960	5039
20	4820	4789	4852	4898	4882	4930	4946	4976	6225	5023
21	4821	4836	4836	4852	4914	4914	4945	4992	5039	4977
22	4804	4883	4836	4789	4914	4914	4976	5008	5023	5023
23	4790	4914	4867	4930	4868	4883	4977	4789	4789	5023
24	4789	4821	4898	4898	4882	4929	4898	4992	4977	4992
25	4820	4820	4852	4852	4899	4930	4914	4961	5007	5055
26	4836	4852	4867	4867	4898	4914	4883	4961	5023	5070
27	4821	4820	4867	4836	4930	4930	4976	4960	5008	5023
28	4820	4976	4883	4820	4883	4945	4946	4930	5101	5023
29	4805	4821	4852	5039	4898	4961	4945	4976	4992	5008
30	4758	4805	4883	4852	4914	4960	4929	4992	5039	5023
31	4774	4789	4882	4867	4867	4899	4977	4946	4961	5039
32	4773	4820	4805	4914	4914	4961	4992	4992	5007	4992
33	4852	4821	4883	4867	4899	4929	4929	4992	4992	5007
34	4820	5023	4852	4821	4867	4696	4961	4992	5070	5039
35	4789	4820	4867	4882	4883	4961	4883	4945	5070	5055
36	4852	4821	4820	4868	4898	4914	4945	4992	4992	5038
37	4758	4820	4789	4898	4883	4976	4961	5008	4977	5039
38	5522	4805	4836	4836	4867	4930	4992	4945	4992	5039
39	4883	4805	4852	4898	4883	4945	4961	4976	4789	5117
40	4836	4836	4805	4899	4914	4961	4976	4821	4992	4976
41	4836	4820	4820	4602	4898	4882	4961	5038	5008	5070
42	5023	5195	4883	4836	5133	4883	4930	5008	4992	5039
43	4961	4852	4820	4883	4883	4914	4929	4976	5007	5039
44	4789	4789	4868	4867	4914	5211	4961	4992	4992	5023
45	4883	4805	4882	4852	4898	4929	4945	4992	4992	5008
46	4821	4820	4634	4851	4898	4946	5008	4946	4961	4992
47	4820	4867	4851	4852	4946	4929	5039	4945	4977	4992
48	4820	4867	4821	4898	4929	4945	4961	4961	5023	4976
49	4868	4852	4867	4852	4852	4930	4914	4976	5070	4992
50	4804	4820	4852	4867	4945	4914	4960	4976	4945	5039
Média	4853,78	4845,68	4847,88	4899,66	4905,28	4953,94	4956,74	4975,16	5020,08	5016,98

Apêndice C – Tempo de Armazenamento RSA 1024 AES 128 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	7987	6038	6037	6006	7597	7878	6053	6115	8159	7706
2	5975	5881	5975	5912	5975	5943	6037	6069	6068	6069
3	5975	5975	6006	5975	6177	5959	5975	6084	6084	6115
4	5928	5881	5959	5959	6022	6022	6069	6037	6069	6053
5	5912	5944	5912	5928	5928	6412	6006	6068	6021	6084
6	6006	5943	5928	5913	5928	6006	6021	6084	6100	6100
7	5944	5975	5913	6037	6053	5959	6053	6038	6022	6037
8	5912	5959	5928	5990	5928	6131	6037	5990	6021	6068
9	5913	5944	5959	5959	5943	6006	6053	6053	6069	6084
10	6068	5897	5912	5975	6131	5990	5990	6068	6286	6084
11	5959	5959	5897	5944	6006	6302	6069	6084	6100	6084
12	5944	5959	5959	6037	5928	6084	6021	6037	6022	6069
13	5975	5959	5897	6006	6006	5960	5991	5975	6068	6084
14	5881	5881	5928	6006	5959	5974	6006	6006	5991	6177
15	5959	5928	5928	5944	5960	5991	6006	6006	6021	6256
16	5913	5913	5928	5990	5974	6037	6006	6053	6069	6146
17	5943	5928	5928	5959	6006	5991	6053	6022	6021	6147
18	6100	5959	5850	5991	5960	5959	6006	6021	6053	6052
19	5990	5959	5913	5959	5990	5990	6084	5975	6084	6069
20	5960	5928	5928	6022	5959	5975	6037	6037	6115	6037
21	5974	5897	5943	5974	5991	5990	6412	6069	6100	6115
22	5913	5975	5928	5944	6021	5991	5974	6068	6068	6069
23	5881	5897	5913	6006	6022	5990	6038	6037	6084	6084
24	5928	5943	5928	5944	5928	5991	6037	6053	5991	6084
25	5975	5960	5975	5943	6022	6037	6021	6006	6037	6084
26	5990	5943	5959	5944	5974	5975	7629	6053	6037	6131
27	5944	5959	5943	6006	5944	6115	6099	6068	6022	6146
28	5990	5991	5913	5959	5990	6006	5975	6069	6099	6084
29	6271	5959	5959	5990	5960	5990	6069	6053	6084	6068
30	5897	5928	5897	5975	5928	6037	6037	6052	6037	6131
31	5944	5897	5897	5975	5943	6038	6053	6069	6069	6131
32	5912	5943	5928	6006	6131	6006	6037	6053	6084	6068
33	5975	5882	5912	5944	5990	5959	5990	6240	6100	6084
34	5944	5928	5928	5990	6131	5944	6053	6084	6084	6100
35	5990	5912	5975	5991	5975	5974	6022	6021	6099	6100
36	5881	5919	5897	5928	7426	5991	6037	6084	6147	6068
37	5913	5959	5943	5943	5959	5990	5959	6038	6208	6115
38	5990	5969	5960	5959	5990	5991	5990	6068	6053	6084
39	5975	5944	5974	5960	6006	6021	5991	6053	6037	6100
40	5975	5959	5991	6006	6225	5991	6022	5990	6100	6084
41	5912	5991	5897	5974	6037	5974	6037	6037	6037	6177
42	5913	5834	5928	5928	6099	5991	6037	6022	6053	6069
43	6021	5944	5881	5960	5944	6021	6006	6053	6053	6084
44	6209	5943	5912	5959	6037	5991	6100	6068	6115	6100
45	5928	5944	5928	6021	6225	5943	6006	6053	6068	6068
46	5990	5943	5959	5928	5943	6006	5990	6037	6084	6131
47	6006	5882	5913	5960	5991	5991	6022	6037	6069	6068
48	5928	5943	5975	5959	5959	6021	5974	5991	6068	6100
49	5897	5944	5990	5959	5944	5960	6006	6053	6069	6115
50	5944	5881	5897	5990	7519	6021	6022	6068	6068	6084
Média	6005,08	5936,46	5934,56	5970,74	6093,68	6050,3	6064,36	6049,38	6113,34	6128,94

Apêndice D – Tempo de Armazenamento RSA 1024 AES 256 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	3591	3595	3607	4522	3811	3674	3689	3732	3733	3768
2	3581	3576	3635	3647	3648	3675	3684	3774	3714	3745
3	3563	3588	3606	3612	3630	3661	3679	3737	3756	3737
4	3541	3582	3618	3617	3626	3693	3676	3748	3720	3743
5	3536	3591	3604	3600	3652	3642	3681	3705	3724	3753
6	3562	3572	3596	3605	3684	3667	3665	3706	3737	3748
7	3545	3567	3622	3608	3645	3647	3715	3708	3732	3739
8	3580	3571	3583	3604	3624	3647	3684	3702	3737	3731
9	3535	3570	3597	3609	3645	3646	3663	3690	3744	3793
10	3549	3572	3602	3602	3625	3663	3677	3688	3714	3736
11	3550	3567	3586	3608	3652	3677	3675	3690	3720	3745
12	3543	3567	3579	3622	3642	3657	3695	3744	3749	3725
13	3543	3567	3614	3621	3636	3671	3686	3696	3709	3760
14	3553	3600	3595	3608	3654	3649	3709	3696	3728	3756
15	3541	3575	3599	3629	3630	3664	3804	3708	3730	3745
16	3736	3583	3604	3627	3638	3662	3689	3842	3716	3779
17	3581	3563	3603	3637	3667	3698	3682	3698	3731	3791
18	3535	3562	3602	3606	3637	3686	3735	3695	3726	3740
19	3543	3604	3605	3608	3659	3634	3680	3681	3741	3743
20	3534	3568	3574	3608	3630	3659	3682	3695	3720	3758
21	3573	3570	3611	3610	3642	3657	3699	3700	3783	3776
22	3543	3571	3595	3628	3626	3653	3666	3776	3785	3748
23	3533	3563	3595	3604	3673	3660	3707	3686	3758	3771
24	3563	3575	3594	3606	3657	3645	3676	3707	3714	3765
25	3553	3568	3577	3632	3643	3672	3669	3699	3728	3832
26	3544	3585	3655	3617	3629	3661	3708	3700	3727	3766
27	3584	3585	3591	3622	3612	3681	3682	3701	3737	3746
28	3592	3581	3587	3760	3627	3833	3695	3710	3708	3742
29	3563	3585	3586	3602	3624	3663	3727	3705	3724	3759
30	3557	3554	3592	3608	3654	3696	3683	3697	3754	3749
31	3570	3573	3585	3590	3637	3645	3673	3710	3767	3766
32	3558	3565	3573	3602	3647	3645	3678	3733	3740	3738
33	3541	3562	3601	3600	3629	3647	3711	3688	3708	3804
34	3574	3586	3604	3601	3651	3643	3668	3697	3727	3770
35	3550	3592	3589	3631	3635	3643	3688	3720	3725	3751
36	3539	3576	3573	3610	3626	3664	3704	3714	3708	3750
37	3567	3575	3627	3640	3625	3660	3677	3688	3715	3790
38	3567	4056	3602	3614	3636	3658	3682	3704	3713	3750
39	3554	3570	3585	3633	3632	3639	3676	3692	3761	3752
40	3542	3555	3604	3636	3623	3668	3726	3705	3750	3745
41	3533	3560	3611	3624	3674	3646	3677	3700	3726	3811
42	3534	3583	3608	3621	3635	3657	3688	3750	3866	3766
43	3551	3601	3632	3614	3626	3708	3674	3720	3756	3751
44	3544	3586	3605	3609	3637	3660	3681	3707	3722	3768
45	3540	3609	3612	3639	3634	3650	3679	3696	3721	3749
46	3576	3578	3603	3624	3650	3664	3680	3685	3717	3739
47	3593	3565	3585	3633	3638	3667	3668	3707	3745	3732
48	3532	3555	3614	3614	3646	3661	3671	3707	3754	3763
49	3545	3569	3581	3603	3651	3646	3703	3686	3714	3779
50	3563	3585	3574	3608	3622	3667	3697	3695	3726	3755
Média	3558,4	3585,56	3599,64	3636,7	3643,52	3664,62	3689,26	3710,4	3735,2	3758,36

Apêndice E – Tempo de Armazenamento RSA 1024 AES 256 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	3768	4718	4743	4748	4767	4800	4791	5159	4830	4886
2	3745	4664	4723	4724	4768	4769	4795	4799	4663	4853
3	3737	4749	4696	4711	4754	4752	4790	4825	4854	4917
4	3743	4683	4706	4712	4728	4768	4806	4822	4941	4834
5	3753	4689	4728	4738	4766	4774	4790	4866	4870	4644
6	3748	4680	4714	4744	5099	4772	4821	4844	4844	4889
7	3739	4660	4711	4740	4741	4911	4823	4836	4819	4872
8	3731	5577	4730	4721	5662	5088	4863	4833	4837	4919
9	3793	4670	4708	4701	4756	4757	4816	4854	4845	4884
10	3736	4701	4706	4727	4768	4760	4807	4841	4889	4876
11	3745	4717	4693	4733	4802	4780	4780	4836	4831	4871
12	3725	4669	4725	4718	4752	4752	4797	4806	4858	4866
13	3760	4681	4702	4742	4738	4764	4797	4818	4832	4897
14	3756	4681	4693	4718	4719	4767	4836	4833	6046	4861
15	3745	4710	5023	4772	4770	4776	4798	4846	4850	4885
16	3779	4701	4702	4765	4758	4757	4784	4899	4838	4873
17	3791	4480	4709	4736	4747	4754	4811	4865	4847	4881
18	3740	4681	4714	4737	4737	4768	4814	4839	4851	4859
19	3743	4674	4711	4704	4735	4766	4793	4840	4844	4892
20	3758	4682	4698	4754	4767	4764	4826	4832	4656	4882
21	3776	4702	4700	4735	4750	4755	4780	4834	4848	4876
22	3748	4688	4700	4718	4734	4579	4818	4828	4862	4651
23	3771	4667	4731	4713	4773	4776	4773	4822	4855	4839
24	3765	4683	4504	4732	4735	4747	4768	4801	4842	4866
25	3832	4709	4699	4715	4748	4817	4794	4805	4825	4878
26	3766	4680	4704	4742	4559	4784	4795	4825	4850	4846
27	3746	4679	4682	4747	4732	4792	4814	4829	4828	4865
28	3742	4692	4681	4726	4749	4768	4806	4835	4834	4874
29	3759	4696	4698	4755	4736	4757	4783	4829	4827	4874
30	3749	4681	4705	4709	4730	4779	5079	4789	4842	4898
31	3766	4669	4713	4706	4745	4772	4799	4818	4855	4844
32	3738	4698	4708	4720	4735	4769	4798	4877	4830	4866
33	3804	4672	4708	4720	4741	4768	4809	4913	4834	4843
34	3770	4661	4734	4744	4760	4769	4786	4801	4890	4856
35	3751	4688	4699	4764	4761	4754	4785	4843	4858	4833
36	3750	4699	4711	4730	4732	4776	4804	4841	4832	4889
37	3790	4718	4686	4758	4772	4767	4794	4855	4861	4879
38	3750	4672	4690	4715	4739	4787	4789	4797	4847	4836
39	3752	4692	4691	4715	4760	4785	4789	4803	4863	4652
40	3745	4689	4701	4717	4752	4790	4796	4819	4830	4853
41	3811	4677	4714	4736	4756	4760	4796	4820	4828	4888
42	3766	4676	4694	4701	4746	4774	4794	4814	4829	4890
43	3751	4714	4690	4730	4742	4785	4806	4817	4848	4876
44	3768	4679	4707	4760	4738	4567	4780	4795	4837	4856
45	3749	4694	4706	4738	4713	4884	4791	4817	4850	4869
46	3739	4483	4702	4719	4754	4783	4794	4809	4887	4860
47	3732	4701	4687	4712	4746	4772	4796	4878	4863	4849
48	3763	4690	4707	4708	4766	4800	4786	4811	4818	4834
49	3779	4702	4714	4706	4759	4778	4808	4788	4848	4863
50	3755	4677	4720	4729	4766	4780	4834	4802	4822	4881
Média	3758,36	4697,9	4708,42	4729,3	4771,26	4775,46	4805,64	4836,16	4863,76	4856,5

Apêndice F – Tempo de Armazenamento RSA 1024 AES 256 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	6850	5920	5997	6016	7559	6043	6069	6115	6084	7920
2	5835	5847	5884	5893	5907	5912	5850	6116	6131	6058
3	5837	5847	5902	5931	5892	5921	6162	6115	6099	6033
4	5841	5861	5888	5932	5897	5924	6068	6115	6131	5979
5	5870	5855	6039	5906	5890	5903	6084	6115	6084	5975
6	5832	5891	5880	5893	5944	5932	6100	6084	6178	6009
7	5840	5851	5864	5897	5912	5926	6099	6115	6146	6008
8	5816	5837	5903	5932	5905	5897	6022	6069	6162	5999
9	5848	5856	5881	5876	5896	5888	6037	6053	6069	5979
10	5836	5862	5879	5871	5890	5925	5991	6177	6099	5986
11	5824	5838	5985	5905	5887	5901	6052	6038	6162	6019
12	5930	5944	6158	5997	5932	6037	6038	6115	6131	6364
13	5836	5883	5944	5921	5869	5903	5990	6068	6068	5998
14	5837	5844	5885	5888	5897	5921	6053	6069	6069	6000
15	5844	5838	5892	5918	5882	5911	6037	6084	6099	6008
16	5837	5854	5894	5890	5886	5917	6068	6099	7691	5997
17	5826	5907	5867	5863	5971	5916	6006	6069	6084	5983
18	5841	5844	5883	5897	5876	5927	6022	6115	6100	6055
19	5845	5842	5879	5949	5859	5898	6053	6084	6115	6031
20	5851	5867	5895	5877	5896	5900	6021	6084	6053	6039
21	5956	5908	5904	5892	5908	5901	6069	6099	6131	5999
22	6027	5832	5893	5910	5885	5928	6084	6147	6099	5963
23	5965	5946	5965	6026	5928	5992	6053	6084	6162	5974
24	5982	5869	5875	5898	5895	5906	6037	6115	6084	6009
25	5973	5856	5886	5885	5881	5888	6053	6084	6147	5976
26	5881	5851	5856	5947	5891	5912	6037	6068	6130	6005
27	5854	5837	5863	5920	5899	5912	6100	6069	6100	6012
28	5841	5872	5853	5896	5946	5875	6052	6084	6178	5996
29	5835	5840	5858	5896	5871	5901	6038	6100	6302	6020
30	6164	5845	5883	5877	5879	5901	5998	6115	6100	6044
31	5868	5858	5890	5875	5899	5901	6100	6458	6131	6041
32	5995	5868	5879	5924	5918	5908	6131	6053	6146	5995
33	5860	5829	5885	5979	5902	5891	6053	6068	6100	5974
34	5977	5934	5951	7515	5933	7539	6068	6084	6099	6062
35	5859	5866	5889	5900	5894	5894	6100	6069	6115	5989
36	6071	5856	5888	5876	5891	5927	6130	6084	6116	6031
37	5873	5851	5876	5929	5904	5923	6038	5819	6115	5994
38	5850	5852	5859	5900	5906	5916	6115	6068	6099	5991
39	5856	5864	5878	6018	5955	5966	5772	6084	6069	5990
40	5852	5861	5885	5878	5914	5905	6053	6115	6131	5976
41	5820	5856	5877	5868	5903	5926	6099	6100	6099	6014
42	5882	5856	5892	5890	5888	5897	6006	6162	6131	6010
43	5855	5846	5883	5883	5890	5910	6100	5990	6068	5971
44	5652	5838	5855	6082	5892	5894	6115	6022	6100	5981
45	5976	5951	5994	5938	5935	5946	6115	6131	6131	5983
46	5858	5865	5862	5925	5887	5908	6069	6099	6131	6001
47	5853	5837	5864	5899	5880	5888	6084	6038	6068	5784
48	5830	6122	5895	5893	5908	5899	6037	6052	6069	6023
49	5882	5853	5856	5883	5901	5903	6037	6116	6130	5985
50	5847	5872	5855	5929	5991	5970	6053	6037	6100	6057
Média	5897,4	5869,58	5898,96	5947,66	5936,42	5950,58	6052,36	6090,26	6146,72	6045,8

Apêndice G – Tempo de Armazenamento RSA 2048 AES 256 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	4034	3664	3676	3723	3719	3653	3796	3717	3733	4405
2	3562	3592	3629	3680	3652	3657	3671	3722	3765	3758
3	3573	3668	3649	3651	3713	3666	3700	3741	3786	3740
4	3594	3620	3624	3690	3704	3653	3678	3697	3744	3758
5	3583	3585	3653	3656	3698	3642	3719	3708	3777	3735
6	3587	3597	3616	3656	3671	3653	3719	3744	3727	3733
7	3609	3606	3641	3687	3668	3726	3684	3702	3570	3866
8	3582	3611	3632	3664	3680	3652	3669	3717	3735	3756
9	3575	3617	3797	3659	3670	3676	3701	3703	3734	3747
10	3570	3579	3646	3671	3694	3652	3682	3693	3779	3832
11	3592	3655	3624	3664	3692	3648	3674	3706	3787	3733
12	3673	3632	3634	3643	3648	3683	3675	3711	3731	3801
13	3643	3625	3646	3643	3691	3739	3701	3737	3767	3760
14	3583	3602	3619	3631	3670	3717	3684	3705	3819	3734
15	3712	3611	3704	3690	3661	3661	3765	3708	3747	3851
16	3603	3596	3621	3652	3675	3662	3775	3696	3737	3750
17	3565	3603	3633	3672	3688	3653	3698	3690	3767	3753
18	3595	3726	3750	3673	3789	3688	3737	3727	3737	3781
19	3580	3603	3653	3647	3670	3660	3708	3696	3772	3745
20	3575	3626	3621	3684	3678	3697	3686	3700	3755	3813
21	3589	3611	3622	3654	3683	3795	3678	3696	3775	3748
22	3578	3630	3649	3456	3688	3743	3688	3701	3807	3778
23	3577	3626	3641	3637	3691	3685	3688	3751	3746	3776
24	3585	3625	3658	3653	3679	3657	3694	3726	3738	3863
25	3553	3599	3631	3652	3924	3771	3698	3777	3771	3736
26	3575	3590	3622	3695	3697	3662	3680	3690	3754	3816
27	3583	3615	3616	3631	3681	3661	3693	3720	3550	3756
28	3571	3619	3628	3704	3700	3742	3703	3723	3777	3770
29	3583	3611	3631	3665	3678	3840	3699	3708	3724	3743
30	3610	3693	3617	3659	3688	3682	3714	3739	3742	3768
31	3564	3604	3653	3666	3677	3670	3687	3731	3807	3797
32	3544	3607	3617	3665	3686	3660	3716	3705	3732	3745
33	3581	3581	3630	3654	3686	3908	3667	3746	3752	3747
34	3593	3606	3653	3657	3672	3690	3698	3734	3736	3807
35	3564	3728	3635	3679	3679	3678	4293	3764	3829	3750
36	3576	3613	3626	3659	3689	3646	3688	3718	3756	3748
37	3600	3623	3636	3664	3668	3660	3695	3702	3782	3783
38	3597	3594	3643	3653	3703	3665	3685	3707	3747	3756
39	3574	3602	3620	3664	3702	3653	3692	3700	3726	3740
40	3580	3600	3642	3653	3717	3673	3711	3701	3748	3760
41	3585	3633	3656	3661	3687	3673	3750	3700	3735	3768
42	3704	3613	3641	3662	3667	3694	3809	3709	3728	3830
43	3560	3589	3631	3673	3680	3669	3677	3724	3754	3761
44	3635	3620	3641	3651	3474	3682	3668	3715	3732	3841
45	3593	3616	3621	3653	3683	3662	3693	3704	3744	3755
46	3575	3610	3622	3659	3695	3665	3694	3688	3769	3742
47	3678	3602	3630	3664	3676	3662	3677	3691	3750	3748
48	3599	3613	3725	3641	3712	3657	3676	3700	3754	3758
49	3587	3600	3656	3642	3681	3650	3675	3716	3750	3827
50	3590	3594	3628	3737	3681	3670	3684	3742	3748	3792
Média	3601,46	3617,7	3643,78	3659,98	3687,1	3685,26	3711,84	3714,96	3748,64	3785,2

Apêndice H – Tempo de Armazenamento RSA 2048 AES 256 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	5887	4557	4751	4768	4750	4797	4847	4844	4889	4900
2	4692	4799	4748	4794	4740	4777	4879	4869	4857	4917
3	4685	4709	4929	4762	4758	4794	4915	4872	4941	5007
4	4672	4716	4749	4755	4743	4778	4833	4871	4887	4910
5	4693	4719	4734	4749	4749	4774	4915	4894	4886	4892
6	4706	4718	4745	4753	4755	4802	4854	4867	4882	4910
7	4780	4748	4745	4763	4792	4766	4870	4859	4968	4932
8	4703	4765	4760	4760	4802	4808	4846	4859	4893	4886
9	4742	4715	4737	4765	4762	4781	4866	4864	4871	5069
10	4684	4720	4763	4762	4778	4848	4814	4910	4909	4913
11	4681	4719	4742	4759	4778	4789	4835	5025	4889	4900
12	4702	4709	4748	4789	4792	4795	4847	4844	4876	4883
13	4676	4718	4758	4602	4738	4825	4840	4881	4869	4889
14	4696	4720	4747	4737	4766	4785	4847	4871	4964	4907
15	4683	4743	4727	4787	4762	4805	4827	4864	4875	4920
16	4704	4715	4742	4756	4744	4792	4873	4887	4874	4892
17	4762	4699	4746	4751	4891	4795	4863	4859	4884	5147
18	4685	4778	4735	4784	4764	4825	4815	4978	4869	4924
19	4684	4748	4729	4776	4841	4782	4826	4868	4968	4888
20	4716	4716	4734	4773	4767	4780	4827	4870	4905	4886
21	4697	4734	4756	4798	4784	4778	4839	4843	4887	4911
22	4705	4715	4749	4766	5996	4779	4838	4876	4879	4889
23	4690	4694	4767	4789	4729	4811	4916	4875	4885	4951
24	4669	4729	4715	4755	4756	4800	4829	4858	4863	4913
25	4662	4717	4735	4769	4743	4802	4835	4858	4704	4951
26	4693	4711	4734	4758	4753	4794	4948	4854	4856	4882
27	4697	4706	4754	4749	4753	4834	4844	4845	4868	4888
28	4727	4713	4728	4818	4801	4794	4997	5202	4956	5048
29	4704	4731	4764	4769	4776	4801	4815	4856	4857	4921
30	4665	4709	4708	4758	4754	4810	4839	4862	4874	4924
31	4680	4719	4730	4785	4783	4804	4847	4874	4885	5008
32	4732	4699	4742	4765	4629	4805	4819	4922	4854	4926
33	4697	4739	4758	4567	4780	4775	4823	4855	4965	4909
34	4672	4719	4742	4884	4763	4782	4856	4843	4882	4906
35	4697	4690	4745	4732	4807	4773	4835	4849	4856	4946
36	4703	4719	4755	4768	4783	4789	4933	4848	4882	4949
37	4674	4719	4760	4795	4780	4794	4846	4842	4863	4899
38	4688	4722	4709	4776	4759	4773	4829	4862	4990	5003
39	4646	4708	4746	4776	4746	4596	4834	4849	4859	4892
40	4720	4726	4740	4879	4778	4782	4814	4856	4872	4907
41	4683	4717	4824	4784	4787	4901	4844	4858	4996	4896
42	4755	4733	4770	4800	4946	4830	4854	4897	4922	5010
43	4682	4788	4752	4777	4760	4820	4856	4863	4908	4901
44	4683	4699	4773	4774	4855	4808	4816	4868	4873	4904
45	4676	4741	4738	4789	4786	4785	4852	4848	4861	4880
46	4706	4707	4742	4772	4767	4787	4848	4890	4863	4905
47	4686	4698	4740	4783	4748	4815	4819	4868	4862	4907
48	4671	4739	4705	4771	4758	4814	4840	4863	4870	4919
49	4692	4698	4721	4787	4759	4784	4829	4945	5177	4943
50	4684	4740	4762	5982	4757	4787	4829	4844	4893	4897
Média	4719,38	4720,2	4748,66	4792,4	4796,96	4794,1	4851,24	4878,58	4894,36	4927,14

Apêndice I – Tempo de Armazenamento RSA 2048 AES 256 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	6107	6150	7351	6204	6001	5960	6083	6015	6066	7981
2	5852	5827	5888	5869	5994	5927	5964	5997	6026	5990
3	5810	5824	5887	5873	5889	5936	5981	5980	6031	6039
4	5782	5867	5860	5867	5912	5927	5968	6025	6013	6040
5	5792	5820	5868	5901	5896	5931	5966	5993	6135	6008
6	5614	5923	5848	5855	5913	5925	6029	5857	6019	5996
7	5782	5830	5853	6038	5915	5940	5958	6039	6028	6012
8	5782	5793	5841	5888	5887	5906	5945	5993	5982	6006
9	5783	5903	5865	5887	5941	5938	6016	6004	6018	6013
10	5802	5845	5869	5904	5886	5968	5785	6015	6027	5988
11	5802	5809	5830	5880	5912	5984	5981	5985	6014	5982
12	5823	5928	5863	5878	5912	5766	5975	5974	6012	5996
13	5842	5845	5856	5890	5917	5933	5979	6000	6024	6148
14	5826	5813	5846	6003	5904	6022	5963	5996	5988	5995
15	5809	5821	5853	5893	5893	5924	5975	6002	5998	6002
16	5790	5831	5848	5874	5894	5968	5977	6029	5969	6009
17	5865	5825	5862	5888	5892	5923	5962	6014	6002	6005
18	5793	5850	5898	5855	5902	5928	5996	6006	6056	6043
19	5792	5803	5851	5874	5911	5920	6080	6029	6163	6002
20	5802	5825	5831	5883	5937	5897	5983	5997	6019	6016
21	5784	6016	5848	5876	5933	5938	6065	5841	6041	6007
22	5802	5849	5881	5888	5903	5954	5977	6005	6023	6000
23	5802	5903	5865	5887	5891	5972	5962	5990	6058	6024
24	5823	5866	5856	5887	5923	5945	5963	6029	6033	6009
25	5802	5816	5848	5900	5903	5990	5984	5997	6020	6023
26	5848	5811	5858	5878	5916	5921	6005	6024	6003	6002
27	5812	5834	5919	5907	5992	5919	5951	6083	6033	5984
28	5834	5844	5879	5883	5902	5930	5965	6003	6052	6005
29	5833	5822	5849	5850	5871	5953	5930	5965	6037	5987
30	5801	5802	5854	5874	5962	5937	5983	5995	6010	5993
31	5802	5805	5875	5884	5900	5955	6008	6035	6012	6040
32	5793	5834	5844	5899	5909	6034	5993	6000	6010	6028
33	5813	5848	5847	5991	5888	5927	5977	6302	6016	5988
34	5822	5823	5868	5867	5889	5956	5965	6034	6018	6017
35	5792	5827	5842	5871	5932	5955	5939	5985	6009	6108
36	5883	5814	5878	5869	5922	5939	5929	5988	6004	6026
37	5792	5812	5852	5859	5915	5930	6061	5998	6016	6093
38	5812	5847	5846	5939	5924	5891	5985	5997	6007	6003
39	5815	5830	5840	5872	5898	5936	5996	5985	6026	5998
40	5781	5826	5885	5788	5899	5924	5989	6043	6016	5985
41	5812	5812	5843	5906	5960	5929	5767	5998	5835	5990
42	5823	5824	5860	5884	5908	5941	5997	5983	6061	5982
43	5823	5832	5881	5878	5927	5924	6084	5995	6034	6047
44	5820	5823	5847	5884	5909	5917	5992	5975	6013	6012
45	5810	5832	5891	5870	5960	5931	6140	6010	6060	5980
46	5793	5846	5882	5907	5897	5927	6006	5995	6030	6025
47	5826	5831	5854	5864	5900	5932	5959	5990	6030	6057
48	5882	5872	5890	5969	5899	5959	5974	5994	6027	6055
49	5913	5815	5857	5870	5922	5925	5984	6015	6011	5991
50	5797	5847	5873	5880	5898	5904	5995	5999	6024	5993
Média	5815,9	5845,9	5891,6	5895,7	5915,2	5936,36	5981,82	6004,06	6023,18	6054,46

Apêndice J – Tempo de Recuperação RSA 1024 AES 128 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	4047	4305	4513	4598	5058	5493	5917	5408	5856	6082
2	3919	4357	4648	4505	4882	5116	5561	5594	5789	6137
3	4172	4279	4455	4511	4657	4845	5287	5372	5858	5945
4	3961	4191	4687	4609	4679	5014	5294	5578	5791	6032
5	4053	4231	4558	4475	4821	5014	5309	5808	5853	6027
6	3971	4314	4591	4385	4832	5004	5280	5419	5775	6087
7	4227	4198	4640	4689	4835	5208	5319	5646	5807	6355
8	3841	4354	4752	4887	4808	5177	5059	5569	5539	6116
9	3885	4118	4534	4637	4922	5081	5405	5465	5893	6071
10	4014	4329	4350	4547	4903	5211	5438	5807	5748	6143
11	3933	4209	4448	4531	4884	5254	5522	5763	6065	6226
12	3995	4346	4616	4510	4752	5237	5377	5505	5825	6052
13	4045	4142	4349	4830	4804	5225	5357	5583	6158	6050
14	4045	4151	4455	4549	4939	5068	5244	5820	5634	5954
15	4008	4353	4337	4599	4991	5253	5429	5835	5697	6449
16	4110	4234	4412	4530	4814	5070	5246	5499	5688	6476
17	4036	4219	4471	5041	4891	5028	5640	5645	5673	6050
18	4045	4226	4363	4680	4723	5125	5203	6400	6188	6541
19	4070	4256	4346	4569	4864	5157	5354	5628	5709	6043
20	4059	4237	4325	4688	5190	4911	5152	5670	6303	6161
21	3922	4277	4519	4549	4826	5359	5360	5562	5565	5947
22	3928	5168	4518	4446	4784	5195	5151	5687	5576	6214
23	4042	4181	4324	4573	4786	5164	5153	5619	5822	6697
24	3915	4348	4395	4603	4786	4949	5287	5556	5631	6456
25	3801	4369	4459	4561	4804	5011	5097	5605	5911	5988
26	3979	4305	4370	4779	4794	4842	5277	5685	5594	5903
27	3989	4297	4540	4625	4756	5119	5204	5447	5719	5875
28	3907	4233	4390	4650	4897	5090	5219	5420	5845	6074
29	3823	4522	4305	4667	4691	5325	5292	5706	5819	6102
30	3943	4222	4483	4478	4879	4992	5399	5763	5658	5946
31	3912	4412	4404	4473	4936	5192	5382	5647	5587	6435
32	3934	4251	4532	4625	4807	5166	5255	5257	5627	5982
33	3908	4396	4477	4578	4856	5329	5084	5758	5833	5802
34	3989	4353	4388	4680	4946	5336	5178	5546	5691	5762
35	3980	4205	4415	4347	4830	5889	5419	5411	5915	6323
36	4106	4198	4260	4532	4890	5138	5290	5538	5730	7439
37	3991	4041	4333	4671	4815	4953	5238	5863	6005	6050
38	4139	4368	4469	4861	4955	5052	5346	5505	5736	5792
39	4143	4184	4378	4659	4835	5199	5348	5324	5692	5856
40	4069	4145	4373	4517	4804	5072	5361	5537	5813	5943
41	4087	4155	4479	4780	5050	5935	5264	5429	5618	6030
42	3965	4267	4288	4511	4804	5308	5420	5603	5796	5839
43	4106	4212	4463	4455	4927	4895	5132	5531	5768	6651
44	3860	4151	4407	4660	4635	5080	5040	5687	5839	5890
45	4007	4286	4442	4565	4816	5052	5523	5566	5829	6082
46	3923	4119	4337	4668	4873	5001	5298	5691	5936	6117
47	3844	4169	4318	4384	4811	5254	5210	5711	5817	6662
48	4136	4189	4330	4517	4901	5183	5287	5663	5783	5776
49	3886	4290	4332	4754	5035	5071	5412	5894	5843	5969
50	3941	4329	4422	4790	4937	4919	5318	5553	6059	5909
Média	3992,22	4273,82	4440	4606,56	4854,3	5151,22	5312,74	5615,56	5798,12	6130,16

Apêndice K – Tempo de Recuperação RSA 1024 AES 128 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	5012	5242	5242	5585	5772	6271	5991	6926	6755	6754
2	4912	5054	5428	5601	5897	5882	6427	6303	6490	6537
3	5098	5132	5476	5600	5819	6115	6131	6396	6614	6583
4	5095	5180	5023	5554	6209	5788	6037	6474	6318	6958
5	5056	5179	5460	5444	5787	5756	6131	7768	7192	6723
6	5031	5553	5320	5601	6069	6084	6490	6412	7207	6521
7	4880	5117	5382	5553	5647	6240	6006	6100	6380	7098
8	4985	5226	5288	5804	5756	5772	6193	6286	6521	7909
9	5202	5086	5335	5694	5617	5803	6458	6209	6287	6864
10	5017	5023	5242	5616	5584	6084	6209	6303	6614	6584
11	4782	5070	5304	5553	5757	5788	6224	6318	6880	6739
12	5053	5164	5413	5382	6146	6006	6334	6177	6661	6833
13	5226	5195	5367	5725	5850	6115	6178	6147	6365	6770
14	4945	5148	5226	5492	5881	5959	6193	6271	6458	6568
15	5190	5194	5429	5475	5585	5881	6318	6630	6459	6520
16	5185	5102	5428	5382	5632	6318	6068	6193	6583	6849
17	4971	5288	5336	5460	5647	6162	6006	6349	6786	6895
18	4946	5101	5226	5538	5756	6318	6069	6178	6459	6614
19	5101	5289	5397	5413	5741	5944	5865	6209	6442	6646
20	5058	5382	5569	5788	5710	5803	6069	6131	6381	6770
21	5008	5350	5507	5444	5647	6084	6130	6146	6443	6771
22	4987	5273	5289	5679	5491	5866	6100	6271	6630	6973
23	4988	5101	5288	5522	5632	6037	5944	6396	6926	6724
24	4992	5008	5304	5569	5865	5959	6224	6349	6568	6583
25	5039	5132	5273	5539	5694	6209	6069	6428	6442	6723
26	4992	5164	5210	5740	5975	6178	6115	6286	6646	6537
27	5039	5257	5632	5476	5679	5819	5959	6365	6724	6755
28	5039	5117	5366	5429	5897	5725	6100	6115	6630	7051
29	4992	5148	5445	5803	5757	6021	6052	6506	7269	8018
30	4820	5195	5350	5413	5569	6069	5991	6255	6568	6880
31	5164	5085	5398	5507	5741	5772	6209	6427	6521	6646
32	5195	5039	5413	5507	5678	5772	6271	6240	6458	6583
33	4914	5148	5195	5382	5788	5819	6068	6272	6505	6521
34	4992	5117	5538	5631	7051	6271	6256	6208	6287	6552
35	4992	5117	5288	5570	5975	5865	6099	6506	6833	6817
36	5007	5070	5226	5818	5631	5788	6272	5896	6458	6552
37	5133	5179	5133	5554	5663	5866	6162	6272	6552	6801
38	5132	5070	5288	5429	5569	5787	5928	6396	6428	6755
39	5195	5117	5398	5460	5803	5975	6084	6209	6333	6693
40	5288	5257	5304	5569	5741	5897	6349	6208	6599	6505
41	4868	5413	5210	5460	5788	5850	6177	6350	6833	6661
42	5101	5226	5382	5429	5663	5819	5944	6255	6427	6552
43	5163	5273	5258	5569	5678	5990	6084	6365	6474	9594
44	5289	5101	5226	5476	5616	5991	6303	6287	6630	6568
45	4961	5211	5382	5584	5725	6006	6333	6240	6583	6864
46	4945	5085	5444	5461	5647	5834	6069	6224	6724	6723
47	4992	5180	5362	5413	5804	5959	6162	6225	6817	6506
48	5070	5101	5382	5413	5772	5741	6037	6208	6505	6801
49	4976	5085	5335	5429	5725	5944	6162	6318	6427	6552
50	4836	5351	5273	5678	5554	5881	6068	6474	6646	6677
Média	5037,08	5173,9	5339,8	5544,26	5773,6	5957,66	6142,36	6329,54	6594,76	6813,46

Apêndice L – Tempo de Recuperação RSA 1024 AES 128 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	7597	6115	6318	6146	6505	6630	7051	8845	7005	7269
2	6053	6131	6458	6162	6567	6926	7223	7004	7129	7239
3	6022	6147	6131	6412	6443	6552	6739	6927	6973	7519
4	6053	6146	6069	6240	6505	6537	7239	6786	6880	7145
5	6146	6146	6193	6302	6537	6552	6676	6864	6957	7160
6	8611	6194	6224	6490	6443	6754	6646	6942	7083	7597
7	6053	6130	6131	6302	6396	6506	6886	6973	7098	7348
8	5990	6100	6146	6349	6458	6614	6755	7036	7082	7129
9	6022	6131	6209	6412	6536	6677	6770	6864	6973	7223
10	6006	6146	6147	6443	6365	6770	6802	7035	7036	7129
11	6084	6178	6099	6286	6474	6521	6520	6895	7129	7020
12	6069	6162	6365	6318	6474	6568	7036	6724	7067	7083
13	6146	6271	6303	6334	6490	6567	6755	7160	7051	7222
14	6068	6256	6052	6412	6443	6615	6723	6942	6849	7176
15	6194	6037	6225	6286	6396	6599	7036	7410	7004	7161
16	6099	6193	6302	6381	6505	6552	7270	6802	6973	7160
17	6053	6069	6147	6427	6443	6754	6630	7160	7020	7239
18	6006	6052	6318	6225	6427	6646	6676	7067	7067	7160
19	6131	6147	6162	6411	6427	6505	6662	6849	6833	6973
20	6084	6099	6130	6303	6490	6568	6895	6754	6879	7098
21	6068	6256	6194	6318	6427	6552	7207	6942	7020	7239
22	6069	6240	6162	6349	6380	6536	6808	6740	7052	7332
23	6162	6193	6224	6255	6474	6552	6904	6723	7222	7082
24	5974	6349	6224	6428	6677	6537	6927	7052	7020	7036
25	6038	6131	6131	6271	6303	6879	6676	6676	7067	7113
26	5990	7816	6240	6318	6474	6521	6603	6849	7192	7036
27	6053	6302	6115	6365	6427	6739	6817	6864	6911	7301
28	6084	6147	6116	6224	6505	6583	6755	6864	6973	7379
29	6053	6115	6099	6427	6396	6771	6771	6879	6848	7176
30	6099	6021	6116	6240	6365	6661	6739	6927	7036	7129
31	6084	6084	6130	6396	6489	6583	6895	6848	6989	7004
32	6116	6069	6100	6256	6537	6646	6802	6942	6895	7036
33	6068	6177	6178	6302	6411	6583	6676	6927	6926	7238
34	6100	6085	6240	6287	6506	6786	6833	6957	6864	7192
35	5990	6084	6255	6240	6443	6630	6849	6973	6802	7441
36	6053	6146	6100	6209	6567	6615	6879	6864	7036	7160
37	5959	6193	6099	6365	6599	6832	6708	6942	6957	7098
38	6022	6209	6256	6240	6349	6677	6755	6927	7129	7192
39	6052	6178	6131	6240	6412	6568	6786	7082	7161	7426
40	6100	6037	6193	6255	6489	6645	6849	6802	7035	7004
41	6131	6068	6084	6365	6381	6630	6801	6833	7083	6973
42	6084	6100	6162	6334	6489	6521	6786	6864	7004	7130
43	6006	6084	6115	6287	6381	6552	6771	6864	7083	7378
44	5990	6068	6287	6318	6443	6615	6739	6848	6910	7239
45	6037	6069	6271	6318	6520	6598	6770	6755	6818	7020
46	6022	6052	6193	6255	6459	6568	6693	6786	7160	7113
47	6053	6131	6350	6271	6411	6599	6598	6942	6880	7067
48	6084	6100	6255	6287	6443	6614	6724	6786	6801	7192
49	5975	6099	6350	6287	6412	6599	6692	6942	7161	7223
50	6068	6084	6130	6318	6411	6817	6974	6614	6864	7628
Média	6141,42	6170,74	6192,58	6313,32	6458,08	6628,44	6815,54	6941,06	6999,74	7192,54

Apêndice M – Tempo de Recuperação RSA 1024 AES 256 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	3949	4430	4549	4702	5169	5300	5468	5820	6182	6461
2	4087	4401	4701	4805	5108	5297	5621	5798	6101	6556
3	4144	4204	4690	4720	4892	5295	5457	5430	6047	6166
4	3873	4478	4422	4648	4900	5219	5699	5788	6124	6467
5	4080	4209	4509	4603	5203	5231	5676	5836	6020	6286
6	4141	4441	4705	4643	5111	5281	5714	5882	6075	6071
7	3954	4345	4363	4604	5291	5219	5593	5824	6082	6445
8	3898	4345	4441	4728	5117	5274	5767	5909	6158	6102
9	3992	4393	4366	4829	5291	5266	5603	5792	6197	6207
10	4065	4299	4477	4799	5155	5273	5777	5869	6059	6100
11	4083	4507	4735	4786	5173	5308	5697	5756	6178	6394
12	3961	4495	4620	4775	4815	5289	5400	5827	6147	6432
13	3955	4207	4700	4697	4965	5277	5471	5900	6076	6052
14	4001	4434	4661	4778	5277	5309	5730	5749	6061	6415
15	4069	4438	4464	4798	4817	5260	5683	5800	6184	6364
16	4104	4304	4540	4655	4819	5201	5406	5907	6134	6183
17	4074	4469	4361	4621	5263	5260	5423	5903	6189	6162
18	4146	4448	4502	4730	4993	5235	5405	5797	6167	6216
19	4078	4254	4488	4659	5045	5256	5635	5823	6036	6462
20	3912	4338	4478	4661	4888	5234	5793	5777	6086	6186
21	3909	4251	4547	4764	5051	5301	5653	5851	6160	6302
22	4019	4240	4342	4773	5050	5225	5998	5896	6178	6295
23	4011	4267	4598	4789	5226	5201	5603	5878	6031	6401
24	3873	4361	4508	4839	4999	5246	5573	5857	6155	6174
25	4023	4385	4800	4636	5259	5335	5691	5744	6107	6058
26	4035	4241	4534	4704	4931	5227	5509	5906	6179	6250
27	3985	4538	4734	4842	4976	5279	5642	5746	6145	6225
28	4123	4504	4564	4656	5011	5270	5744	5845	6095	6671
29	4101	4536	4447	4762	5187	5241	5637	5840	6080	6552
30	4045	4258	4354	4687	4764	5256	5644	5885	6198	6196
31	3971	4203	4752	4847	5178	5252	5591	5880	6079	6170
32	4094	4353	4378	4643	5199	5232	5998	5730	6063	6422
33	3975	4337	4607	4711	5200	5206	5607	5857	6084	6107
34	3999	4527	4341	4806	4714	5299	5628	5806	6070	6427
35	4120	4248	4602	4675	4811	5298	5673	5876	6066	6477
36	4001	4223	4395	4712	5344	5260	5796	5866	6092	6063
37	4152	4471	4504	4692	5073	5352	5632	5886	6149	6476
38	4045	4389	4506	4750	5148	5302	5641	5850	6079	6642
39	4108	4777	4604	4603	5001	5306	5565	5755	6025	6578
40	4086	4489	4458	4824	4727	5304	5553	5778	6128	6287
41	3899	4201	4623	4648	5237	5281	5478	5773	6125	6224
42	4001	4209	4784	4821	4724	5278	5652	5899	6155	6229
43	4142	4338	4790	4845	4755	5301	5762	5861	6029	6446
44	4201	4101	4522	4656	5079	5290	5609	5787	6111	6076
45	3884	4489	4592	4625	4849	5254	5681	5874	6183	6493
46	4038	4248	4410	4829	5328	5301	5561	5877	6149	6336
47	3987	4151	4459	4850	4719	5237	5627	5888	6111	6239
48	4090	4203	4422	4700	4942	5243	5698	5834	6080	6539
49	4215	4342	4441	4818	5194	5218	5697	5833	6061	6092
50	4131	4361	4539	4849	5351	5301	5722	5801	6068	6502
Média	4037	4354	4539	4732	5046	5268	5638	5827	6111	6314

Apêndice N – Tempo de Recuperação RSA 1024 AES 256 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	5060	5559	5118	5533	5527	5837	5871	6326	6237	6607
2	5153	5386	5320	5446	5439	5880	6203	6227	6457	6502
3	5263	5164	5293	5411	5486	5825	5928	6463	6391	6474
4	5290	5422	5114	5479	5474	5748	5992	6107	6164	6458
5	5043	5311	5317	5430	5792	5831	6273	6183	6125	6600
6	5053	5565	5211	5442	5662	5808	5986	6336	6573	6561
7	5133	5550	5254	5494	5482	5842	6078	6111	6115	6467
8	5194	5441	5308	5543	5609	5774	6201	6334	6682	6570
9	5062	5216	5211	5487	5778	5865	5808	6318	6660	6464
10	5213	5444	5401	5408	5688	5720	6198	6460	6334	6571
11	5305	5183	5306	5524	5776	5772	6110	6003	6332	6548
12	5006	5230	5339	5523	5608	5841	6071	6049	6202	6523
13	5378	5100	5184	5492	5578	5897	6008	6220	6281	6438
14	5061	5276	5274	5410	5728	5832	6337	6219	6098	6513
15	5229	5447	5442	5464	5778	5794	5683	5907	6101	6558
16	5283	5231	5352	5383	5789	5709	5812	6078	6637	6425
17	5142	5443	5249	5354	5673	5840	5854	6048	6468	6531
18	5203	5094	5336	5488	5597	5702	6042	6442	6514	6465
19	5127	5168	5480	5407	5575	5737	5876	6473	6096	6535
20	5069	5141	5469	5368	5567	5812	6276	6008	6377	6579
21	5309	5335	5112	5409	5761	5860	6035	6081	6234	6606
22	5286	5202	5241	5392	5486	5715	5685	6144	6532	6452
23	5363	5208	5236	5403	5596	5789	5668	6062	6414	6482
24	5268	5461	5176	5472	5710	5751	6189	6285	6452	6518
25	5014	5185	5128	5443	5800	5900	6033	6070	6674	6436
26	5051	5234	5434	5491	5803	5862	6163	6022	6215	6573
27	5165	5432	5276	5522	5576	5829	6037	6312	6388	6566
28	5078	5070	5771	5523	5457	5856	5640	6099	6256	6562
29	5066	5125	5294	5487	5469	5879	5799	6197	6517	6586
30	5120	5452	5222	5416	5633	5736	6315	6298	6387	6602
31	5110	5194	5224	5421	5465	5723	5681	6301	6158	6454
32	5154	5341	5410	5421	5660	5867	6392	6324	6312	6491
33	5298	5379	5336	5450	5701	5741	5926	6118	6403	6549
34	5235	5302	5335	5432	5743	5833	6283	6104	6561	6484
35	5393	5153	5456	5486	5488	5779	5751	6151	6278	6468
36	5245	5303	5403	5503	5748	5875	5752	6019	6294	6466
37	5269	5395	5130	5388	5526	5891	5835	6282	6349	6507
38	5126	5301	5178	5369	5751	5899	6338	6061	6381	6433
39	5254	5308	5458	5416	5569	5738	5999	6333	6412	6617
40	5302	5372	5148	5499	5712	5861	5634	6117	6589	6478
41	5163	5404	5484	5405	5634	5818	5894	6173	6590	6525
42	5336	5155	5349	5430	5629	5753	6211	6349	6347	6514
43	5232	5318	5500	5404	5743	5791	5747	6103	6608	6578
44	5156	5095	5260	5388	5597	5834	6266	6449	6432	6537
45	5013	5172	5442	5475	5692	5851	6366	6103	6545	6592
46	5194	5041	5161	5412	5497	5731	6072	6444	6289	6508
47	5201	5185	5407	5521	5682	5846	6209	5975	6231	6523
48	5320	5232	5333	5421	5570	5745	5610	6096	6557	6575
49	5325	5101	5305	5408	5755	5799	6290	6081	6398	6445
50	5221	5279	5196	5513	5816	5850	6085	6118	6437	6458
Média	5191	5282	5308	5448	5638	5809	6010	6192	6382	6519

Apêndice O – Tempo de Recuperação RSA 1024 AES 256 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	6089	6183	6208	5990	6068	6001	7020	6942	8923	7285
2	5979	6183	6050	6061	6002	5994	6880	7207	7176	7101
3	5985	6203	6011	6050	6350	6611	7176	7395	7254	7297
4	6071	6161	6139	6304	6295	6388	6864	6957	7160	7179
5	5957	6075	6359	6054	6141	6210	7207	7301	7130	7211
6	6152	6123	6741	6359	6884	6391	6958	7020	7113	7159
7	5978	6037	6275	6140	6220	6182	6942	6895	7083	7460
8	5921	6287	6226	6120	6500	6170	7020	7083	7113	7519
9	5982	6603	6197	6210	6303	6321	7020	6865	7364	7707
10	6020	6116	6243	6134	6202	6197	6786	7051	7082	7410
11	7078	6317	6234	6222	6218	6336	7082	7223	7160	7394
12	5962	6050	6141	6082	6183	6290	6740	7113	7192	7192
13	6042	6217	6008	6208	6144	6209	6864	7161	7145	7316
14	5956	6219	6193	6212	6206	6231	6848	7066	7160	7270
15	5977	6337	6169	6327	6327	6194	7067	7067	7379	7581
16	6195	6452	6130	6330	6269	6188	6926	7098	6880	7488
17	6033	6122	6227	6232	6197	6234	6989	7005	7160	7488
18	6189	6110	6152	6214	6522	6194	7114	7160	7051	7332
19	5945	6108	6043	6233	6344	6223	6708	6926	7051	7395
20	6057	6143	6205	6140	5915	6154	6786	7052	7130	7129
21	6211	7137	6192	6374	6349	6315	6770	8533	7051	7176
22	6114	6075	6132	6685	6269	6597	6708	6786	7270	7145
23	6145	6024	6070	6279	6166	6367	6692	6833	7456	7566
24	5999	6049	6188	6211	6210	6311	6864	6848	7223	7223
25	6052	6142	6004	6204	6160	6585	7332	7067	7161	7457
26	6130	6203	6396	6311	6322	6793	6942	6989	6942	7300
27	6026	6188	6086	6069	6197	6227	6802	6864	7129	7457
28	5925	5975	6058	6223	6138	7364	6739	6973	7098	7207
29	6002	6024	5906	6132	6212	7100	6864	7067	7020	7239
30	6012	6155	6016	6205	6238	6095	6864	7020	7129	7238
31	6137	6362	6084	6316	6264	6486	6974	6973	7098	7410
32	5981	6084	6041	6145	6161	6230	6676	7036	7036	7426
33	6129	6050	6038	6103	6382	6634	6771	6895	7191	7316
34	6051	6040	5983	6136	6214	6408	6848	6817	7161	7301
35	5914	6047	6015	6123	6079	6336	6973	6864	7347	7628
36	6025	6342	6105	6221	6233	6530	6677	6880	6958	7145
37	5960	6256	6040	6224	6157	6196	6771	6942	7176	7317
38	5959	6095	6178	6087	6070	6188	6786	6895	6958	7316
39	6073	6178	6037	6031	6184	6187	6848	7067	7254	7519
40	5936	6032	6053	6266	6247	6263	6708	6942	7098	7161
41	6143	6096	6167	6304	6290	6878	8362	7004	6973	7176
42	5988	5965	6021	5997	6100	6830	6770	6927	7113	7566
43	6005	6259	5960	6189	6048	6431	6630	6879	6864	7503
44	5988	5992	6051	6099	6174	6260	6817	6895	7052	7208
45	5998	6105	5966	6085	6101	6198	6740	6927	7129	7285
46	5909	6171	6114	6176	6198	6212	6770	6848	6911	7347
47	6012	6224	6085	6121	6269	6204	6864	6911	7004	7566
48	6014	6199	6026	6185	6128	6166	6911	6770	7004	7208
49	6025	6114	6162	6202	6080	6175	6879	7005	7223	7222
50	5995	6147	6184	6234	6176	6259	6864	6864	7192	7301
Média	6048,52	6175,52	6126,18	6191,18	6222,12	6350,86	6904,26	7018,16	7158,54	7336,84

Apêndice P – Tempo de Recuperação RSA 2048 AES 256 (3 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	4089	4202	4356	4520	4799	5079	6193	6303	6147	7940
2	4155	4145	4454	4669	4641	5022	5351	5148	5756	6615
3	4223	4171	4527	4672	4821	5036	5429	5475	5757	6193
4	4073	4274	4378	4511	4783	5099	5586	5648	6115	6661
5	4140	4124	4407	4653	4958	5964	5394	5350	6131	6256
6	4116	4255	4399	4616	4905	5209	5225	5850	5896	5741
7	4037	4287	4444	4512	4949	5043	5429	5554	5819	6208
8	4056	4157	4406	4653	5007	5072	5179	5429	5990	5850
9	4196	4258	4301	4653	4754	5053	5359	7082	6162	6365
10	4119	4151	4638	4541	4729	5214	5382	5492	5881	6053
11	3965	4135	4341	4458	4751	5108	5101	5428	6069	6334
12	3997	4263	4440	4680	4821	5180	5148	5507	5865	5990
13	4038	4183	4509	4588	4788	5036	5195	5850	6147	6006
14	4050	4175	5323	4657	5073	5222	5148	5757	5741	6053
15	4038	4252	4274	4474	4804	5031	5772	5538	5834	8284
16	3987	4132	4406	4633	4825	5052	5335	5506	5741	6224
17	4301	4138	4326	4636	4882	5075	5180	5445	6521	5990
18	4123	4158	4230	4641	4722	5174	5241	5631	5803	6303
19	3968	4205	4309	4703	4774	4953	5601	5601	5850	5928
20	4095	4108	4330	4526	4730	5004	5413	5444	5538	6723
21	4040	4086	4333	4907	4724	5543	5132	5491	6037	5726
22	3952	4132	4330	4739	4970	5307	5226	5616	5523	5974
23	4187	4139	4524	4752	5209	5160	5445	5429	5740	6100
24	4223	4117	4314	4548	4730	5105	5428	5772	5741	7894
25	3953	4115	4354	4839	4770	4988	5226	5476	6802	8377
26	4039	4129	4492	4607	4773	5092	5304	5881	5538	6560
27	3944	4123	4328	4722	4795	5186	5351	5538	5928	6389
28	3922	4125	4327	4670	4782	5312	5289	5413	6021	6224
29	4085	4113	4320	4793	4968	5233	5272	5944	6006	6253
30	4043	4133	4120	4612	4898	5150	5367	5382	5804	6165
31	3937	4121	4323	4672	4944	5066	5101	5507	5881	6986
32	4102	4129	4389	4579	4954	5029	5351	5709	5694	6076
33	4006	4108	4479	4595	4634	5035	5101	5414	5569	6472
34	4074	4155	4417	4549	4895	5069	5226	5475	6006	6393
35	3997	4102	4440	4490	4829	5061	5211	5585	5881	6509
36	3934	4132	4396	4605	4920	4979	5257	5741	6084	5898
37	4034	4106	4336	4620	4694	5087	5351	5491	5725	6244
38	4030	4169	4333	4586	4764	4987	5226	5398	5819	6383
39	3956	4083	4425	4774	4780	5101	5210	5366	5882	6187
40	4115	4409	4407	4678	4811	5125	5366	5429	5694	6428
41	4069	4141	4329	4568	4832	5067	5429	5475	6583	5875
42	4077	4103	4352	4545	4765	5197	5663	5351	5819	6013
43	4020	4188	4436	4639	4891	5095	5226	5632	5647	6014
44	4082	4161	4389	4648	4828	5113	5195	5865	6037	6180
45	4002	4145	4313	4582	4860	4952	5413	5445	5678	7289
46	4069	4251	4217	4747	4903	4951	5179	5460	6272	5870
47	4360	4074	4326	4502	4697	5107	5195	5663	5756	5940
48	3988	4134	4332	4539	4830	5239	5335	5834	5569	6481
49	4050	4212	4239	4615	4731	5139	5211	6162	6459	6563
50	4044	4145	4415	4627	4729	5186	5241	5647	5678	6305
Média	4062	4161,06	4390,66	4626,9	4828,52	5125,74	5323,76	5612,58	5912,72	6389,7

Apêndice Q – Tempo de Recuperação RSA 2048 AES 256 (4 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	4977	5246	5337	5531	5525	5713	6496	6311	6759	6761
2	4958	5046	5303	5446	5746	5729	6147	6125	6152	6778
3	5224	5168	5282	5443	5648	5776	6057	6197	6305	6704
4	5164	5355	5340	5409	5710	5801	6047	6241	6256	6477
5	5070	5133	5310	5459	5647	5829	6247	6152	6217	6722
6	4966	5226	5189	5362	5673	5933	6074	6460	6381	6547
7	5119	5204	5400	5391	5545	5841	6224	6152	6332	6566
8	4985	5223	5452	5501	5735	5864	5873	6122	6436	6410
9	4967	5131	5261	5378	5616	6248	6072	6888	7007	6494
10	5028	5207	5175	5425	5519	5580	6260	6361	6366	6624
11	5180	5101	5430	5416	5453	5825	5974	6202	6508	6543
12	4967	5156	5237	5329	5580	5813	6168	6640	6261	6474
13	5107	5094	5321	5394	5694	5988	5961	6060	6573	6647
14	4962	5196	5456	5544	5668	6018	6184	6128	6873	6500
15	5104	5245	5290	5434	5679	5875	6082	6140	6293	6433
16	5005	5204	5477	5450	5787	5814	6078	6072	6376	6867
17	4948	5219	5145	5509	5737	5768	5916	6197	6392	6600
18	5032	5114	5262	5482	7200	5860	6064	6185	6338	6462
19	5134	5182	5288	5480	5676	5949	6241	6191	6395	6494
20	5013	5075	5189	5578	5670	5640	6203	6396	6283	6499
21	4935	5269	5160	5539	5747	5861	6015	6104	6298	6739
22	4939	4972	5206	5424	5541	5954	5950	6570	6361	6656
23	4998	5067	5310	5438	5577	5708	5912	6246	6490	6542
24	5052	5147	5323	5425	5767	5724	5985	6383	6334	6896
25	5023	5070	5297	5493	5473	5716	6159	6723	6442	6809
26	4926	5037	5461	5416	5887	5913	6098	6235	6345	6878
27	5132	5030	5231	5521	5411	5845	6076	6313	6313	6840
28	5041	5169	5272	5427	5427	5762	6361	6398	6610	6548
29	4957	4974	5370	5415	5551	5925	5907	6122	6337	6534
30	5104	5072	5211	5480	5508	5771	6084	6565	6280	6421
31	5025	5096	5128	5355	5752	5798	5792	6362	6489	6876
32	4987	5037	5357	5401	5546	5727	6077	6142	6424	6736
33	5053	5116	5398	5318	5541	5784	5961	6204	6186	6657
34	5338	5035	5285	5364	5580	5833	6043	6223	6299	7865
35	5005	5015	5263	5253	5809	5728	6222	6188	6830	6586
36	4973	5138	5300	5381	5593	5734	6040	6420	6392	6620
37	5049	5047	5337	5582	5816	6019	6207	6347	6389	6515
38	5127	5138	5503	5348	5408	5784	6133	5969	6364	6913
39	4861	5141	5389	5506	5606	5935	5912	6181	6314	6669
40	5362	5037	5231	5269	5541	5807	6054	6404	6557	6713
41	5025	5154	5227	5580	5756	5857	6049	6246	6572	6508
42	5074	5298	5363	5354	5540	6225	6171	6152	6300	6779
43	4970	5116	5187	5421	6018	5793	6080	6220	6454	6564
44	5138	5167	5087	5319	5621	5834	5978	6091	6377	6417
45	4928	5198	5291	5263	5754	5869	5944	6176	6468	6717
46	5275	5139	5108	5388	5562	5713	5825	6238	6321	6705
47	5050	5053	5138	5493	6120	5819	5846	6400	6311	6530
48	4992	5183	5292	5389	5619	5799	5984	6099	6175	6574
49	5019	5013	5186	5465	5572	5851	6130	6063	6337	6504
50	5002	5019	5332	5481	6105	6105	5947	6072	6423	7041
Média	5045,4	5129,44	5287,74	5429,38	5685,12	5841,14	6066,2	6261,52	6405,9	6659,08

Apêndice R – Tempo de Recuperação RSA 2048 AES 256 (5 blocos)

	tamanho do arquivo									t (ms)
teste	**300k**	**600k**	**900k**	**1200k**	**1500k**	**1800k**	**2100k**	**2400k**	**2700k**	**3000k**
1	6095	6033	7671	6179	6361	6718	6779	6932	7014	7380
2	5957	6122	6221	6053	6369	6672	6750	6856	7285	7376
3	6099	6208	6248	6223	6555	6590	6871	6930	7288	7126
4	6031	6252	6146	6147	6515	6720	6773	6950	7028	7401
5	5951	6032	6355	6212	6505	6642	6982	7088	7100	7557
6	6120	6115	6175	6237	6551	6915	6881	7214	7164	7427
7	6028	6147	6167	6153	6473	6741	6723	7017	7047	7313
8	5963	6133	6332	6120	6391	6657	6695	7078	7204	7223
9	6043	6048	6146	6202	6420	6835	6840	6829	7060	7279
10	6082	6053	6250	6048	6421	7009	6825	7020	7104	7236
11	6041	6130	6247	6089	6511	6516	6895	7055	7020	7186
12	5984	6133	6439	6173	6356	6738	6992	6915	8585	7383
13	5999	6129	6110	6144	6463	6970	6729	6901	7220	7363
14	6021	6066	6232	6111	6715	6808	6843	6980	6881	7305
15	5933	6070	6185	6076	6504	6598	6773	6847	7425	7046
16	6014	6051	6258	6209	6455	6740	6987	7120	7127	7253
17	5938	6042	6148	6049	6429	6821	6772	6810	7184	7167
18	6035	6030	6122	6124	6450	6628	6936	6831	7016	7202
19	6028	6063	6311	6060	6431	6957	6805	6868	7834	7203
20	5940	6006	6179	6129	6371	6736	6806	6835	7196	7381
21	6037	6064	6366	6111	6429	6772	6698	7098	7038	7262
22	6019	6054	6083	6123	6442	6627	6827	6864	7148	7118
23	5940	5997	6201	6144	6588	6718	6766	7035	7356	7301
24	6037	6105	6068	6041	6467	6635	6721	6680	6950	7168
25	6017	6036	6232	6210	6343	6617	6747	7108	7022	7330
26	6041	6162	6232	6149	6427	6631	6722	7041	7072	7280
27	6035	6044	6212	6066	6564	6670	6779	7338	7300	7447
28	6012	6040	6070	6124	6455	6591	6916	7316	7131	7227
29	5937	5994	6119	6208	8010	6452	6837	6906	7178	7306
30	6009	6024	6054	6139	6422	6926	6820	7132	7225	7350
31	5937	6031	6166	6114	6717	6594	6761	7009	7105	7165
32	5933	6021	6201	6146	6788	6735	6642	7048	6924	7314
33	5947	6047	6118	6184	6482	6808	6628	6913	7198	7269
34	6015	6172	6113	6129	6502	6587	6720	7019	7049	7370
35	5968	6067	6208	6204	6443	6635	6768	7193	7067	7303
36	6015	6075	6085	6129	6602	6650	6811	6866	7230	7551
37	6089	6005	6131	6048	6448	6617	6868	7157	6896	7226
38	5992	6116	6234	6158	6554	6625	6711	7088	7048	7355
39	6056	6032	6205	6217	6482	6612	6631	6822	7371	7333
40	5966	6050	6061	6209	6471	6743	6826	6918	6954	7619
41	5959	6021	6046	6070	6326	6920	6742	7064	7151	7131
42	6011	6032	6167	6130	6384	6762	6742	7041	7106	7133
43	6045	6048	6111	6203	6498	6590	6754	7101	7022	7211
44	5994	6124	6188	6051	6629	6617	6755	6937	7011	7176
45	5981	6047	6179	6055	6428	6523	6837	6839	7117	7491
46	6017	6023	6099	6150	6516	6565	6887	6834	7060	7260
47	6021	6054	6130	6076	6507	6623	6703	6986	7147	7109
48	6034	6078	6060	6133	6493	6636	6708	7020	6983	7255
49	6034	6142	6228	6030	6529	8025	6743	6794	7319	7306
50	6023	6143	6224	6036	6393	7039	6752	6900	7204	7273
Média	6008,46	6074,22	6210,66	6130,5	6511,7	6731,12	6789,58	6982,86	7163,28	7288,92

Apêndice S – Tempo Via Internet RSA 2048 AES 256 (3 blocos)

	tamanho do arquivo				
teste	**300k**	**900k**	**1500k**	**2400k**	**3000k**
1	6508	5339	6004	5313	5387
2	6271	12605	7690	8216	8184
3	9275	7275	8356	11085	8333
4	12074	15423	11944	8631	7986
5	5911	7022	7661	8427	8578
6	7376	14844	7803	8161	8060
7	6328	10046	7981	12197	8247
8	9085	7165	8265	9631	8386
9	6550	8172	8753	13984	7665
10	7412	7417	8189	11803	9053
11	7527	9843	8430	8321	12916
12	6586	7779	7690	10164	7959
13	7899	13259	8318	8233	8529
14	6067	8006	11829	8206	7861
15	8477	7721	8552	12630	7874
16	6561	7468	7796	8308	7039
17	7907	6493	11346	9863	14155
18	12209	7796	8122	13935	10701
19	6472	7505	8339	7878	11719
20	9069	7834	8594	7274	10540
21	7481	7896	7282	8310	8498
22	6350	12162	8809	9316	8697
23	8487	7208	8481	9973	8748
24	11101	14189	10665	8018	9219
25	7111	7078	7789	9040	7663
26	7276	13632	7921	9152	8834
27	6840	9273	7853	11206	8127
28	8995	7606	8499	9503	7109
29	6739	7383	8550	10987	9079
30	7325	7860	8528	10507	8061
31	7617	7954	8196	9495	11502
32	6686	7338	7810	8990	8079
33	7820	10702	7979	9529	8114
34	6154	7950	10710	8319	9138
35	7265	8933	8432	11530	8866
36	7773	7535	8909	8436	7954
37	7718	7266	10234	9750	11044
38	11697	8585	8325	11723	9468
39	7260	8739	8221	8990	11206
40	7869	9723	8469	9486	9766
Média	7778,2	8950,6	8583,1	9613,0	8958,7

	tamanho do arquivo				
teste	**300k**	**900k**	**1500k**	**2400k**	**3000k**
1	4077	3772	3936	3504	10476
2	5111	7661	7693	6963	7772
3	5029	3838	7734	7015	7191
4	5203	7674	3965	7018	6980
5	5052	3969	7641	3957	7247
6	5182	7758	7620	7356	7310
7	5018	4030	3963	7313	7429
8	5175	7213	7612	7317	7139
9	4994	4073	7651	3849	7247
10	5361	7797	3968	7364	7256
11	5173	4010	7663	7244	7214
12	5254	7620	7631	7527	7318
13	5173	3966	4680	3885	7389
14	5086	7833	13327	7410	7133
15	5165	4012	3935	7353	7466
16	5030	10851	7683	7923	7820
17	5065	4428	7737	3837	7560
18	5142	7782	3960	7474	7266
19	5466	3959	7674	7267	7451
20	5262	7838	7621	7439	7576
21	5196	6773	5933	6513	7486
22	5088	6435	7029	6837	7646
23	5117	5053	7595	6681	7525
24	5189	6860	6065	7108	8869
25	5203	4963	7526	3767	7058
26	4296	6765	7055	7022	7345
27	5097	4844	6074	6535	7763
28	5143	5998	8575	6192	8131
29	5195	4881	6653	6290	8369
30	5273	7364	5087	7246	8152
31	5196	5003	6218	6795	8014
32	5175	6626	6428	6638	7518
33	5121	4399	5792	7883	6500
34	5118	7025	7804	6521	6629
35	5121	5456	6300	6912	6966
36	5082	7850	6689	6589	7596
37	5109	5516	7425	6086	6560
38	4991	6338	7057	5124	7651
39	5247	5185	6540	5269	7229
40	5061	6750	5849	7007	7233
Média	5101,0	6004,1	6684,7	6450,8	7512

* t (ms)

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

CCMN - Bloco C - Cidade Universitária - Ilha do Fundão
Rio de Janeiro - RJ CEP: 21941-916
www.ppgi.ufrj.br