UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

DANIEL MELO

Uso de Webservices Criptográficos a partir de Dispositivos Móveis

Avaliação de viabilidade

Goiânia
2016

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE INFORMÁTICA

AUTORIZAÇÃO PARA PUBLICAÇÃO DE DISSERTAÇÃO EM FORMATO ELETRÔNICO

Na qualidade de titular dos direitos de autor, **AUTORIZO** o Instituto de Informática da Universidade Federal de Goiás – UFG a reproduzir, inclusive em outro formato ou mídia e através de armazenamento permanente ou temporário, bem como a publicar na rede mundial de computadores (*Internet*) e na biblioteca virtual da UFG, entendendo-se os termos "reproduzir" e "publicar" conforme definições dos incisos VI e I, respectivamente, do artigo 5º da Lei nº 9610/98 de 10/02/1998, a obra abaixo especificada, sem que me seja devido pagamento a título de direitos autorais, desde que a reprodução e/ou publicação tenham a finalidade exclusiva de uso por quem a consulta, e a título de divulgação da produção acadêmica gerada pela Universidade, a partir desta data.

Título: Uso de Webservices Criptográficos a partir de Dispositivos Móveis – Avaliação de viabilidade

Autor(a): Daniel Melo

Goiânia, 13 de Dezembro de 2016.

_____

Daniel Melo – Autor

_____

Marcelo Akira Inuzuka – Orientador

DANIEL MELO

Uso de Webservices Criptográficos a partir de Dispositivos Móveis

Avaliação de viabilidade

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Informática da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Computação.

Área de concentração: Otimização.

Orientador: Prof. Marcelo Akira Inuzuka

Goiânia
2016

DANIEL MELO

Uso de Webservices Criptográficos a partir de Dispositivos Móveis

Avaliação de viabilidade

Dissertação defendida no Programa de Pós–Graduação do Instituto de Informática da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Computação, aprovada em 13 de Dezembro de 2016, pela Banca Examinadora constituída pelos professores:

Prof. Marcelo Akira Inuzuka
Instituto de Informática – UFG
Presidente da Banca

Prof. <Nome do membro da banca>
<Unidade acadêmica> – <Sigla da universidade>

Profa. <Nome do membro da banca>
<Unidade acadêmica> – <Sigla da universidade>

Daniel Melo

Graduado na Universidade Federal de Goiás como Baracharel em Sistemas de Informação no ano de 2016, tendo desenvolvimento como Trabalho de Conclusão de Curso um estudo de viabilidade do fornecimento de webservices criptográficos seguindo o padrão OpenPGP a partir de dispositivos móveis.

Dedido este trabalho aos meus pais, Maria de Lourdes de Oliveira Melo e Antonio Melo Lima, a quem eu amo, que com seu esforço, carinho e dedicação, construiram as bases de todas as capacidades que me permitem concluir este curso.

Agradecimentos

<Texto com agradecimentos àquelas pessoas/entidades que, na opinião do autor, deram alguma contribuíção relevante para o desenvolvimento do trabalho.>

<Epígrafe é uma citação relacionada com o tópico do texto>

<Nome do autor da citação>,
<Título da referência à qual a citação pertence>.

Resumo

Melo, Daniel. **Uso de Webservices Criptográficos a partir de Dispositivos Móveis**. Goiânia, 2016. 57p. Dissertação de Mestrado. Instituto de Informática, Universidade Federal de Goiás.

Apesar de a criptografia ser conhecida há muitos anos o desenvolvimento das ferramentas e técnicas não tem sido suficiente para assegurar a sua adoção por grandes grupos de usuários. Neste trabalho propomos o uso de web services capazes de oferecer recursos de criptografia a partir de dispositivos móveis, oferecendo uma alternativa para que o usuário final possa realizar o transporte e a gestão de seus recursos de segurança com mais simplicidade. Essa abordagem também busca facilitar a integração à outras ferramentas que desejem usar tais recursos. Essas capacidades são desenvolvidas mantendo o controle dos recursos criptográficos com o usuário final.

Palavras–chave

Criptografia, PGP, Webservices, Dispositivo Móvel

Abstract

Melo, Daniel. **Using Cryptographic Web services from Mobile Devices**. Goiânia, 2016. 57p. MSc. Dissertation. Instituto de Informática, Universidade Federal de Goiás.

Although the encryption be known for many years the development of tools and techniques have not been sufficient to ensure its adoption by large groups of users. In this paper we propose the use of web services capable of offering encryption capabilities from mobile devices, offering an alternative so the end user can perform transport and management of its security features with more simplicity. This approach also aims to facilitate the integration with other tools that want to use such resources. These capabilities are developed maintaining the end user in total control of his cryptography resources.

Keywords

Cryptography, PGP, Web services, Mobile devices

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Algoritmos

Lista de Códigos de Programas

CAPÍTULO 1

Introdução

O uso crescente de ferramentas sociais para comunicação entre as pessoas em ambientes diversificados traz a necessidade da garantia de privacidade de forma efetiva e fácil de usar. A produção de informação é parte da vida das pessoas em muitos contextos em que convivem. Estes dados trafegam por vários meios desprotegidos, como a internet. As formas de proteger os dados e a privacidade de quem usa os recursos computacionais são frequentemente desconhecidas dos próprios usuários dos sistemas.

Ferramentas de comunicação tem alcançado grande público e compõem uma parte importante da troca de mensagens. Um exemplo atual é o Whatsapp, que conta com mais de 600 milhões de usuários. A ferramenta promete privacidade total nas versões mais recentes, dotadas de criptografia fim a fim, segundo a própria empresa [REF19]. Como se trata de uma aplicação proprietária, não é possível auditar se a implementação de fato segue o que é divulgado ao público. Sem a possibilidade de verificar o que é, de fato, realizado pela aplicação o controle sobre as pontas não está nas mãos dos usuários.

Assim, percebe-se a demanda de software criptográfico auditável, necessariamente de código aberto, que o usuário tenha condições plenas de controlar pessoalmente, ou por terceiros confiáveis, toda informação protegida por criptografia desde sua origem até o seu destino.

Apesar do uso da criptografia ser conhecido há muitos anos [REF3] ele ainda é de difícil compreensão e uso para usuários finais. Visto que a facilidade de uso precede uma adoção em massa de qualquer tecnologia [REF4], existe necessidade de desenvolver formas mais simples de uso para potencializar ações de segurança da informação.

Este trabalho faz uma análise do uso atual de criptografia de chaves assimétricas utilizando o software GnuPG, que segue o padrão PGP, para troca de mensagens em ferramentas com recursos de criptografia. Propõe-se em seguida a implementação de uma chaveiro criptográfico em dispositivo móvel que ofereça facilidade de gestão dos recursos de segurança. Tal chaveiro será dotado de web services para que aplicações que desejem fazer uso de seus recursos de segurança de criptografia consigam com complexidade agora reduzida.

Neste trabalho, procuramos oferecer uma solução de acesso simples via web-

services à chaveiro criptográfica em dispositivo móvel, a fim de que aplicações diversas possam consumi-lo e assim facilitar o uso da criptografia por usuários finais.

O capítulo 1 levanta alguns pontos desafiadores para a criptografia fim a fim e sua relação com a necessidade por software aberto. O capítulo 2 apresenta a tecnologia de criptografia PGP, e, em seguida, o capítulo 4 traz a análise de algumas ferramentas que implementam essa tecnologia de criptografia com ênfase na sua forma de acessar os recursos privados. No capítulo 4 propomos uma forma de acesso aos recursos de chaveiro mantidos em um celular e é feito um experimento desta proposta, descrito no capítulo 6. O capítulo 7 traz análises de desempenho e vulnerabilidades relevantes à forma de acesso proposta e experimentada e o trabalho é finalizado com o capítulo 8, que apresenta algumas conclusões obtidas no desenvolvimento desta obra.

CAPÍTULO 2

Desafios da criptografia fim a fim

A criptografia fim a fim é definida pela implementação de técnicas que garantam que somente o remetente e o destinatário tem acesso às mensagens trocadas, sendo computacionalmente inviável que alguém as leia, seja por meio de interceptação ou acesso indevido aos dispositivos físicos envolvidos. Esse tipo de criptografia não tem sido historicamente desenvolvida com foco no usuário final [REF5]. Como explorado por Sheng et Al, várias dificuldades são encontradas por usuários finais quando é colocada à prova a usabilidade das ferramentas para criptografia avaliadas. Verificamos mais à frente como algumas ferramentas com essa proposta acessam o chaveiro criptográfico.

Neste trabalho exploramos a ideia de que o desenvolvimento de aplicações que usem os serviços de criptografia oferecidos por um chaveiro PGP pode ser simplificado. O experimento explorado em seções não trata a usabilidade final, que é delegada à aplicação OpenKeyChain [REF 27]. Seu escopo limita-se à exploração de um facilitador de uso do chaveiro por desenvolvedores, simplificando o desenvolvimento de aplicações que precisem fazer uso de tais recursos de segurança.

Um dos grandes desafios dos sistemas operacionais modernos está na sua capacidade de manter a segurança dos dados de seus usuários. A segurança desses dados deve observar alguns conceitos fundamentais, como a confidencialidade - manter o acesso à informação somente à quem tem esse direito - e a integridade - a certeza de que o conteúdo não foi corrompido, seja por acidente ou de forma proposital.

Frequentemente os sistemas tem adotado alguma tecnologia para proteger as mensagens trocadas por meio de redes, como a internet.São exemplos os protocolos protegidos por camada de segurança SSL, como o HTTPS, SMTPS, para troca de hipertexto e e-mail, respectivamente. [REF6] Essa estratégia busca impedir que mensagens interceptadas possam ser lidas por atacantes. Também torna computacionalmente complexo introduzir conteúdo nas mensagens sem que isso seja notado, preservando sua integridade.

Esses meios, entretanto, somente protegem a mensagem no caminho. Quando aplicado à troca de mensagens, isso significa que o provedor do serviço terá acesso ao seu conteúdo se ele não for previamente encriptado e ele será armazenado sem proteção.

Conforme exemplificado no anexo 1, o processamento das mensagens por provedores de e-mail é uma prática comum nessas ferramentas [REF8].

A criptografia assimétrica propõe um modelo de solução para o problema de proteção dos dados armazenados. Cada usuário gera um par de chaves criptográficas, sendo uma de propósito privado e a outra de propósito público. A chave privada é usada para assinar e descriptografar as mensagens. A chave pública, por sua vez é usada para verificar assinaturas e criptografar as mensagens, que só poderão ser lidas por quem possuir a chave privada equivalente. Isso cria um mecanismo onde somente o destinatário pode ler as mensagens, visando a confidencialidade. Além disso, a capacidade de assinatura provê o recurso de não-repúdio e integridade da comunicação. Se esses recursos forem empregados na troca de mensagens temos um exemplo de criptografia fim a fim.

Outro componente essencial na criptografia fim a fim é a proteção das chaves privadas, geralmente realizado por meio de um software denominado chaveiro criptográfico. O chaveiro tem como funções a proteção das chaves privadas, a importação de chaves públicas alheias, revogação de chaves comprometidas e configuração do nível de confiança. Sendo a camada responsável por estas tarefas, está fortemente ligado à facilidade de uso das chaves pelo usuário final. O chaveiro desempenha a função crucial de proteção das chaves privadas por meio de senha. A solução adotada em implementações como o GnuPG cria um chaveiro na estação de trabalho do usuário durante a instalação, que pode então ser usado diretamente por meio de linha de comando ou acessado por através de bibliotecas específicas por softwares de terceiros.

CAPÍTULO 3

Uso do padrão OpenPGP para criptografia

PGP é uma família de softwares da área de segurança desenvolvidos inicialmente por Philip R. Zimmermann [REF12] e liberada como um freeware em 1991 e atualmente é mantida pela PGP Corp, adquirida em 2010 pela Symantec.Tendo como base esta experiência foi desenvolvido o padrão OpenPGP, que contém a mesma proposta de criptografia por meio de chaves assimétricas, uma pública e outra privada, mas agora com uma especificação publicada na RFC 4880 - OpenPGP Message Format. A publicação desta especificação permitiu o nascimento de implementações abertas. A mais conhecida para desktop é a GnuPG, ou simplesmente GPG, tanto que, por vezes, os termos PGP e GPG são usados de forma intercambiável.

Esse formato de comunicação estabelece o sigilo da mensagem e o não-repúdio [REF7] - incapacidade de uma das partes de negar que assinou a mensagem se, de fato, o fez - da mensagem, tudo isso mantendo as chaves privadas - o recurso que guarda o poder de assinar e, portanto, de identificação - em sigilo.

Essa tecnologia encontrou um forte caso de uso nas trocas de e-mail, impedindo que a interceptação das mensagens comprometesse seu sigilo e, que um terceiro pudesse se passar por um dos interlocutores de forma despercebida ou, ainda, que um dos interlocutores mais tarde negasse que ele assinou a mensagem.

Outro caso de uso bastante explorado é a assinatura de arquivos. Dado que uma assinatura precisa da senha do chaveiro do usuário somada à posse da chave privada ela pode ser usada com propósitos legais na assinatura de documentos digitais.

GPG está disponível para todos os grandes sistemas operacionais, de estações desktop até celulares e várias bibliotecas permitem desenvolvimento sobre esta tecnologia.

CAPÍTULO 4

Analise de formas de acesso à chaveiros criptográficos

Várias aplicações fazem uso do chaveiro PGP para melhorar a segurança dos seus recursos e proteger a comunicação entre os usuários. O chaveiro em si precisa ser capaz de fornecer os serviços discutidos anteriormente e, para isso, existem algumas formas utilizadas por aquelas aplicações. Segue uma análise de algumas dessas formas de acesso ao chaveiro PGP e algumas aplicações que empregam tal forma.

4.1 Acesso através de linha de comando e bibliotecas

A obra de W. Lucas traz várias das funções de acesso à recursos PGP explicadas com rico detalhe, além de exemplos de uso [REF32]. A aplicação GnuPG é uma das formas mais conhecidas de fazer uso de chaves PGP.

O GnuPG é uma implementação da do formato OpenPGP, que permite a geração e uso das chaves privadas em interface de linha de comando. Essa é a principal implementação do formato em uso atualmente, e é instalada por padrão em várias distribuições Linux. Também está disponível para Microsoft Windows por meio da suite Gpg4win. Essa implementação é uma ferramenta completa, contando com todas as operações esperadas de um chaveiro criptográfico.

Como exemplo de acesso ao chaveiro por linha de comando, segue como criptografar um arquivo textual com a chave pública de um usuário fictício, cujo e-mail é bob@email.com e a assinatura pelo usuário de e-mail alice@email.com. Bob representa quem receberá a mensagem e Alice será o emitente neste exemplo. O anexo XX traz também um pequeno passo-a-passo de como criar novos pares de chave e como descriptografar a mensagem deste exemplo.

Para que esta chave seja usada para criptografar um conteúdo utilizamos o mesmo comando gpg, agora com a instrução –encrypt, seguido de –local-user indicando a chave do usuário emitente da mensagem e –recipient, que indica o usuário que receberá

a mensagem. No exemplo abaixo o usuário Bob encriptará uma mensagem para Alice. O comando completo será:

```
gpg  --encrypt --output mensagem.cifrada.pgp \
   --armor --local-user bob@email.com  --recipient \
   alice@email.com mensagem.plana.txt
```

No comando acima, os detalhes da operação são os seguintes:

- `--encrypt` : instruiu o gpg que se trata de uma operação de encriptação
- `--output`: informa o arquivo destino, onde será gravada a mensagem cifrada
- `--armor`: opcionalmente usada para que a mensagem cifrada esteja em formato ASCII
- `--local-user`: usuário local que está gerando a mensagem
- `--recipient`: usuário que receberá a mensagem. A sua chave pública deve ser conhecida no chaveiro.

Essa forma de acesso pode ser explorada por qualquer aplicação que resida na máquina onde o GnuPG está instalado. Além da chamada pelo binário gpg, demonstrada anteriormente, o gpg instalado em estações de trabalho contém uma biblioteca padrão chamada GPGME, que oferece exposição de recursos da aplicação de forma padronizado para linguagens diversas. Em aplicações que fazem uso do chaveiro instalado localmente essas chamadas são abstraídas por diversas bibliotecas, de acordo com a linguagem desejada. A página de ferramentas do GnuPG trás alguns exemplos dessas bibliotecas [REF21]. Alguns exemplos são:

- gpgme - A biblioteca padrão fornecida pelo GnuPG, já citada [REF22]
- `gpg_encrypt()` - Função nativa da linguagem PHP [REF23]
- py-gnupgp - Módulo para linguagem Python que faz interface com o GnuPG [REF24]
- gnupg-for-java - Biblioteca para linguagem Java que expõe os recursos da biblioteca gpgme[REF25]
- ruby-gpgme - Biblioteca para linguagem Ruby que expõe os recursos da gpgme [REF26]

Algumas ferramentas conhecidas que fazem uso de bibliotecas como essas são o Enigmail, o Apache OpenPGP, o Claws Mail e o WebPG para Firefox. Em todos os casos a instalação oferecida na estação de trabalho é usada para realizar as operações necessárias junto ao chaveiro criptográfico.

O Enigmail é um plugin desenvolvido para o cliente de e-mail Mozilla Thunderbird. Este plugin estende as capacidades do Thunderbird dando-lhe a capacidade de

encriptar, desencriptar, assinar e verificar assinatura de e-mails. O Claws Mail é outro cliente de e-mail que também implementa os recursos de segurança usando o chaveiro local para proteger as mensagens.

O Apache OpenPGP é uma extensão para o servidor HTTP Apache que permite que requisições HTTP sejam assinadas e verificadas pelo servidor. Ela faz par com a extensão Enigform para o Firefox, que modifica as requisições usando a instalação local do chaveiro PGP.

4.2 Token de Segurança Móvel

Tokens móveis são dispositivos capazes de oferecer recursos de segurança e ainda manter a capacidade de transporte desses recursos. Eles costumam carregar consigo senhas, dados biométricos ou chaves criptográficas.

Esses dispositivos são um conjunto de um token, com formato similar ao de um cartão de memória ou de um pendrive, e o software que é instalado na estação de trabalho que permite acessá-lo. Os dispositivos levam consigo as chaves privadas e públicas do usuário ou empresa, além de uma cadeia de certificados ligados à Autoridade Certificadora Raiz da ICP-Brasil [REF28]. Existe a possibilidade de usar esses recursos para criptografar conteúdo, realizar assinaturas digitais e mesmo encriptar conexões HTTPS, estabelecendo identificação entre aplicações remotas de forma confiável e juridicamente aceita.

Alguns dos tipos de tokens móveis são:

- Cartão e leitor de cartão criptográfico, como no e-CPF desenvolvido pela Serasa
- Token em formato de pendrive, conectado ao USB da estação de trabalho
- Token móvel, instalado em dispositivo móvel, como o MobileID, da Certisign
- Token não conectado, que gera um número secreto de tempo em tempo
- Token não conectado, que gera um número secreto mediante apresentação de senha pessoal

Uma das soluções mais conhecidas no Brasil é o e-CPF, para pessoa física, e o e-CNPJ, para pessoas jurídicas.

Exemplos de diversos tipos de token, como aqueles em formato de pendrive, cartão criptográfico e token desconectado, gerador de código secreto com e sem entrada de senha pessoal

Avaliando os dispositivos oferecidos pela Serasa, uma das maiores revendedoras do país, nota-se que não existe suporte para outros sistemas operacionais que não o Microsoft Windows a partir da versão XP [REF 29]. O acesso as operações do token é feito

a partir do software que o acompanha. Aplicações que desejam usar essa aplicação devem acessar as bibliotecas fornecidas por cada fabricante instaladas no sistema operacional.

A Certisign oferece, além desses modelos, uma versão para celular [REF29]. A aplicação está disponível para Windows, MacOS e Android. A criação e validação dos certificados acontece presencialmente e, com alguns códigos de segurança, o certificado pode ser emitido no dispositivo. O acesso à essa instalação no dispositivo móvel também é feito por meio de software da fabricante, de forma similar aos desenvolvidos pela Serasa.

Em ambos os casos apresentados, o acesso pode ser simplificado pelo seguinte diagrama:

Alguns tokens podem ser usados de forma desconectada. Um exemplo no Brasil é utilizado por bancos para autenticar operações por internet banking. Um pequeno dispositivo gera um número aleatório que muda de tempo em tempo. Para realizar operações junto ao banco, o usuário deve fornecer o número que o token mostra naquele momento. Somente se o sistema bancário autenticar a entrada fornecida pelo usuário a operação poderá continuar.

Nesse caso não há acesso direto ao token e também não é possível que diferentes aplicações usem seu sistema de segurança, já que a forma de geração do código secreto somente é conhecida pela instituição bancária, no exemplo citado.

4.3 Considerações

Em várias das aplicações apresentadas é necessário que o usuário configure repetidamente as diversas estações de trabalho nas quais precisa usar os recursos do chaveiro criptográfico. A gestão das chaves já é, por si só, uma tarefa que lhe exigirá atenção. O uso de tokens móveis torna esta gestão mais simples, trazendo mobilidade ao chaveiro.

O desenvolvimento de outras aplicações que usem tais chaveiros também dependerá da configuração do ambiente, que se repete em cada estação de trabalho.

CAPÍTULO 5

Proposta de chaveiro pessoal móvel acessível por Webservices

5.1 Descrição da proposta

Neste trabalho propõe-se uma solução para as dificuldades com configuração de ambiente e mobilidade do chaveiro, dando ao usuário a capacidade de manter consigo o chaveiro PGP com seus recursos privados de criptografia e, ainda assim, ser capaz de utilizar tais recursos nas aplicações com as quais interage cotidianamente em suas estações de trabalho.

O capítulo 4 apresentamos formas de acesso ao chaveiro estão concentradas em bibliotecas e outros softwares na estação de trabalho.. Buscamos neste trabalho oferecer uma interface única de acesso ao chaveiro por meio de webservices seguindo a filosofia REST. É esperado que isso simplifique a manutenção do chaveiro pelo usuário final. Também espera-se contribuir com o desenvolvimento de aplicações que usam os recursos do chaveiro, de forma que possam usar os webservices de forma centralizada e ubíqua e seja desnecessário ter a instalação em várias estações de trabalho espalhadas. cada estação de trabalho.

Para que aplicações de terceiros consigam realizar as operações necessárias, como criptografar, assinar, descriptografar e verificar assinatura, é necessário um canal de comunicação para que as aplicações localizadas nas estações de trabalho possam acessar o chaveiro e fazer uso dos recursos criptográficos agora protegidos enclausurados no dispositivo móvel. Para este fim, é proposta neste trabalho uma camada de serviço implementando estas operações como web services.

A principal vantagem do uso de web services é a simplicidade de uso por parte das aplicações clientes. Como este é um protocolo bem conhecido o desenvolvedor do cliente poderá usar bibliotecas já testadas para a sua linguagem de escolha. Somado a isto, o uso de REST com JSON torna esta API simples e transparente algo mais familiar para o desenvolvedor, visto que estas tecnologias são conhecidas e suportadas em todas as grandes linguagens de programação e são plenamente provadas no mercado.

Usando chamadas remotas de webservice será possível fazer uso dos recursos independente de uma instalação na máquina cliente dedicada à manipulação das chaves conhecidas, mantendo todo o arcabouço de segurança de interesse do usuário centralizado em seu dispositivo.

Para isso será usada uma uma implementação de chaveiro criptográfico disponível para Android chamada Open KeyChain [REF27]. Ela implementa um chaveiro PGP com uma interface simples para o usuário final. Essa ferramenta de código aberto dá suporte completo à geração de chaves privadas, importação de chaves públicas de diversos servidores comunitários, criptografia, descriptografia, assinatura e verificação de assinaturas no conteúdo desejado. Note-se que esta aplicação já se encontra pronta para uso na plataforma Android.

O escopo deste trabalho está em demonstrar a viabilidade do uso de um chaveiro criptográfico em dispositivo móvel por meio de consultas HTTP aos web services desenvolvidos, na forma de um um software com serviços desenvolvidos para demonstrar essa viabilidade e testar a proposta.

Abaixo uma representação simplificada da proposta, exibindo os principais elementos envolvidos numa operação de criptografia:

Legenda: representação de uma operação de criptografia com chaveiro em dispositivo móvel Quando necessário, será pedida na tela do usuário a senha de sua chave privada para realizar operações de assinatura e descriptografia.

Legenda: ilustração de como a chamada de um serviço criptográfico aciona o Open KeyChain que, por sua vez, pede a senha do chaveiro do usuário para proceder.

Legenda: Requisição de criptografia de uma mensagem à ser enviada para alice@email.com

5.2 Operações dos Webservices

Os webservices respondem através de um servidor web em execução no dispositivo móvel. Aplicações clientes capazes de enviar mensagens no formato especificado à frente poderão usufruir dos recursos do chaveiro no celular.

A forma de implementação desta demonstração adota um modelo assíncrono para as operações de criptografia e descriptografia. Essa forma foi escolhida pois os aplicativos móveis são geralmente desenvolvidos explorando-se recursos assíncronos e o webservice precisa tratar os casos em que o usuário deve interagir com a tela sem bloquear as chamadas ao serviço de forma indefinida. Dessa forma, contamos na demonstração deste trabalho com quatro operações básicas, sendo duas delas de pedido e duas de consulta de resultados destes. As operações são as seguintes:

- Pedido para criptografar um novo conteúdo endereçado à um destinatário

Tabela 5.1: *Atributos da mensagem JSON de pedido de criptografia de conteúdo*

Chave	Tipo do conteúdo	Descrição

- Consulta a um pedido de criptografia anterior
- Pedido para descriptografar um novo conteúdo recebido
- Consulta a um pedido de descriptografia realizado anteriormente

Seguem nas próximas subseções o detalhamento destes serviços.

5.2.1 Autorização para utilizar os serviços

Para que uma aplicação cliente utilize os serviços ela deve usar uma chave de segurança gerada no aplicativo móvel. Todas as requisições devem contar com o cabeçalho Authorization preenchido com uma chave aleatória, exposta no dispositivo do usuário. A aplicação cliente deve ser atualizada com a chave atual, do contrário as suas requisições serão negadas pelo serviço. com o código HTTP 403 - Unauthorized e uma mensagem indicando que a chave está vazia ou incorreta.

5.2.2 Criptografar um novo conteúdo

Esta operação demanda um conteúdo textual para ser encriptado e o e-mail do destinatário. A chave pública do destinatário deve estar importada na instalação do Open KeyChain no dispositivo móvel.

Legenda: Funcionamento de uma requisição de encriptação com assinatura

- **Endpoint**: `/cryptows/encrypt-content`
- **Método HTTP**: POST
- **Content-type**: application/json

Para criptografar um novo conteúdo deve ser enviado um objeto JSON com os seguintes atributos:

- **content** (String) - A mensagem que será encriptada.
- **receiver** (String) - E-mail do destinatário da mensagem. Sua chave pública deve estar no chaveiro do Open KeyChain

Exemplo:

Código 5.1 Mensagem do pedido de criptografia

```
1 {
2       "content": "Mensagem para ser encriptada",
3       "receiver": "bob@email.com"
4 }
```

A resposta deste serviço em caso de sucesso fará uso do código HTTP 200 - OK indicando que o processamento foi iniciado. A aplicação cliente receberá uma resposta com o identificador desta ação. Ele deve ser guardado e usado posteriormente para consultar o resultado do pedido de criptografia. O formato dessa resposta conterá os seguintes dados, em formato JSON:

- **requestId** (String) - Identificador gerado para consulta posterior do processamento da encriptação
- **code** (Número inteiro) - Código HTTP referente ao sucesso ou falha da operação
- **time** (Número / Timestamp) - Timestamp do momento do recebimento da requisição pelo aplicativo no dispositivo

Exemplo:

Código 5.2 Resposta do pedido de criptografia

```
1 {
2       "requestId": "123e4567-e89b-12d3-a456-426655440000",
3       "code": 200,
4       "time": 1480902494377
5 }
```

5.2.3 Consultar resultado da criptografia de conteúdo

Esta operação somente exige o identificador do do pedido anterior de criptografia, chamado na resposta daquele pedido de requestId. Esse identificador deve ser informado na URL de consulta.

Legenda: diagrama com o fluxo de consulta do resultado de uma operação de criptografia

- **Endpoint**: `/cryptows/encrypt-content/requestId/123e4567-e89b-12d3-a456-426655`
- **Método HTTP**: GET
- **Content-type**: application/json

A resposta deste serviço em caso de sucesso fará uso do código HTTP 200 - OK indicando que o processamento foi concluído. Caso a aplicação no celular ainda esteja processando a requisição, o código HTTP 404 - Not Found é retornado. A aplicação cliente deve tentar novamente em alguns segundos. Em caso de retorno com sucesso a mensagem criptografada será descartada pelo serviço para poupar recursos do dispositivo móvel. O formato dessa resposta conterá os seguintes dados, em formato JSON:

- **cipherContent** (String) - Mensagem criptografada com a chave pública do usuário informado em ?receiver?, no ato da requisição de criptografia
- **code** (Número inteiro) - Código HTTP referente ao sucesso ou falha da operação
- **statusMessage** (String) - Mensagem auxiliar do resultado da operação. Pode conter detalhes em caso de erros durante o processamento.

Exemplo em caso de processamento concluído:

5.2.4 Descriptografar uma mensagem PGP recebida

Esta operação demanda uma mensagem em formato OpenPGP em ASCII Armour para uma tentativa de desencriptação. O formato ASCII Armour permite que a mensagem possa ser enviada com formato JSON sem mais processamento, visto que JSON não suporta dados binário. Essa operação somente é possível se o Open KeyChain contém a chave privada equivalente à chave pública utilizada para criptografia. O conteúdo não necessariamente precisa ter sido encriptado usando o webservice apresentado no item 6.1.1, uma vez que o padrão OpenPGP não leva isso em conta.

- **Endpoint**: `/cryptows/decrypt-content`
- **Método HTTP**: POST
- **Content-type**: application/json

Para descriptografar um novo conteúdo deve ser enviado um objeto JSON com os seguintes atributos:

- **content** (String / Mensagem OpenPGP) - A mensagem que deve ser desencriptada com uma das chaves privadas conhecidas

Exemplo:

A resposta deste serviço em caso de sucesso fará uso do código HTTP 200 - OK indicando que o processamento foi iniciado. A aplicação cliente receberá uma resposta com o protocolo desta ação. Ele deve ser guardado e usado posteriormente para consultar o resultado do pedido de criptografia. O formato dessa resposta conterá os seguintes dados, em formato JSON:

- **requestId** (String) - Identificador gerado para consulta posterior do processamento da decriptação
- **code** (Número inteiro) - Código HTTP referente ao sucesso ou falha da operação
- **time** (Número / Timestamp) - Timestamp do momento do recebimento da requisição pelo aplicativo no dispositivo

Exemplo:

5.2.5 Consultar resultado da descriptografia de conteúdo

Esta operação somente exige o identificador do do pedido anterior de criptografia, chamado na resposta daquele pedido de requestId. Esse identificador deve ser informado na URL de consulta.

- **Endpoint**: `/cryptows/decrypt-content/protocol/123e4567-e89b-12d3-a456-42665544`
- **Método HTTP**: GET
- **Content-type**: application/json

A resposta deste serviço em caso de sucesso fará uso do código HTTP 200 - OK indicando que o processamento foi concluído. Caso a aplicação no celular ainda esteja em processamento a requisição, o código HTTP 404 - Not Found é retornado. A aplicação cliente deve tentar novamente em alguns segundos. O formato dessa resposta conterá os seguintes dados, em formato JSON:

- **plainContent** (String) - Mensagem descriptografada com a chave privada do usuário.
- **code** (Número inteiro) - Código HTTP referente ao sucesso ou falha da operação
- **statusMessage** (String) - Mensagem auxiliar do resultado da operação. Pode conter detalhes em caso de erros durante o processamento.

Exemplo em caso de processamento concluído: "plainContent": "Uma mensagem que foi enviada", "code": 200, "statusMessage": ?Requisicão processada com sucesso?

Exemplo em caso de processamento ainda em andamento: "plainContent": , "code": 404, "statusMessage": ?O processamento ainda não foi concluído.?

CAPÍTULO 6

Experimento

Para verificar a viabilidade da proposta de serviços criptográficos funcionando a partir de um dispositivo móvel, foi desenvolvido neste trabalho de conclusão um aplicativo que contém algumas funcionalidades demonstrativas de tais serviços e uma aplicação cliente para verificação do seu funcionamento de forma simplificada. A aplicação desenvolvida faz uso dos serviços de uma outra aplicação Android chamada Open KeyChain. Ela é em uma carteira de chaves PGP com uma interface simples para o usuário final.

O protocolo de comunicação e troca de mensagens segue a especificação apresentada anteriormente. As operações foram implementadas em um aplicativo Android de modo a demonstrar de forma minimizada a viabilidade da proposta.

6.1 Implementação dos serviços para o chaveiro PGP

Os serviços PGP foram implementados a partir de um aplicativo Android seguindo as especificações da proposta no capítulo anterior. Ao iniciar o aplicativo exibe seu IP e porta para os serviços, que devem ser configurados em aplicações clientes para a correta invocação dos serviços.

Para sua implementação foram usadas os seguintes itens de configuração detalhados no anexo 6. O dispositivo móvel usado no desenvolvimento e testes está detalhado no anexo 5. Os detalhes do ambiente de desenvolvimento utilizado em todos os casos está no anexo 7. O anexo 8 contém um exemplo de aplicação cliente capaz de consumir os serviços fornecidos a partir do dispositivo móvel.

A arquitetura adotada pode ser representada pelo seguinte diagrama, as principais entidades da aplicação:

Legenda: Principais camadas na implementação dos webservices em dispositivo móvel

São destacados nesta implementação:

- **Serviço HTTP**: responsável por lidar com novas requisições e despachar respostas de requisições de consulta. Caso o resultado já esteja disponpivel em RequestRe-

pository, este serviço o retorna para a aplicação cliente. Também é responsável por validar a chave de acesso que deve ser informada pelas aplicações clientes para fazer uso do serviço.

- **Serviço OpenPGP**: contém as rotinas de operações criptográficas. Gerencia o que está disponível para o serviço HTTP quando este precisa realizar chamadas de ações criptográficas.
- **EncryptCallback** - Classe que lida com os eventos de criptografia
- **DecryptCallback** - Classe que lida com os eventos de descriptografia
- **Message**: representa toda mensagem de entrada, seja no pedido de uma operação criptográfica, seja na consulta do resultado de seu processamento
- **Response**: representa todas as saídas da aplicação. Contém o resultado da operação requisitada, além de poder transportar o requestID quando gerado e os conteúdos, tanto criptografados quanto em formato plano/original.

CAPÍTULO 7

Elementos do texto

7.1 Figuras

Rótulos de figuras e tabelas devem ser centralizados se tiverem até uma linha (Figura 8.1), caso contrário devem estar justificados e identados em ambas as margens, como mostrado na Figura 8.2. Essa formatação já é realizada automaticamente pela classe inf-ufg.

Os compiladores LaTeX provêem um mecanismo bastante simples para inclusão de figuras, o que pode ser feito com o auxílio de várias classes auxiliares (as mais comuns são `graphic` e `graphicx`). A classe `inf-ufg` usa o comando `\includegraphics`, da classe `graphicx`, para a inclusão de figuras e não é necessário você colocar a extensão do arquivo neste comando. Por exemplo, para a figura 8.1 os comandos usados foram:

```
\begin{figure}[htb]
 \centering
 \includegraphics[width=0.40\textwidth]{./fig/exemploFig1}
 \caption{Uma figura típica.}
 \label{fig:exemploFig1}
\end{figure}
```

Ao se usar o compilador LaTeX, as figuras podem estar nos formatos *eps* e *ps*. Ao se usar o PDFLaTeX, as figuras podem estar nos formatos *png*, *jpg*, *pdf* e *mps*. A classe `graphicx` também pode ser usada para a inclusão de figuras, nos formatos listados, ao se usar o PDFLaTeX. Os comandos necessários são os mesmos ao se incluir figuras ao se usar o compilador LaTeX. O uso do comando `\includegraphics` faz com com que PDFLaTeX procure primeiro por figuras com extensão *pdf*, depois *jpg*, depois *mps* e por último *png*. Aqui também não é necessário especificar a extensão do arquivo.

Para a inclusão das figuras 8.1 à 8.3 os comandos usados, tanto no LaTeX quanto no PDFLaTeX, seriam os mesmos. É claro que em cada caso devem estar disponíveis as figuras nos formatos suportados por cada compilador. Por exemplo, para a inclusão da figura 8.3 foram usados:

```
 \begin{figure}[H]
  \centering
  \includegraphics[width=0.40\textwidth]{./fig/exemploFig3}
  \caption{Figura incluída no texto com a classe graphicx.}
  \label{fig:exemploFig3}
\end{figure}
```

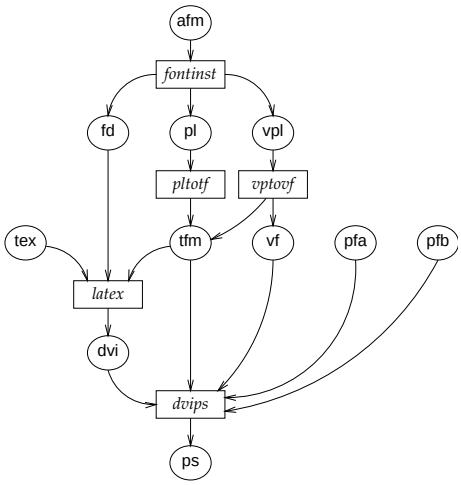


Figura 7.1: *Uma figura típica.*

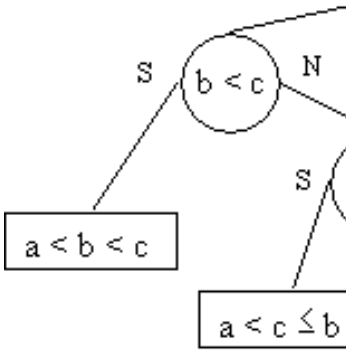


Figura 7.2: *Esta figura é um exemplo de um rótulo de figura que ocupa mais de uma linha, devendo ser identado e justificado.*

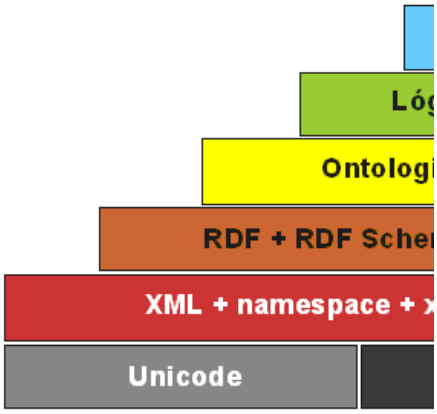
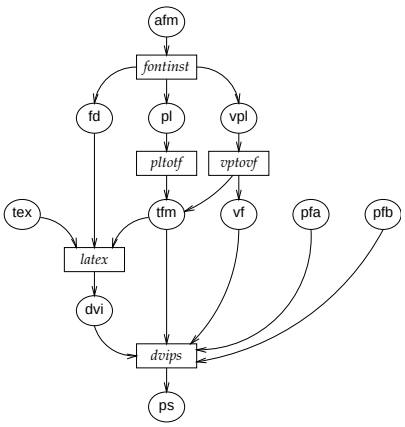


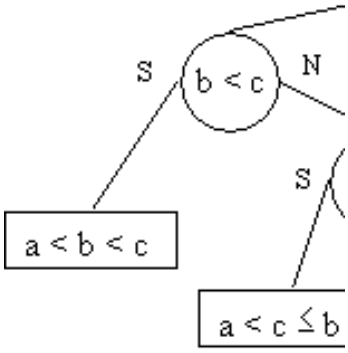
Figura 7.3: *Figura incluída no texto com a classe graphicx.*

7.1.1 Subfiguras

A classe `subfigure` pode ser usada para a inclusão de figuras dentro de figuras (consulte a documentação da classe para maiores detalhes). Por exemplo, a Figura 8.4 contém duas subfiguras. Estas podem ser referencidas por rótulos independentes, ou seja, podem ser referenciadas como Figuras 8.4(a) e 8.4(b) ou Subfiguras (a) e (b).



(a) *Primeira subfigura.*



(b) *Segunda subfigura (um pedaço).*

Figura 7.4: *(a) e (b) representam dois exemplos do uso de subfiguras dentro de uma única figura.*

A figura 8.4 foi incluída com os comandos listados a seguir. Observe que há rótulos independentes para cada uma das subfiguras e um rótulo geral para a figura, os quais podem ser todos referenciados.

```
\begin{figure}[h]
 \centering
  \subfigure[Primeira subfigura.]
   {
    \includegraphics[width=0.35\textwidth]{./fig/exemploFig1}
    \label{subfig:ex1}
   } \qquad
  \subfigure[Segunda subfigura (um pedaço).]
   {
    \includegraphics[width=0.30\textwidth]{./fig/exemploFig2}
    \label{subfig:ex2}
   }
   \caption{{\subref{subfig:ex1}} e {\subref{subfig:ex2}} representam
            dois exemplos do uso de subfiguras dentro de uma única
            figura.}
  \label{fig:subfiguras}
\end{figure}
```

Caso uma subfiguras não tenha rótulo, para evitar que o apenas o número da mesma apareça na Lista de Figuras, use o comando `\subfigure[][]`. Caso uma subfigura tenha rótulo e deseja-se evitar que a mesma apareça na Lista de Figuras, use o comando `\subfigure[][Rótulo]`.

7.2 Tabelas

Em tabelas, deve-se evitar usar cor de fundo diferente do branco e o uso de linhas grossas ou duplas. Ao relatar dados empíricos, não se deve usar mais dígitos decimais do aqueles que possam ser garantidos pela sua precisão e reprodutibilidade. Rótulos de tabelas devem ser colocados antes das mesmas (veja a Tabela 8.1).

7.3 Algoritmos

Algoritmos devem ser representados no formato do Algoritmo 8.1, que foi descrito com o uso da classe algorithm2e. A rigor não é obrigatório o uso dessa classe,

contudo o uso da mesma permite que seja gerada automaticamente uma lista de algoritmos logo após o sumário.

Algoritmo 7.1: $MSR(A, i, j)$

Entrada: vetor $A[i\,..\,j]$, inteiros não negativos i e j.
Saída: vetor $A[i\,..\,j]$ ordenado.

```
1 n ← j − i.
2 se (n < 4) então
3 |   Ordene com ≤ 3 comparações.
4 senão
5 |   Divida A em ⌈√n⌉ subvetores de comprimento máximo ⌊√n⌋.
6 |   Aplique MSR a cada um dos subvetores.
7 |   Intercale os subvetores.
8 fim
```

7.4 Códigos de Programa

Códigos de programa podem ser importados, mantendo-se a formatação original, conforme se pode ver no exemplo do Código 8.1. Este exemplo usa o ambiente codigo, definido na classe inf-ufg, que permite que uma lista de programas seja gerada automaticamente logo após o sumário.

Código 7.1 `insertionsort()`

```
1  void insertionSort( int* v, int n )
2  {
3    int i   = 0;
4    int j   = 1;
5    int aux = 0;
6
7    while (j < n)
8    {
9      aux = v[j];
10     i   = j - 1;
11     while ((i >= 0) && (v[i] > aux))
12     {
13       v[i + 1] = v[i];
14       i = i - 1;
15     }
16     v[i + 1] = aux;
17     j = j + 1;
18   }
19 }
```

7.5 Teoremas, Corolários e Demonstrações

O uso do ambiente theorem permite a escrita de teoremas, como no exemplo a seguir:

```
\begin{theorem}[Pitágoras]
Em todo triângulo retângulo o quadrado do comprimento
da hipotenusa é igual a soma dos quadrados dos
comprimentos dos catetos.
\end{theorem}
```

O resultado é o mostrado a seguir:

Teorema 7.1 (Pitágoras) *Em todo triângulo retângulo o quadrado do comprimento da hipotenusa é igual a soma dos quadrados dos comprimentos dos catetos.*

Da mesma forma pode-se usar o ambiente proof para demonstrações de teoremas:

```
\begin{proof}
Para demonstrar o Teorema de Pitágoras \dots
\end{proof}
```

Neste caso, o resultado é:

Prova. Para demonstrar o Teorema de Pitágoras ... □

Além desses dois ambientes, estão definidos os ambientes definition (Definição), corollary (Corolário), lemma (Lema)), proposition (Proposição), comment (Observação).

7.6 Citações Longas

Segundo as normas da ABNT, uma citação longa (mais de 3 linhas) deve seguir uma formação especial. Para tanto foi criado o ambiente `citacao`, o qual é baseado no ambiente de mesmo nome definido pelo grupo ABNTex [**?**]:

> Uma citação longa (mais de 3 linhas) deve vir em parágrafo separado, com recuo de 4cm da margem esquerda, em fonte menor, sem as aspas [**?**, 4.4] e com espaçamento simples [**?**, 5.3]. Uma regra de como fazer citações em geral não é simples. É prudente ler [**?**] se você optar for fazer uso freqüente de citações. Para satisfazer às exigências tipográficas que a norma pede para citações longas, use o ambiente citacao.

Este exemplo de citação longa foi produzido com o uso do ambiente `citacao`, como descrito logo a seguir:

```
\begin{citacao}
Uma citação longa (mais de 3 linhas) deve vir em parágrafo
separado, com recuo de 4cm da margem esquerda, em fonte menor,
sem as aspas \cite[4.4]{NBR10520:2001} e com espaçamento
simples \cite[5.3]{NBR14724:2001}. Uma regra de como fazer
citações em geral não é simples. É prudente ler
\cite{NBR10520:2001} se você optar for fazer uso freqüente
de citações. Para satisfazer às exigências tipográficas que a
norma pede para citações longas, use o ambiente citacao.
\end{citacao}
```

7.7 Referências Bibliográficas

Esta seção mostra exemplos de uso de referências bibliográficas com BIBTEX e do comando `\cite`. Muitas das entradas listadas na página 50 foram obtidas de: http://liinwww.ira.uka.de/bibliography/index.html. Outro grande repositório de referências já em formato BIBTEX está disponível em: http://www.math.utah.edu/ beebe/bibliographies.html.

As referências bibliográficas devem ser não ambíguas e uniformes. Recomenda-se usar números entre colchetes, como por exemplo [**?**], [**?**] e [**?**]. O comando `\nocite` não produz texto, mas permite que a entrada seja incluída nas referências. Por exemplo, o comando `\nocite{Ber1970}` gera na lista de referências bibliográficas a entrada referente à chave Ber1970, mas não inclui nenhuma referência no texto. O comando `\nocite{*}` faz com que todas as entradas do arquivo de dados do BIBTEX sejam incluídas nas referências.

Existem vários livros sobre LATEX, como [**?**, **?**, **?**], embora os mais famosos sejam sem dúvida [**?**] e [**?**]. Para converter documentos LATEX para HTML veja [**?**, pg.1–10].

Tabela 7.1: *Conteúdo do diretório [**?**]*

Tag	Comprimento	Início		Tag	Comprimento	Início
001	0020	00000		100	0032	00235
003	0004	00020		245	0087	00267
005	0017	00024		246	0036	00354
008	0041	00041		250	0012	00390
010	0024	00082		260	0037	00402
020	0025	00106		300	0029	00439
020	0044	00131		500	0042	00468
040	0018	00175		520	0220	00510
050	0024	00193		650	0033	00730
082	0018	00217		650	0012	00763

CAPÍTULO 8

Elementos do texto

8.1 Figuras

Rótulos de figuras e tabelas devem ser centralizados se tiverem até uma linha (Figura 8.1), caso contrário devem estar justificados e identados em ambas as margens, como mostrado na Figura 8.2. Essa formatação já é realizada automaticamente pela classe inf-ufg.

Os compiladores LaTeX provêem um mecanismo bastante simples para inclusão de figuras, o que pode ser feito com o auxílio de várias classes auxiliares (as mais comuns são `graphic` e `graphicx`). A classe `inf-ufg` usa o comando `\includegraphics`, da classe `graphicx`, para a inclusão de figuras e não é necessário você colocar a extensão do arquivo neste comando. Por exemplo, para a figura 8.1 os comandos usados foram:

```
\begin{figure}[htb]
 \centering
 \includegraphics[width=0.40\textwidth]{./fig/exemploFig1}
 \caption{Uma figura típica.}
 \label{fig:exemploFig1}
\end{figure}
```

Ao se usar o compilador LaTeX, as figuras podem estar nos formatos *eps* e *ps*. Ao se usar o PDFLaTeX, as figuras podem estar nos formatos *png*, *jpg*, *pdf* e *mps*. A classe `graphicx` também pode ser usada para a inclusão de figuras, nos formatos listados, ao se usar o PDFLaTeX. Os comandos necessários são os mesmos ao se incluir figuras ao se usar o compilador LaTeX. O uso do comando `\includegraphics` faz com com que PDFLaTeX procure primeiro por figuras com extensão *pdf*, depois *jpg*, depois *mps* e por último *png*. Aqui também não é necessário especificar a extensão do arquivo.

Para a inclusão das figuras 8.1 à 8.3 os comandos usados, tanto no LaTeX quanto no PDFLaTeX, seriam os mesmos. É claro que em cada caso devem estar disponíveis as figuras nos formatos suportados por cada compilador. Por exemplo, para a inclusão da figura 8.3 foram usados:

```
 \begin{figure}[H]
  \centering
  \includegraphics[width=0.40\textwidth]{./fig/exemploFig3}
  \caption{Figura incluída no texto com a classe graphicx.}
  \label{fig:exemploFig3}
\end{figure}
```

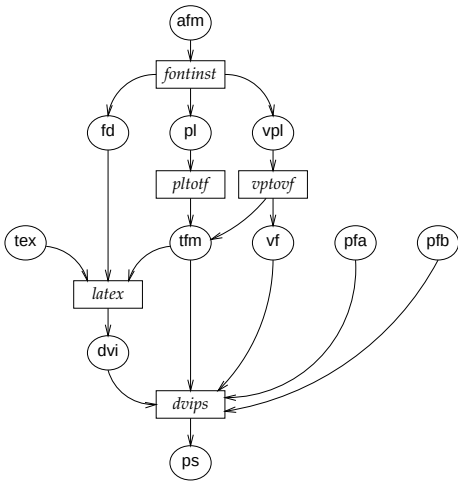


Figura 8.1: *Uma figura típica.*

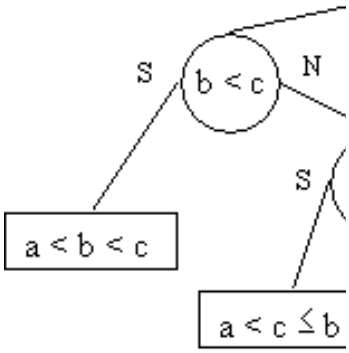


Figura 8.2: *Esta figura é um exemplo de um rótulo de figura que ocupa mais de uma linha, devendo ser identado e justificado.*

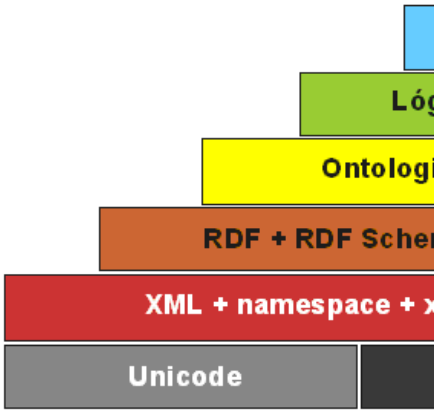
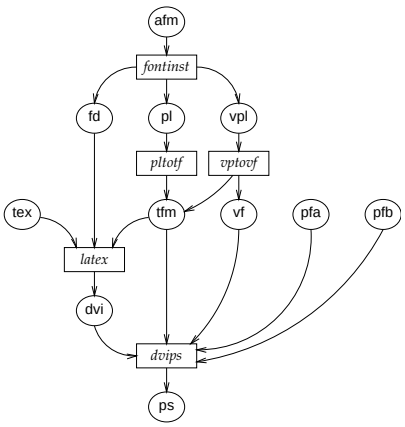


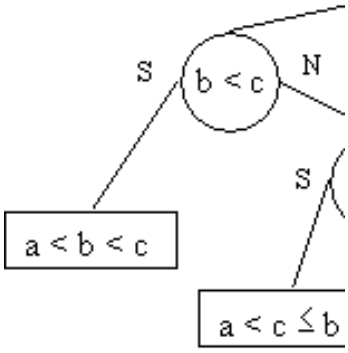
Figura 8.3: *Figura incluída no texto com a classe graphicx.*

8.1.1 Subfiguras

A classe `subfigure` pode ser usada para a inclusão de figuras dentro de figuras (consulte a documentação da classe para maiores detalhes). Por exemplo, a Figura 8.4 contém duas subfiguras. Estas podem ser referencidas por rótulos independentes, ou seja, podem ser referenciadas como Figuras 8.4(a) e 8.4(b) ou Subfiguras (a) e (b).



(a) *Primeira subfigura.*



(b) *Segunda subfigura (um pedaço).*

Figura 8.4: *(a) e (b) representam dois exemplos do uso de subfiguras dentro de uma única figura.*

A figura 8.4 foi incluída com os comandos listados a seguir. Observe que há rótulos independentes para cada uma das subfiguras e um rótulo geral para a figura, os quais podem ser todos referenciados.

```
\begin{figure}[h]
 \centering
  \subfigure[Primeira subfigura.]
   {
    \includegraphics[width=0.35\textwidth]{./fig/exemploFig1}
    \label{subfig:ex1}
   } \qquad
  \subfigure[Segunda subfigura (um pedaço).]
   {
    \includegraphics[width=0.30\textwidth]{./fig/exemploFig2}
    \label{subfig:ex2}
   }
   \caption{{\subref{subfig:ex1}} e {\subref{subfig:ex2}} representam
            dois exemplos do uso de subfiguras dentro de uma única
            figura.}
  \label{fig:subfiguras}
\end{figure}
```

Caso uma subfiguras não tenha rótulo, para evitar que o apenas o número da mesma apareça na Lista de Figuras, use o comando `\subfigure[][]`. Caso uma subfigura tenha rótulo e deseja-se evitar que a mesma apareça na Lista de Figuras, use o comando `\subfigure[][Rótulo]`.

8.2 Tabelas

Em tabelas, deve-se evitar usar cor de fundo diferente do branco e o uso de linhas grossas ou duplas. Ao relatar dados empíricos, não se deve usar mais dígitos decimais do aqueles que possam ser garantidos pela sua precisão e reprodutibilidade. Rótulos de tabelas devem ser colocados antes das mesmas (veja a Tabela 8.1).

8.3 Algoritmos

Algoritmos devem ser representados no formato do Algoritmo 8.1, que foi descrito com o uso da classe algorithm2e. A rigor não é obrigatório o uso dessa classe,

contudo o uso da mesma permite que seja gerada automaticamente uma lista de algoritmos logo após o sumário.

Algoritmo 8.1: $MSR(A, i, j)$

Entrada: vetor $A[i\,..\,j]$, inteiros não negativos i e j.
Saída: vetor $A[i\,..\,j]$ ordenado.

```
1 n ← j − i.
2 se (n < 4) então
3 |   Ordene com ≤ 3 comparações.
4 senão
5 |   Divida A em ⌈√n⌉ subvetores de comprimento máximo ⌊√n⌋.
6 |   Aplique MSR a cada um dos subvetores.
7 |   Intercale os subvetores.
8 fim
```

8.4 Códigos de Programa

Códigos de programa podem ser importados, mantendo-se a formatação original, conforme se pode ver no exemplo do Código 8.1. Este exemplo usa o ambiente codigo, definido na classe inf-ufg, que permite que uma lista de programas seja gerada automaticamente logo após o sumário.

Código 8.1 `insertionsort()`

```
1  void insertionSort( int* v, int n )
2  {
3    int i   = 0;
4    int j   = 1;
5    int aux = 0;
6
7    while (j < n)
8    {
9      aux = v[j];
10     i   = j - 1;
11     while ((i >= 0) && (v[i] > aux))
12     {
13       v[i + 1] = v[i];
14       i = i - 1;
15     }
16     v[i + 1] = aux;
17     j = j + 1;
18   }
19 }
```

8.5 Teoremas, Corolários e Demonstrações

O uso do ambiente theorem permite a escrita de teoremas, como no exemplo a seguir:

```
\begin{theorem}[Pitágoras]
Em todo triângulo retângulo o quadrado do comprimento
da hipotenusa é igual a soma dos quadrados dos
comprimentos dos catetos.
\end{theorem}
```

O resultado é o mostrado a seguir:

Teorema 8.1 (Pitágoras) *Em todo triângulo retângulo o quadrado do comprimento da hipotenusa é igual a soma dos quadrados dos comprimentos dos catetos.*

Da mesma forma pode-se usar o ambiente proof para demonstrações de teoremas:

```
\begin{proof}
Para demonstrar o Teorema de Pitágoras \dots
\end{proof}
```

Neste caso, o resultado é:

Prova. Para demonstrar o Teorema de Pitágoras ... □

Além desses dois ambientes, estão definidos os ambientes definition (Definição), corollary (Corolário), lemma (Lema)), proposition (Proposição), comment (Observação).

8.6 Citações Longas

Segundo as normas da ABNT, uma citação longa (mais de 3 linhas) deve seguir uma formação especial. Para tanto foi criado o ambiente `citacao`, o qual é baseado no ambiente de mesmo nome definido pelo grupo ABNTex [**?**]:

> Uma citação longa (mais de 3 linhas) deve vir em parágrafo separado, com recuo de 4cm da margem esquerda, em fonte menor, sem as aspas [**?**, 4.4] e com espaçamento simples [**?**, 5.3]. Uma regra de como fazer citações em geral não é simples. É prudente ler [**?**] se você optar for fazer uso freqüente de citações. Para satisfazer às exigências tipográficas que a norma pede para citações longas, use o ambiente citacao.

Este exemplo de citação longa foi produzido com o uso do ambiente `citacao`, como descrito logo a seguir:

```
\begin{citacao}
Uma citação longa (mais de 3 linhas) deve vir em parágrafo
separado, com recuo de 4cm da margem esquerda, em fonte menor,
sem as aspas \cite[4.4]{NBR10520:2001} e com espaçamento
simples \cite[5.3]{NBR14724:2001}. Uma regra de como fazer
citações em geral não é simples. É prudente ler
\cite{NBR10520:2001} se você optar for fazer uso freqüente
de citações. Para satisfazer às exigências tipográficas que a
norma pede para citações longas, use o ambiente citacao.
\end{citacao}
```

8.7 Referências Bibliográficas

Esta seção mostra exemplos de uso de referências bibliográficas com BIBTEX e do comando `\cite`. Muitas das entradas listadas na página 50 foram obtidas de: http://liinwww.ira.uka.de/bibliography/index.html. Outro grande repositório de referências já em formato BIBTEX está disponível em: http://www.math.utah.edu/ beebe/bibliographies.html.

As referências bibliográficas devem ser não ambíguas e uniformes. Recomenda-se usar números entre colchetes, como por exemplo [**?**], [**?**] e [**?**]. O comando `\nocite` não produz texto, mas permite que a entrada seja incluída nas referências. Por exemplo, o comando `\nocite{Ber1970}` gera na lista de referências bibliográficas a entrada referente à chave Ber1970, mas não inclui nenhuma referência no texto. O comando `\nocite{*}` faz com que todas as entradas do arquivo de dados do BIBTEX sejam incluídas nas referências.

Existem vários livros sobre LATEX, como [**?**, **?**, **?**], embora os mais famosos sejam sem dúvida [**?**] e [**?**]. Para converter documentos LATEX para HTML veja [**?**, pg.1–10].

Tabela 8.1: *Conteúdo do diretório [**?**]*

Tag	Comprimento	Início		Tag	Comprimento	Início
001	0020	00000		100	0032	00235
003	0004	00020		245	0087	00267
005	0017	00024		246	0036	00354
008	0041	00041		250	0012	00390
010	0024	00082		260	0037	00402
020	0025	00106		300	0029	00439
020	0044	00131		500	0042	00468
040	0018	00175		520	0220	00510
050	0024	00193		650	0033	00730
082	0018	00217		650	0012	00763

APÊNDICE A

Exemplo de um Apêndice

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess

são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`.

Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndicess são iniciados com o comando `\apendices`. Apêndi-

cess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices. Apêndicess são iniciados com o comando \apendices.

APÊNDICE B

Exemplo de Outro Apêndice

Texto do Apêndice B.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`. Apêndices são iniciados com o comando `\apendices`.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndi-

ces são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.

Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices. Apêndices são iniciados com o comando \apendices.