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. 36p. 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. 36p. 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.

Este documento mostra como usar o LaTeX com a classe inf-ufg para formatar teses, dissertações, monografias e relatórios de conclusão de curso, segundo o padrão adotado pelo Instituto de Informática da UFG. Este documento e a classe inf-ufg foram, em grande parte, copiados e adaptados da classe thesisPUC e do texto de Thomas Lewiner [**?**] que descreve a sua utilização.

LaTeX é um sistema de editoração eletrônica muito usado para produzir documentos científicos de alta qualidade tipográfica. O sistema também é útil para produzir todos os tipos de outros documentos, desde simples cartas até livros completos.

Se você precisar de algum material de apoio referente ao LaTeX, dê uma olhada em um dos sites do Comprehensive TEX Archive Network (CTAN). O site está em www.ctan.org. Todos os pacotes podem ser obtidos via FTP ftp://www.ctan.org e existem vários servidores em todo o mundo. Eles podem ser encontrados, por exemplo, em ftp://ctan.tug.org (EUA), ftp://ftp.dante.de (Alemanha), ftp://ftp.tex.ac.uk (Reino Unido).

Você pode encontrar uma grande quantidade de informações e dicas na página dos usuários brasileiros de LaTeX (TeX-BR). O endereço é http://biquinho.furg.br/tex-br/. Tanto no CTAN quanto no TeX-BR estão disponíveis bons documentos em português sobre o LaTeX. Em particular no CTAN, está disponível uma introdução bastante completa em português: CTAN:/tex-archive/info/lshort/portuguese-BR/. No TeX-BR também existe um documento com exemplos de uso de LaTeX e de vários pacotes: http://biquinho.furg.br/tex-br/doc/LaTeX-demo/ . O objetivo é ser, através de exemplos, um guia para o usuário de LaTeX iniciante e intermediário, podendo, ainda, servir como um guia de referência rápida para usuários avançados.

Se você quer usar o LaTeX em seu computador, verifique em quais sistemas ele está disponível em CTAN:/tex-archive/systems. Em particular para MS Windows, o sistema gratuito MikTeX, disponível no CTAN e no site www.miktex.org é completo e atualizado de todas as opções que você poderia precisar para editar o seu texto.

O estilo inf-ufg se integra completamente ao LaTeX 2ε. Uma tese, dissertação ou

monografia escrita no estilo padrão do LaTeX para teses (estilo `report`) pode ser formatada em 15 minutos para se adaptar às normas da UFG.

O estilo inf-ufg foi desenhado para minimizar a quantidade de texto e de comandos necessários para escrever a sua dissertação. Só é preciso inserir algumas macros no início do seu arquivo LaTeX, precisando os dados bibliográficos da sua dissertação (por exemplo o seu nome, o titulo da dissertação...). Em seguida, cada página dos elementos pré-textuais será formatada usando macros ou ambientes específicos. O corpo do texto é editado normalmente. Finalmente, as referências bibliográficas podem ser entradas manualmente (via o comando `\bibitem` do LaTeX padrão) ou usando o sistema BiBTeX (muito mais recomendável). Neste caso, os arquivos `inf-ufg.bst` e `abnt-alf.bst` permitem a formatação das referências bibliográficas segundo as normas da UFG.

CAPÍTULO 2

Descrição da classe inf-ufg

2.1 Opções da classe

Para usar esta classe num documento LaTeX 2ε, coloque os arquivos `inf-ufg.cls`, `inf-ufg.bst`, `abnt-num.bst`, `atbeginend.sty` e `tocloft.sty` numa pasta onde o compilador LaTeX pode achá–lo (normalmente na mesma pasta que seu arquivo `.tex`), e defina–o como o estilo do seu documento. Por exemplo, uma dissertação de mestrado que usa o modelo abnt de citações bibliográficas:

```
\documentclass[dissertacao,abnt]{inf-ufg}
...
\begin{document}
```

As opções da classe são `[tese]` (para tese de doutorado), `[dissertacao]` (para dissertação de mestrado), `[monografia]` (para monografia de curso de especialização e `[relatorio]` (para relatório final de curso de graduação). Se nenhuma opção for declarada, o documento é considerado como uma dissertação de mestrado. Se a opção `[abnt]` for utilizada, as citações bibliográficas serão geradas conforme definido pelo grupo de trabalho abnt-tex. Contudo, o mais recomendável é não utilizar essa opção. Com a opção `[nocolorlinks]` todos os *links* de navegação no texto ficam na cor preta. O ideal é usar esta opção para gerar o arquivo para impressão, pois a qualidade da impressão dos *links* fica superior.

2.2 Parâmetros da classe

Os elementos pré-textuais são definidos página por página e dependem da correta definição dos parâmetros listados a seguir (aqueles que contém um texto/valor padrão não precisam ser definidos, caso atenda a situação do autor do texto que está usando a classe `inf-ufg.cls`):

- `\autor` : Nome completo do autor da tese, começando pelo apelido (ex.: José da Silva);

- `\autorR` : Nome completo do autor da tese, começando pelo nome (ex.: da Silva, José);
- `\titulo` : Título da tese, dissertação, monografia ou relatório de conclusão de curso;
- `\subtitulo` : Se tiver um subtítulo, use este macro para defini–lo;
- `\cidade` : A cidade de edição. A cidade padrão é Goiânia.
- `\dia` : Dia do mês da data de defesa (1–31);
- `\mes` : Mês da data de defesa (1–12);
- `\ano` : Ano da data de defesa;
- `\universidade` : Nome completo da universidade. O nome padrão é Universidade Federal de Goiás;
- `\uni` : Sigla da universidade. A sigla padrão é UFG;
- `\unidade` : Nome da unidade acadêmica. O padrão é Instituto de Informática;
- `\departamento` : Nome do departamento, com maiúscula na primeira letra (para o caso de unidades com mais de um departamento);
- `\programa` : Nome do programa de pós-graduação, com maiúscula na primeira letra. O padrão é Computação;
- `\concentracao` : Nome da área de concentração;
- `\orientador` : Nome completo do orientador, começando pelo apelido;
- `\orientadorR` : Nome completo do orientador, começando pelo nome;
- `\orientadora` : Nome completo da orientadora, começando pelo apelido; use este comando e o próximo se for orientadora e nao orientador.
- `\orientadoraR` : Nome completo do orientadora, começando pelo nome;
- `\coorientador` : Nome completo do co–orientador, começando pelo apelido;
- `\coorientadorR` : Nome completo do co–orientador, começando pelo nome;
- `\coorientadora` : Nome completo da coorientadora, começando pelo apelido; use este comando e o próximo se for coorientadora e nao coorientador.
- `\coorientadoraR` : Nome completo do coorientadora, começando pelo nome;
- `\universidadeco` : Nome da universidade do coorientador;
- `\unico` : Sigla da universidade do coorientador;
- `\unidadeco` : Nome da unidade acadêmica do coorientador.[1]

2.3 Elementos Pré–Textuais

Os elementos pré–textuais são definidos página por página, conforme descritos a seguir:

[1] Se não tiver um co–orientador, não defina esses últimos sete parâmetros.

capa

`\capa` : Gera o modelo da capa externa do trabalho. Esta página servirá apenas como modelo para a encadernação da versão final do texto. Nenhum dado é necessário.

publicação

`\publica` : Gera a autorização para publicação do trabalho em formato eletrônico e disponibilização do mesmo na biblioteca virtual da UFG.

rosto

`\rosto` : Gera a folha de rosto, a qual é a primeira folha interna do trabalho. Nenhum dado é necessário.

aprovação

`\aprovacao` : ambiente para a reprodução do termo de aprovação da Banca Examinadora da tese ou dissertação.

banca

`\banca` : Entrada para o nome dos examinadores, exceto o(s) orientador(es).
`\profa` : Entrada para o nome das examinadoras, exceto o(s) orientador(es).

direitos

`\direitos` : Macro com 2 argumentos para gerar os direitos autorais, o perfil do aluno e a ficha catalográfica da Biblioteca Central da UFG.

- O primeiro argumento é o Perfil do aluno; e
- O segundo argumento é a lista das palavras–chaves para a Ficha Catalográfica.

dedicatória

`\dedicatoria` : ambiente para escrever a dedicatória. É possível trocar o espaçamento dentro desse ambiente do mesmo jeito que no LaTeX padrão.

agradecimentos

`\agradecimentos` : ambiente para escrever os agradecimentos. É possível trocar o espaçamento dentro desse ambiente do mesmo jeito que no LaTeX padrão.

resumo

`\chaves` : A lista das palavras chaves, separadas por ';'. Deve ser definido antes do ambiente `\resumo`, o qual é usado para escrever o resumo em português.

abstract

`\keys` : A lista das palavras chaves em inglês, separadas por ';'. Deve ser definido antes do ambiente `\abstract`, o qual contém 1 argumento e é usado escrever o resumo em inglês. O argumento deve ser o título do trabalho em inglês.

tabelas

`\tabelas` : Macro com 1 argumento opcional para gerar as tabelas. O argumento pode ser:

- nada [] : gera apenas o sumário;
- fig : gera o sumário e uma lista de figuras;
- tab : gera o sumário e uma lista de tabelas;
- alg : gera o sumário e uma lista de algoritmos;
- cod : gera o sumário e uma lista de programas.

Pode-se usar qualquer combinação dessas opções. Por exemplo:

- figtab : gera o sumário e listas de figuras e tabelas,
- figtabcod : gera o sumário e listas de figuras, tabelas e códigos de programas;
- figtabalg : gera o sumário e listas de figuras, tabelas e algoritmos;
- figtabalgcod : gera o sumário e listas de figuras, tabelas, algoritmos e códigos de programas

epígrafe

`\epigrafe` : Macro com 3 argumentos que permite editar um epígrafe. O primeiro argumento é o texto da citação. O segundo argumento é o nome do autor da citação. O terceiro argumento é o título da referência à qual a citação pertence.

CAPÍTULO 3

Elementos do texto

3.1 Figuras

Rótulos de figuras e tabelas devem ser centralizados se tiverem até uma linha (Figura 3.1), caso contrário devem estar justificados e identados em ambas as margens, como mostrado na Figura 3.2. 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 3.1 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 3.1 à 3.3 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 3.3 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}
```

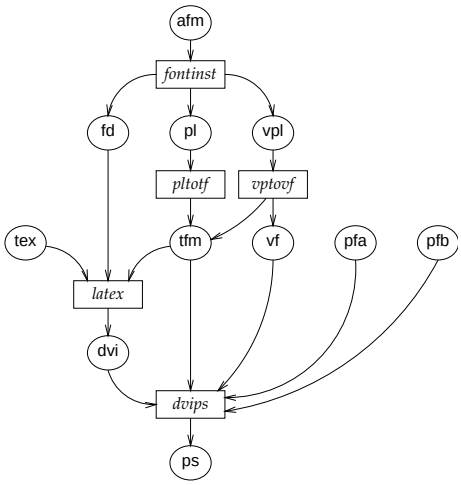


Figura 3.1: *Uma figura típica.*

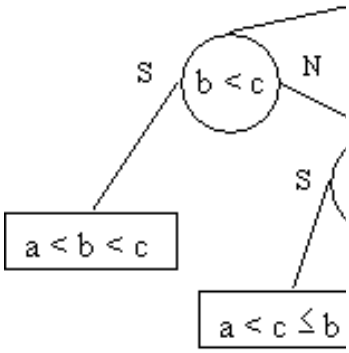


Figura 3.2: *Esta figura é um exemplo de um rótulo de figura que ocupa mais de uma linha, devendo ser identado e justificado.*

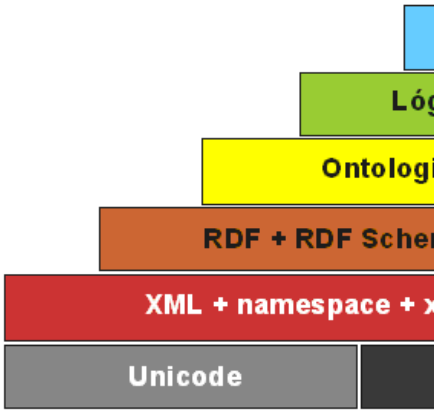
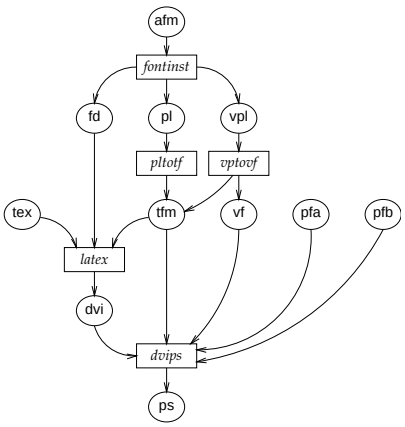


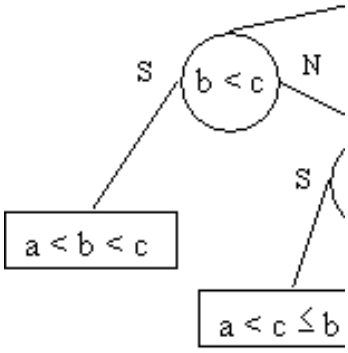
Figura 3.3: *Figura incluída no texto com a classe graphicx.*

3.1.1 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 3.4 contém duas subfiguras. Estas podem ser referencidas por rótulos independentes, ou seja, podem ser referenciadas como Figuras 3.4(a) e 3.4(b) ou Subfiguras (a) e (b).



(a) *Primeira subfigura.*



(b) *Segunda subfigura (um pedaço).*

Figura 3.4: *(a) e (b) representam dois exemplos do uso de subfiguras dentro de uma única figura.*

A figura 3.4 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]`.

3.2 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 3.1).

3.3 Algoritmos

Algoritmos devem ser representados no formato do Algoritmo 3.1, 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 3.1: $MSR(A, i, j)$

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
```

3.4 Códigos de Programa

Códigos de programa podem ser importados, mantendo-se a formatação original, conforme se pode ver no exemplo do Código 3.1. 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 3.1 `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 }
```

3.5 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 3.1 (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).

3.6 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}
```

3.7 Referências Bibliográficas

Esta seção mostra exemplos de uso de referências bibliográficas com BIBTEX e do comando `\cite`. Muitas das entradas listadas na página 29 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 3.1: *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`. 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.

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`. 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.