Cryptography

Ashan J

2024-05-15

Contents

1 Overview of cryptographic **5**

1.1 Substitution ciphers 5

1.2 Cryptographic goals 5

1.3 Basic terminology and concepts 5

1.4 Symmetric-key encryption 5

1.5 Introduction to cryptoanalysis 5

2 Hello bookdown **7**

2.1 A section 7

3 Cross-references **9**

3.1 Chapters and sub-chapters 9

3.2 Captioned figures and tables 9

Chapter 1

Overview of cryptographic

1.0.1 Secure Communication!

- Alice need to send a valuable item to Bob through post. However, there is no guarantee that the item will not be stolen while in transit.
- How can Alice and Bob can come up with a secure way to send the item through the post?
  - What is your solution?
  - Can you improve your solution?

What is Cryptography?
Cryptography (cryptology) is the (mathematical) science of techniques for secure communication in the presence of an adversary.

1.1 Substitution ciphers

1.2 Cryptographic goals

1.3 Basic terminology and concepts

1.4 Symmetric-key encryption

1.5 Introduction to cryptoanalysis

Chapter 2

Hello bookdown

All chapters start with a first-level heading followed by your chapter title, like the line above. There should be only one first-level heading (`#`) per .Rmd file.

2.1 A section

All chapter sections start with a second-level (`##`) or higher heading followed by your section title, like the sections above and below here. You can have as many as you want within a chapter.

An unnumbered section

Chapters and sections are numbered by default. To un-number a heading, add a `{.unnumbered}` or the shorter `{-}` at the end of the heading, like in this section.

Chapter 3

Cross-references

Cross-references make it easier for your readers to find and link to elements in your book.

3.1 Chapters and sub-chapters

There are two steps to cross-reference any heading:

1. Label the heading: `# Hello world {#nice-label}`.
    - Leave the label off if you like the automated heading generated based on your heading title: for example, `# Hello world` = `# Hello world {#hello-world}`.
    - To label an un-numbered heading, use: `# Hello world {-#nice-label}` or `{# Hello world .unnumbered}`.
2. Next, reference the labeled heading anywhere in the text using `\@ref(nice-label)`; for example, please see Chapter 3.
    - If you prefer text as the link instead of a numbered reference use: any text you want can go here.

3.2 Captioned figures and tables

Figures and tables *with captions* can also be cross-referenced from elsewhere in your book using `\@ref(fig:chunk-label)` and `\@ref(tab:chunk-label)`, respectively.

See Figure 3.1.

```
par(mar = c(4, 4, .1, .1))
plot(pressure, type = 'b', pch = 19)
```

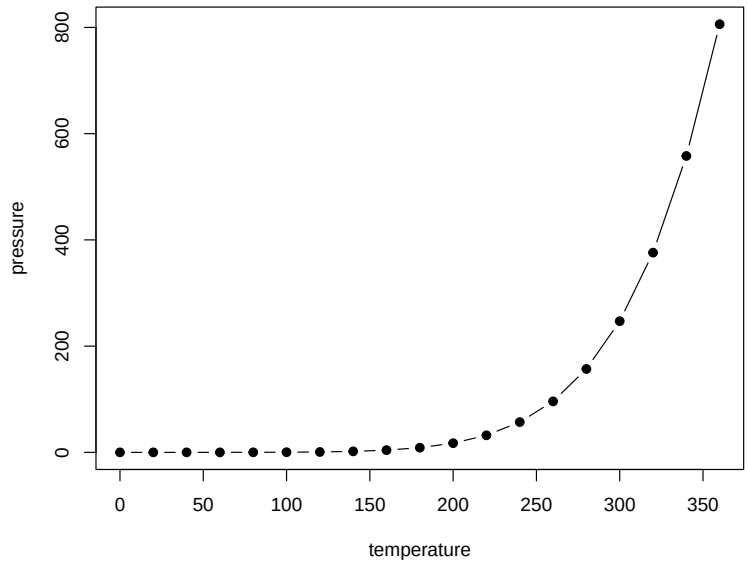

Figure 3.1: Here is a nice figure!

Don't miss Table 3.1.

```
knitr::kable(
  head(pressure, 10), caption = 'Here is a nice table!',
  booktabs = TRUE
)
```

Table 3.1: Here is a nice table!

temperature	pressure
0	0.0002
20	0.0012
40	0.0060
60	0.0300
80	0.0900
100	0.2700
120	0.7500
140	1.8500
160	4.2000
180	8.8000