# 0. Additional Books

The Internet has several good sources of information on Information Security. For those who want to learn more about the subject - beyond the scope of this course - can start with these two books.

Both are available free online (and legally so as long as you do not print it all out, or decide to sell it to your friends, etc). If you have read these, and you like the books and you really like information security, then consider supporting the authors by buying the book.

These books are NOT prescribed for the course, they are for your additional interest only.

For an overall view of security (not very technical but covering a lot of topics from a system security perspective)

Security Engineering by Ross Anderson, Wiley.

http://www.cl.cam.ac.uk/~rja14/book.html

If you like the cryptography and protocols try

Handbook of Applied Cryptography

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

[http://cacr.uwaterloo.ca/hac/Links to an external site.](http://cacr.uwaterloo.ca/hac/)

# 1. Introductory Concepts of Security (Tutorial 1 + Reading)

In Week 1 we will cover some basic security concepts, terminology and security standards.

Slides (pdf): [Lecture 1-Introduction - DG.pdf](https://cityu-dg.instructure.com/courses/253/files/2483?wrap=1)[Download Lecture 1-Introduction - DG.pdf](https://cityu-dg.instructure.com/courses/253/files/2483/download?download_frd=1)

Notes: [Lecture 1-Introduction - DG - Notes.pdf](https://cityu-dg.instructure.com/courses/253/files/2589?wrap=1)[Download Lecture 1-Introduction - DG - Notes.pdf](https://cityu-dg.instructure.com/courses/253/files/2589/download?download_frd=1)

The notes will often note whether a slide is only for reference or needs to be studied. Reference work is for interest, to complement other core concepts and you do not need to study these in detail for exam of mid-term.

Extra reading and questions for next week: [Lecture 1 - Reading.pdf](https://cityu-dg.instructure.com/courses/253/files/3033?wrap=1)[Download Lecture 1 - Reading.pdf](https://cityu-dg.instructure.com/courses/253/files/3033/download?download_frd=1)

Tutorial 1 (Week 2): [Tutorial1.pdf](https://cityu-dg.instructure.com/courses/253/files/3032?wrap=1)[Download Tutorial1.pdf](https://cityu-dg.instructure.com/courses/253/files/3032/download?download_frd=1)

Solutions (Tutorial plus extra reading): [Exercise 1 + Weekly Reading Solutions.pdf](https://cityu-dg.instructure.com/courses/253/files/4109?wrap=1)

# 1.1 Human aspect of security

For interest.

Even though we mostly consider security from a technical perspective in this course, you should also recognise the human aspect.

If you understand people, it is entirely possible to 'hack' without needing to understanding technology.

Watch: https://www.youtube.com/watch?v=L5J2PgGOLtE

2. Symmetric Encryption (Tutorial 2+3)

Lecture 2 deals with symmetric encryption algorithms. We start of looking at some historic approaches to symmetric encryption and look in detail at the algorithms and approaches we use today.

Lecture 2 is split across Weeks 2+3. I will post slide notes  after lecture in Week 3.

The notes file will be ppt so the animation also works.

Slides: [Lecture 2- Symmetric-Key-Encryption.pdf](https://cityu-dg.instructure.com/courses/253/files/3030?wrap=1)[Download Lecture 2- Symmetric-Key-Encryption.pdf](https://cityu-dg.instructure.com/courses/253/files/3030/download?download_frd=1)

Slides (ppt): [Lecture 2- Symmetric-Key-Encryption-SlidesOnly.pptx](https://cityu-dg.instructure.com/courses/253/files/3031?wrap=1)[Download Lecture 2- Symmetric-Key-Encryption-SlidesOnly.pptx](https://cityu-dg.instructure.com/courses/253/files/3031/download?download_frd=1)

Notes:

Worked example of how Feistel structure encrypts/decrypts: [Feistel\_example.pdf](https://cityu-dg.instructure.com/courses/253/files/3034?wrap=1" \o "Link" \t "_blank)[Download Feistel\_example.pdf](https://cityu-dg.instructure.com/courses/253/files/3034/download?download_frd=1)

Tutorial 2 (Week 4 Tue): [tut02.pdf](https://cityu-dg.instructure.com/courses/253/files/4107?wrap=1)[Download tut02.pdf](https://cityu-dg.instructure.com/courses/253/files/4107/download?download_frd=1)

Tutorial 2 Solutions:

Tutorial 3 (Week 4 Sunday):

Tutorial 3 Solutions:

In Lecture 1 reading, Sony's 2011 data breach is an older but very common story. We know confidentiality is on of the main services to address this threat and that encryption can provide confidentiality. Unfortunately data loss like this is not uncommon - and in these cases records are not encrypted. For famous cases see:

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

This link is a bit older but shows also some different ways the breaches were caused (for example, an employee losing an unencrypted disk by accident in the train or taxi on the way to work is also data loss, it is not different from hacking)

https://digitalguardian.com/blog/history-data-breaches

# 2.1 Encryption Optional Exercise 1

Try to do frequency analysis on the message on slide 33. If you have an answer that you think make sense - you can send to me and I will tell you if it is right.

You can do it by yourself, or in a group.

This is not an assignment for grade, and you do not have to do it.

# 2.4 Zodiac 340 Code (Interest Only)

In December 2020, some hobby code breakers solved a code that people have been trying to solve for 50 years. Substitution ciphers with some variations (unknown ordering of plaintext, custom alphabet, etc.) can be very tricky to solve even with modern technology.

[https://www.bbc.com/news/world-us-canada-55285805Links to an external site.](https://www.bbc.com/news/world-us-canada-55285805)

https://www.youtube.com/watch?v=-1oQLPRE21o&feature=youtu.be