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

Slides (ppt): Lecture 2- Symmetric-Key-Encryption-SlidesOnly.pptx

Notes: Lecture 2- Symmetric-Key-Encryption - Notes.pdf

Worked example of how Feistel structure encrypts/decrypts:

Feistel_example.pdf

Tutorial 2 (Week 4 Tue): tut02.pdf

Tutorial 2 Solutions: tut02_sol.pdf

Tutorial 3 (Week 4 Sunday): tut03.pdf

Tutorial 3 Solutions: tut03_sol.pdf

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