Information Security

(COMP 41280)

Course Introduction

Félix Balado

School of Computer Science
University College Dublin

What This Course Is About

- Information security is a broad field mainly concerned with ensuring
  - authenticity
  - integrity
  - privacy (confidentiality)

  of information
- This course is an introduction to
  1. the theoretical underpinnings of information security
  2. the most important techniques and algorithms that are used to secure information

Requisites

- Basic concepts from fields relevant to the course will be introduced along the way:
  - probability theory
  - information theory: "the" theory of information
  - number theory: essential for modern cryptography
- The course will be as self-contained as possible, but you may need additional self-study depending on your academic background

Course Outline

- Shannon's cryptography model. Channel/source coding and cryptography.
- Classic ciphers. Block ciphers. DES. AES. Operation modes. Stream ciphers.
- Public key cryptography. Diffie-Hellman scheme. RSA.
- Hash functions. SHA. Authentication Codes. Digital signatures and certificates.
- Noncryptographic security. Digital data hiding: watermarking and steganography. Digital forensics and counterforensics.

Practical Information

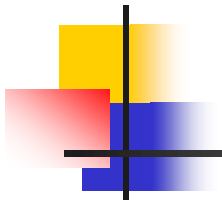
- Lectures
  - Mondays: 15:00 – 15:50 & 16:00 – 16:50 (room: CSI B002)
  - course information available on Brightspace as we go along: `https://brightspace.ucd.ie`
- Assessment:
  - three assignments
    - questions and problems related to the course materials

Practical Information

- Rules for assignment submission
  - only accepted through Brightspace (i.e., no hardcopy or email submissions please)
  - submissions must be typed (i.e., no scanned handwritten stuff) and in PDF format
  - please stick to submission length guidelines
  - deadline: two weeks after assignment is posted
    - deductions for late submissions: 10 marks up to one week late, 20 marks up to two weeks late
    - no submissions accepted after two weeks late
    - exceptions: medical reason, force majeure (bereavement, etc)
    - if you are going to miss the one month deadline after which submissions are not allowed, please email me
    - justifications must be in writing (no emails please), and must be handed in to me at the end of a lecture

Practical Information

- If an assignment requires programming, you can use any language you are familiar with
  - suggestion: GNU Octave or Matlab
  - no code should be submitted, just results (i.e., plots, tables, numbers,...)
- Although discussion with other students is okay, assignments are individual work
  - declaration of authorship: "I declare that all material in this assessment is my own work except where there is explicit acknowledgment and reference to the work of others"



Plagiarism & UCD Computer Science

- **Plagiarism is a serious academic offence**
  - [Student Code, sections 6.2 & 6.3] or [UCD Registry Plagiarism Policy] or [CS Plagiarism policy and procedures]
- Our staff and demonstrators are **proactive** in looking for possible plagiarism in all submitted work
- Suspected plagiarism is investigated by the CS Plagiarism subcommittee
  - Usually includes an interview with student(s) involved
  - 1st offence: **usually** 0 or NG in the affected components
  - 2nd offence: may be referred to the **University disciplinary committee**
- Student who enables plagiarism is equally responsible

http://www.ucd.ie/students/guide/academicregs.html

http://libguides.ucd.ie/academicintegrity

Grades in COMP41280

Grade	Low	High	Average
A+	95	100	97.5
A	90	95	92.5
A–	85	90	87.5
B+	80	85	82.5
B	75	80	77.5
B–	70	75	72.5
C+	65	70	67.5
C	60	65	62.5
C–	55	60	57.5
D+	50	55	52.5
D	45	50	47.5
D–	40	45	42.5

Grade	Low	High	Average
E+	35	40	37.5
E	30	35	32.5
E–	25	30	27.5
F+	20	25	22.5
F	15	20	17.5
F–	10	15	12.5
G+	8	10	9.0
G	5	8	6.5
G–	2	5	3.5
NG	0	0	0.0

Some References

- **Lecture notes**
- Cryptography:
  - *Practical cryptography*, N. Ferguson and B. Schneier. Wiley, 2003
  - *Understanding cryptography*, Paar & Pelzl. Springer, 2010
  - *Cryptography and data security*, Denning. Wiley, 1982
- Probability theory:
  - *A first course on probability*, S. Ross. Prentice Hall, 8th edition, 2010
- Information theory:
  - *Elements of information theory*, Cover & Thomas. Wiley, 2nd edition, 2006