CS7NS1/CS4400 Intro

Practical things...

stephen.farrell@cs.tcd.ie

https://github.com/sftcd/cs7ns1

Overview of Assignments

- 4 assignments
  - 3 individual, 1 as a team
- Submitty tool for submission of solutions
- Submitty supports automated marking so is in addition to blackboard
  - You'll get username/password in mail
  - Christian can help with password resets
  - Change your password to something you don't use for anything important

Marking

- 100% continuous assessment
  - Supplemental TBD, Not only practical assignments
  - Blackboard for submission of some (marked “BB”), submitty for others (marked “SM”)
- Quizzes: 20% (Ciaran, BB)
- Assignment1: 10% (Stephen, SM)
- Assignment2: 10% (Stephen, SM)
- Assignment3: 15% (Stephen, SM)
- Assignment4: 25% (Stephen, SM)
- Overall module report: 20% (Ciaran/Stephen, BB)
  - What I did and what I understood

123456

->

1rQ6rVJ3K$8TUEpMb6ZTmW10O6lVaOt1

->

123456

Password cracking

- Problem: Given a list of password hashes, recover the passwords?
- Real world problem
  - Leaked password databases
  - “I forgot my password”
  - Forensic investigations

Scale and Password Cracking

- Password hashing algorithm
  - Variation in time/memory difficulty
  - Hundreds of algorithm variants (maybe non-standard)
- Size of list
  - Can be up to 100’s of millions
  - Can be one
- Number of processes/processors applied
  - Multi-threaded, CPU, GPU
  - Distributed processing

Tooling for Assigments

- You'll get a US$100 budget for use on AWS
  - Default educational partner thing
  - If you overspend... tough! **Don't leave instances running when not needed!**
- You can use that to solve password cracking problems
- Assignments will start easy and get a bit harder as we go
  - First one is generally being setup in AWS
  - Thereafter you'll get individual lists of hashes to solve
- Marking: pro-rata, depending on how many hashes cracked, will be explained as we go
- Sharing: it's ok to help or share findings with one another, it's not ok to plagiarise!
  - If you used/benefited from someone else's work, make that clear in your overall module report
- Starting: next week