[aps]

{abertay /*PROGRAMMING*/ society;}

femsoc ABERTAY

Ada Lovelace Day Workshop

Abertay Programming Society in collaboration w/ Abertay Feminist Society

09-10-2018

Andrew, Gayan, Jessica & Paul

Announcements

- Cut-off date for membership payments
  = 16th October !!!

- Social Event - TBD 🎉

Over to FemSoc!

Ada Lovelace Day

Women in Programming

[aps]

{abertay /*PROGRAMMING*/ society;}

femsoc ABERTAY

Ada Lovelace Day

Second Tuesday of October

- Celebrate women in STEM
- Encourage more girls into STEM careers
- Support women already working in STEM

Ada Lovelace

First Computer Programmer

- Skilled mathematician – fascinated by Babbage's Difference Engine
- Translated an Italian description of the Analytical Engine, and included the first computer algorithm: Calculating sequence of Bernoulli Numbers
- Understood the potential of computers to create graphics and music

Joan Clarke

Bletchley Park Cryptanalyst

- Worked with Alan Turing to break Enigma ciphers
- Double First in Mathematics from GCCS, although prevented from receiving a full degree
- Decoded messages from German navy in real time, leading to immediate military action
- Classed as a linguist as there was no protocol for a senior female cryptanalyst

Margaret Hamilton

Apollo Software Engineer

- Worked at MIT on weather forecasting program, then SAGE on radar monitoring software
- Director of software engineering - developed guidance and navigation system for at MIT for Apollo missions
- Told NASA to add software to prevent astronauts loading pre-launch program during flight
- Coined ‘software engineering’ when not taken seriously as a science

Grace Hopper

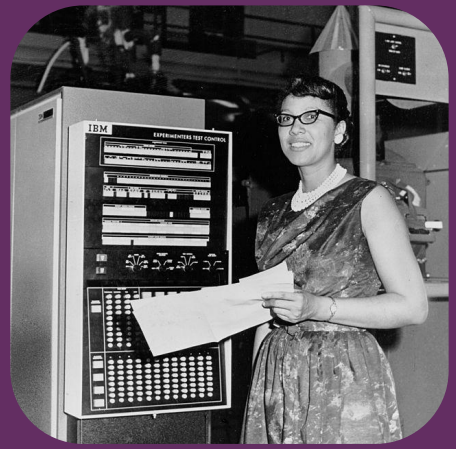
“Grandma COBOL”

- Pioneered accessible programming languages using words rather than numbers – led to COBOL, still used by businesses today
- Joined the US Navy and programmed the Mark I – wrote the world’s first programming manual
- Coined the term ‘compiler’ for her A-0 system – loaded subroutines and arguments to computer

And many more!

- Women have always been integral to computer programming and software engineering
- Behind many of the most valuable discoveries in space exploration and military

- Do it for her!



Melba Roy Mouton
NASA satellite tracking and A Programming Language

ENIAC women
First all-electronic, programmable computer

Hedy Lamarr
Patented frequency-hopping technology

Now some programming!

Challenge

- A simple caesar cipher to translate messages
  - Based on loops and dealing with characters - Ada Lovelace
  - Decryption - Joan Clarke

- The reason for a caesar cipher:
  - Most of are not mathematicians - @Jessica
  - Cipher basis for
    - Password cracking
    - Starting point for crypto - NOT bitcoins - Cryptography

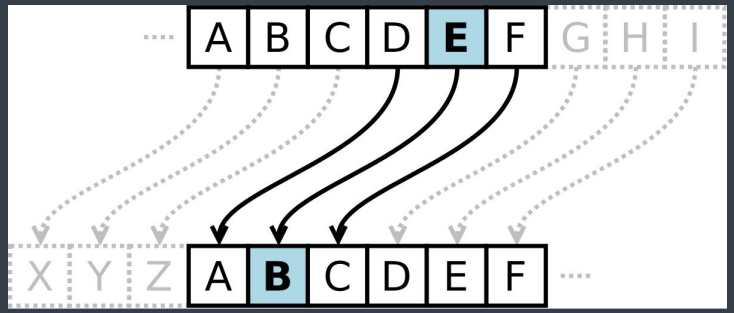
What is a Caesar Cipher

- A cipher is a way to encrypt and decrypt messages
- A caesar cipher is the most simple of cipher
  - Encryption -
    - Shifting the current letters forward by a set value
  - Decryption -
    - Shifting the current letters back by a set value
  - Key -
    - The value used for the alteration
    - Key is secret
  - The issue easy to break
- A caesar cipher is a type of shift cipher, where the key is numerical (e.g. 3)

Caesar Cipher Demo

Encoding

- Shift a character
  - How can a machine identify a character?
  - How can we manipulate that identifier?



- “Hello world from Abertay Femsoc and Abertay Programming Society!”

Decoding

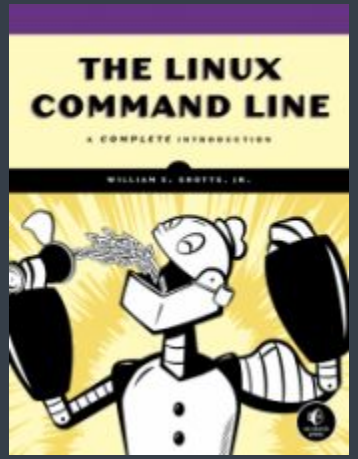
- Shift the characters back to retrieve original message
  - What did the encoding do?
  - How can we we reverse the process of the encoding?

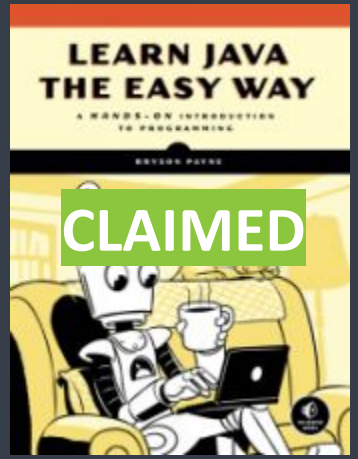
- “Frqjudwxodwlrqv rq ghfrglqj wklv phvvdjh. Qrz rq wr wkh qhaw fkdoohqjh.”

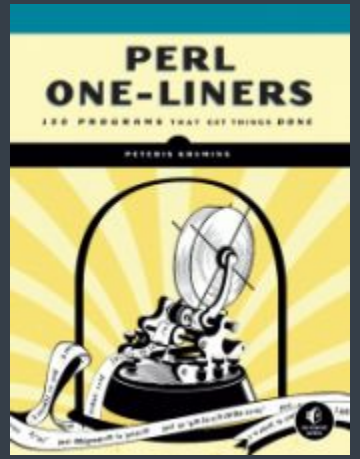
Prizes

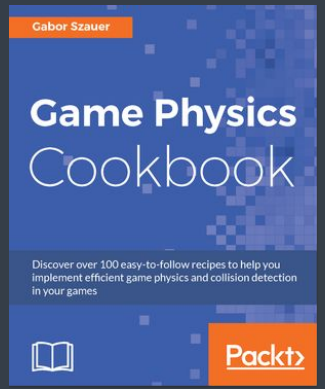
- Quickest solution
- Efficient solution
- Dirtiest solution

Prizes - One of each available









Brute-force (because ignorance!)

- Test every key to figure out the message
  - This is not a caesar cipher but a shift cipher as you don’t know the key.
- “IVqkmMiagMfiuxtm”
- “UfWyPcWmSqMkCyLrMkC”
- “JUUhxdaKjBnbJanKnuxWpCxDB”
- “SuHqYqBdUlQ”

Brute-force (ANSWERS!)

- Test every key to figure out the message
  - Andrew's Solution: github.com/AbertayProgrammers/Ada-Lovelace-Day/blob/master/cipher.py

- "IVqkmMiagMfiuxtm" -8- ANiceEasyExample
- "UfWyPcWmSqMkCyLrMkC" -24-WhYaReYoUsOmEaNtOmE
- "JUUhxdaKjBnbJanKnuxWpCxDB"-9-ALLyourBaSesAreBeloNgToUS
- "SuHqYqBdUlQ" -12-GiVeMePrIzE

Next Week - Make a Voice Assistant

- Text to speech and speech to text
- The basis of my assistant:
  - Record speech to text for journals, rather than typing - because lazy
  - Read text of what is contained in a document so you don’t have to read it - because very lazy
  - The starting point for a potential voice controlled ‘AI’ - because I want to be Tony Stark

Thanks for listening!

See you next week