HANDLING DATA

A PRACTICAL ENCRYPTION EXERCISE

MIKE STANNETT

7 MAY 2014

1 WHERE TO FIND YOUR CHALLENGE

- Open a **web browser**, and browse to http://staffwww.dcs.shef.ac.uk/people/M.Stannett/ambassadors/vigenere.php
- Choose a key and a message, and follow the instructions to encrypt it
- The following activities are no longer available.
    - When you're happy with your ciphertext, click the button to submit it
    - You will be given another team's Vigenère cipher to decrypt

2 HOW TO CRACK A VIGENÈRE CIPHER

- The first thing you need to do is find the length of the key
- Look for repeating blocks of letters, and count the gaps between them
- The key's length will usually be a factor of the various gap lengths. For example, if you find various repeating blocks are separated by gaps of length 15, 20 and 25, it's very likely that the key is 5 characters long, as 5 is almost the only factor of all three gap lengths
- Once you have the key's length, split the message into chunks. For example, if the key's length is 5, there will be 5 chunks
    - Chunk 1 contains the characters in positions 1, 6, 11, 16, 21, 26, …
    - Chunk 2 contains the characters in positions 2, 7, 12, 17, 22, 27, …
    - Chunk 3 contains the characters in positions 3, 8, 13, 18, 23, 28, …
    - Chunk 4 contains the characters in positions 4, 9, 14, 19, 24, 29, …
    - Chunk 5 contains the characters in positions 5, 10, 15, 20, 25, 30, …
- In each of these chunks, all of the letters have been encrypted using the same letter from the key, i.e. using a Caesar cipher
- Use frequency analysis to find out which letter occurs most frequently in each chunk. This is likely to be the letter E, encrypted using the corresponding letter of the key. This tells you what that letter is, and how to decrypt all the other letters in the chunk.
- Look out for easy answers. For example, a one-letter word is likely to be 'A' or 'I'. A letter at the end of a word that follows an apostrophe is likely to be an 'S'.

3 How to run PHP on your machine

- Create somewhere to store your files
- Start the PHP system if you need to
    - There are various free systems available - see the slides for some suggestions.
- Check it works
    - Open the **web browser** and browse to http://staffwww.dcs.shef.ac.uk/people/M.Stannett/ambassadors/
    - Right click on code-tester.txt and download it to your PHP folder
    - Change the filename ending to ".php"
    - Open the file in your web browser.

- Writing and editing files
    - Open the **file browser** and make sure filename endings are visible in Windows, so you can be certain your files really do end with ".php" when saving them in a text editor
    - For new files, create a new "Text Document" in your PHP folder, and give it a suitable name, e.g., "mycode.php"
    - To open a file for editing, right-click it and select an editor.

4 Find out more

These resources will remain available after today's sessions (but may move to the main 'ambassadors' website).

- http://staffwww.dcs.shef.ac.uk/people/M.Stannett/ambassadors/handlingdataOHP6.pdf
- http://staffwww.dcs.shef.ac.uk/people/M.Stannett/ambassadors/handlingdata.pdf
- http://staffwww.dcs.shef.ac.uk/people/M.Stannett/ambassadors/code-tester.php

5 Online Resources

- To find frequency analysers, do a Google search for "online frequency analysis tool"
- For the latest research papers on cryptology (and other aspects of computer science and physics), try
    - http://citeseer.ist.psu.edu/index
    - http://scholar.google.co.uk/
    - http://arxiv.org/