Applied Cryptography & Cryptoanalysis

The aim of this session is to introduce a range of cryptography and cryptoanalysis techniques and provide an opportunity for you to investigate and apply the range of technologies available.

Task 1: Decrypting simple ciphers

Please attempt to decrypt the following ciphertexts. You may find using a wheel helpful (http://inventwithpython.com/cipherwheel/). Please do NOT use automated solutions!

1. LQIRUPDWLRQ VHFXULWB LV WKH EHVW
2. RIXASVOW MW FSVMRK
3. EPG QA XTGUWCBP ITEIGA EMB?
4. TUBNJOTAO HIRFUVHZG ECOOMEEYX QKWXPRLDX

5. TWT BYIRZ MVOLC QSX YJXTS DKPV TWT WEZN SZK
6. YL JIO, AG OETHC HLA, AW FCUH SX FTVXLWVU; MSV ZI VV-HEQ XJHX WZIFZ LMK FNVSH OMVO QI KLCSP FW QA IVSLLGY

(Warning: Do not spend too much time on 5 and 6!)

Task 2: Exploring Polyalphabetic ciphers

Channel 4 put on a four-part television series discussing the history and use of cryptography. Whilst a little old, it remains a fascinating insight – particularly of the challenges involved.

1. Encryption and Le Chiffre Indechiffrable (24 minutes) – Link on the DLE under *Additional Information* (Crypto1)

Attacking alphabetic ciphers using frequency analysis. The lecturer will provide a technology demonstration using Cryptool 2 to illustrate how polyalphabetic ciphers can be cracked.

Task 3: Password Hacking Techniques

Password hacking can be undertaken using three core techniques:

- Brute Force
- Dictionary and Rule-Based
- Rainbow Tables

The lecturer will provide a technology demonstration of how to undertake each of these hacks and explore the reasons behind the challenges and ease to which they can recover passwords.

Task 4: Devising your own secure communications

In small groups, devise a secure communications system for an application or service. You are free to determine which (e.g. a web application, mobile phone network, Bluetooth network) and give thought to how to secure the channel and associated information.

In the design, given specific consideration to:

- What approach would you use to secure data at rest in database on the client/server?
- What approach would you use to secure data in transit?
- How do you manage the keys?

Task 5: The origins of Public Key Cryptography

A second part of the Science of Secrecy series presents the history of asymmetric cryptography. If time within the session (if not for after), please watch this episode:

1. Going Public (24 minutes) – Links the two parts of this episode can be found on the DLE module page under *Additional Resources* (Crypto 2 Part A and Part B).