Chapter 4

CYBER WARFARE SIMULATIONS

4.1 Simulation 1: The encrypted intelligence files

Topics: Breaking simple encryption

In the second security briefing, we heard of several examples of security failures. The first recorded computer break-in involved an attacker stealing *encrypted* passwords and breaking the encryption *offline*. That is, because the attacker had a copy of the encrypted passwords, he had an infinite number of attempts to decrypt them, as opposed to *e.g.* a modern website's login form which might restrict the number of attempts a client has for logging in before the system locks them out.

For this week's labs, you have been provided with several encrypted files containing vital intelligence which will enable us to protect the department's reputation. Many of our Bothan spies have died in order to obtain these from the Warwick Megalomaniacs Group. Your goal is to write an arsenal of tools (in whatever programming language you like and with the help of whatever libraries you like) to help you break the encryption. This will also be useful for working out the passwords for the module content.

The files are contained in a repository on GitHub which you can clone by running the following command in a terminal:

```
$ git clone https://github.com/dcs-cs263/lab1
```

Ex1 The `staff_passwords` file contains encrypted passwords belonging to Warwick Megalomaniacs Group staff. Fortunately, their staff are idiots and only use dictionary words for their passwords. Write a program to decrypt the passwords in this file and which tries to check whether you have successfully done so.

Ex2 Our Bothan spies have intercepted an email exchange between members of the Warwick Megalomaniacs Group. These are contained in the `emails` folder. Break the encryption and establish what they are up to.

Ex3 Certain systems used by the Warwick Megalomaniacs Group are more sophisticated and hash passwords. These are contained in `tabula_staff_passwords`. However, more sophisticated systems don't make up for stupid users which still only use dictionary words for their passwords. Write a program to try and figure out what password is contained on each line.
