Distributed Systems and Security Coursework 2

Manos Panaousis, with some alterations by Graham White

December 2013

1. **Cryptography**

   Encode the following plaintext, using the Caesar cipher `http://en.wikipedia.org/wiki/Caesar_cipher`:

   LORD OF THE RINGS

   (a) The following ciphertext

   `jw njbh lxmn cx kanjt`

   has been encoded using a generalised Caesar cipher where the following rule computes a character c_i in the cipher text from a character p_i in the plain text:

   $$c_i \quad = \quad E(p_i) \quad = \quad p_i + d(\mod 26)$$

   where d is a positive integer, and where $a = b \mod c$ means that $a - b$ is an integer multiple of c.

   Find the number d and the plain text by *frequency analysis*, in the following way. Notice that the cipher always encodes the same character by the same character, so the most frequent character in the ciphertext will correspond to the most frequent character in the plaintext. Now we can guess what the most frequent character in the plaintext is by using a table of English letter frequencies: probably the best one is here `http://norvig.com/mayzner.html`

   (b) Now consider the following cipher text:

   `homlox prv hetorx orxolxpersorx`

   A general substitution cipher has been used. This means that every letter of the alphabet appearing in the plain text is replaced with another unique letter of the alphabet. For example, the letter ‘a’ could be mapped into ‘h’, the letter ‘b’ into ‘x’ etc. The ciphertext then simply consists of these mapped letters.

Work out the original plain text message, using the following approach:

i. Write a line of dashes ("_") as placeholders for the plaintext characters corresponding to each letter in the above cipher text. Make sure you also mark the spaces between the different words as they will give you clues as soon as you know some of the letters.

ii. Using the English letter frequency table, find the letter which the letter 'e' is most likely to be replaced with. Use this to replace some of the "_" by the letter 'e'.

iii. Now look at a table of the frequencies of trigrams, i.e. sequences of three consecutive letters: find the most common trigram in English. Find the most common trigram in the ciphertext: this should tell you more about the substitution. Make the new substitutions that you have found.

iv. At this stage, you already might be able to guess the remaining characters. If you succeed then write the plain text into a new line and you have finished this exercise. Otherwise, look at the second word consisting of three characters. Again using the table of trigrams, try successively to match trigrams of decreasing frequency with this word (write down your choices as to document how you proceed). Each time, this will give your candidates for three more letters. Fairly soon, you should be able to guess the remaining characters. Write down the plain text. Make sure you describe precisely the different steps of your analysis.

(c) Consider the following ciphertext:

```
eaeairtntrnaeemtve
```

i. Read the Wikipedia article on transposition ciphers, `http://en.wikipedia.org/wiki/Transposition_cipher`

ii. By using letter frequency analysis, decide whether a substitution or transposition cipher has been used. Say what your answer is, and explain the evidence for your answer.

2. **Enigma** Write a 200-word mini-essay on the ENIGMA encryption device

(a) Briefly explain what the ENIGMA is and for what purpose and in what historical context it was used.

(b) When and where was it first invented?

(c) Describe the basic principle of the ENIGMA.

(d) How was the ENIGMA finally cracked, and why was this an important achievement?

(e) Use the online ENIGMA simulator at `http://enigmaco.de/enigma/enigma.html` to encrypt the plaintext "SECURITY SECURITY". Explain why these two identical plaintext words result in two different encrypted words, and how this is different to the simple substitution ciphers discussed in the lecture.

3. **Asymmetric Cryptography**

Alice and Bob are using the RSA algorithm for exchanging messages. Bob's public key is $(n_B, e_B) = (33, 17)$.

You are a cryptanalyst who intercepts the following ciphertext:

23 2 27 1 7 15

You know that this message has been sent by Alice to Bob, using Bob's public key for encoding the plaintext (therefore granting security, but not authentication). You know that it has been encoded letter by letter, using a numerical representation which goes $A = 1, B = 2, \cdots$. Your goal is to find out what it says. The following steps will help you cracking the code

(a) Your first task will be to find Bob's secret key d_B. Remember that the formula for determining d_B is

$$d_B \times e_B = 1 \quad (\mod N)$$

where $N = (p-1) \times (q-1)$ and $n = p \times q$. So first you need to find the two prime numbers p and q. This is generally very hard, but Bob used a very small number for n_B which you can factorise in your head. Having found p and q, you can now find N. Write down your results for p, q and N, with a brief description of how you did it.

(b) From this, you will be able to deduce the secret key d_B: remember that $d_B e_B = 1(\mod n)$, and we know e_B and n. There are fancy ways of doing this (based on what is called the Euclidean algorithm), but for this problem n is very small, so you could simply do this by trial and error: multiply e_B by all the numbers less than n, and the one which gives you a result of $1(\mod n)$ is d_B. Or you could use the modular arithmetic calculator here `http://ptrow.com/perl/calculator.pl`

(c) Now you know Bob's private key d_B, you can decrypt the message: you simply take each of the numbers in the cypher text, and for each number n you compute $n^{d_B} \mod 33$. There are, again, two ways of doing this: the hard way is to do it by repeated squaring and multiplication, and the easy way is to do use the online modular arithmetic calculator.

(d) Finally convert the numbers back to letters, using the $A = 1 \cdots$ code.

You should write up a description of the decoded message, and the steps you took to decode it.

4. **Hash Functions** In this exercise, you will learn more about the MD5 hash function. Visit the online MD5 calculator at `http://pajhome.org.uk/crypt/md5/`

   (a) Compute the MD5 hash of some input strings. For example try the values "The quick brown fox jumps over the lazy dog" and the same sentence including a "." at the end of the sentence. You could also try your name or one of your passwords.

   (b) Test experimentally whether MD5 satisfies Shannon's diffusion requirement: take a short string and compare its MD5 with the MD5s of the strings which you get from it by altering only one letter. How widespread are the changes?

   (c) Go to one of the websites which does dictionary attacks on MD5 hashes, such as `http://md5.gromweb.com/` See whether you can find the MD5 of your password in there: if it can, then change it . . .

   Write a summary of what you have found, saying whether your password was vulnerable, whether you changed it, what Shannon meant by diffusion, and whether you think MD5 does that.