SWP: Handin #2

Søren Løbner
Troels T. Hansen
Martin S. Kristiansen
{lobner,tth,martinsk}@cs.au.dk

September 7, 2010

Assignment 1.21(c)

In this assignment we have an example of a **ciphertext only attack**, as described in section **1.2 Cryptoanalysis** in the book. This would suggest a cryptoanalysis on the frequency of the letters. With the highest frequencies being:

`[C:32], [B:21], [K:20], [P:16]...`

But as the assignment does not state from where the plaintext originates, we do not know what language it is written in, and thus we do not know what to look for.

We know from Theorem 1.1 and Cryptosystem 1.3 that the Affine Cipher has a unique solution if the ciphertext and plaintext, C and P both are in Z_{26} and $gcd(a, 26) = 1$. Then we have the set K:

$$K = \{(a, b) \in Z_{26} \times Z_{26} : gcd(a, 26) = 1\}$$

And from this we also know that affine cipher has $12 \times 26 = 312$ possible keys.

Now we can perform 312 evaluations of the cipher-text, from these analyze which keys are the correct and retrieve our $K = (a, b)$.

And when we have $K = (11, 4)$, that is, after $4 \times 12 + 11$ iterations, a string starting with the following, appears:
"ocanadaterredenosaieuxtonfrontestceintdefl"

This is in fact the beginning of the Canadian anthem.

```
function decrypt($c) {
  for($i=0;$i<strlen($c);$i++) {
    $x = ord($c[$i])-65;
    $res = chr((((((($x-4)*11)%26)+26)%26)+65);
    echo strtolower($res);
  }
}

/***** cifertext ******/

decrypt(".
"KQEREJEBCPPCJCRKIEACUZBKR".
"VPKRBCIBQCARBJCVFCUPKRIOF".
"KPACUZQEPBKRXPEIIEABDKPBC".
"PFCDCCAFIEABDKPBCPFEQPKAZ".
"BKRHAIBKAPCCIBURCCDKDCCJC".
"IDFUIXPAFFERBICZDFKABICBB".
"ENEFCUPJCVKABPCYDCCDPKBCO".
"CPERKIVKSCPICBRKIJPKABI");



/***** plaintext ******/

O Canada! Terre de nos aïeux,
Ton front est ceint de fleurons glorieux.
Car ton bras sait porter l'épée,
Il sait porter la croix.
Ton histoire est une épopée,
Des plus brillants exploits.
Et ta valeur, de foi trempée,
Protégera nos foyers et nos droits.
Protégera nos foyers et nos droits.
```