Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

January 25, 2019

Cryptography & Encryption:6G7Z1011 : Simple Ciphers , Statistical Analysis and $\mathbb{Z}(n)$

1 Cryptography & Encryption:6G7Z1011 : Simple Ciphers , Statistical Analysis and $\mathbb{Z}(n)$

1.1 Caesar Cipher, Symmetric Cipher

The Caesar cipher, the affine cipher and the symmetric cipher are all attackable by statistical analysis.

1.2 problem:statistical analysis

⌜ Write a Java program that statistical analyses a long paragraph taken from an online document:

1. Store the paragraph as a Java String.
2. Using the split function place the string into array that contains the words of the string.
3. Split each word into an array of characters.
4. Run through the character array incrementing a counter each time it meets a particular letter.

For example

'code snippet'

```
String sentence="the cat sat on the mat";
int charoccurs[]=new int [26];
// charoccurs[0] = 3
// as 'a' occurs three times in sentence
```

⌟

1.3 problem:affine cipher

⌜We showed that the affine cipher only worked for particular key pairs.

1. Pick a legitimate key pair and let $e(i)$ denote the encryption of i. Print out the encrypted values of $e(0), e(1), \ldots e(25)$. Note there should be 26 different number printed out.
2. Pick an illegitimate key pair and print out the encrypted values of $e(0), e(1), \ldots e(25)$. Note there will be duplications.

⌟

1.4 problem:

⌜ Determine those elements of $\mathbb{Z}(26)$ that have a multiplicative inverse (hint, there are seven) ,and in each case state what the inverse is.
⌟

1.5 problem:

⌜ Write a JAVA program that takes two integers and returns true if and only if they are relatively prime. ⌟

1.6 problem:

⌜ Write a JAVA program that prints out the Euler ϕ function for the first 1000 integers. ⌟

1.7 problem:

⌜This is not an encryption question, it is a utility question (that is it performs a simple task of use to us in this unit).

1. Write a JAVA program that opens a file, say data.txt, and reads it line by line into an array of Strings. That is, array element zero contains the first line of the file, array element one contains the second line of the file, and so on.

2. Close the file.

3. Loop over the array and print out each line.

⌟

1.8 problem:

⌜ Write a JAVA program that prints out a file consisting of two columns. The first column is a list of the integers from 1 to 1000 and the second column is the number of prime numbers found up to that point. For example, consider 10 then 2, 3 5, 7 are the primes less that or equal to 10 so the file entry is

$$\begin{array}{ll} 9 & 4 \\ 10 & 4 \\ 11 & 5 \\ 12 & 5 \\ 13 & 6 \\ 14 & 6 \\ & . \end{array} \tag{1}$$

Using MATLAB (or visualisation software of your choosing) plot column one against

$$\frac{\text{column one}}{\text{column two}} \tag{2}$$

(that is we are plotting the density of the primes).
Any thoughts?
⌟