Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

February 1, 2019

Cryptography & Encryption:6G7Z1011 : Euclid, and the Fast Powering Algorithm

1 Cryptography & Encryption:6G7Z1011 : Euclid, and the Fast Powering Algorithm

1.0.1 ☞:

Please code the following in JAVA.

1.1 problem:Introduction to Blocks

⌜ This problem introduces some of the ideas used in the DES algorithm which we will meet later.

1. Create a string with some plain text in, we will use the plain text 'abcdefghijklmnopqr'
2. Split the string into an array of strings, each string in the array being of size n^2, in our example $n = 3$ so we are slitting on 9.
3. Write each string in the array into a $n \times n$ matrix.
4. Encrypt each matrix as shown in table 2.
5. Write out the encrypted string, in the example this is 'adfbehcfijmpknqlor'.
6. Write the decryption algorithm

For example if the string is 'abcdefghijklmnopqr' and $n = 3$ then the array has two elements:

1. the first is 'abcdefghi'
2. the second is 'jklmnopqr'.

Store each string in the array in a square array of size $n \times n$ so we have the situation in table 1. Encrypting each string gives table 1, and the strings are joined to give the encrypted message 'adfbehcfijmpknqlor'. ⌟

1.2 problem:Euclid

⌜Code Euclid's algorithm in JAVA. Fix a large integer a and let $1 \leq b \leq a$. Plot b against the number of divisions required to evaluate $\gcd(b, a)$, and overlay the function from the notes to see how well they agree. ⌟

a	b	c
d	e	f
g	h	i

first string

j	k	l
m	n	o
p	q	r

second string

Table 1: The encryption involves making the first row the first column, the second row the second column and the third row the third column.

a	d	g
b	e	h
c	f	i

first string encrypted

j	m	p
k	n	q
l	o	r

second string encrypted

Table 2: Encrypting the array strings, the rows become columns.

1.3 problem:Fast Power

⌜ Evaluate, on paper first if you wish, using the fast powering algorithm

$$x = 3^{123456} \mod 17 \tag{1}$$

⌟

1.4 problem:

⌜Find all the solutions to

$$x^2 + x = 1 \mod 19 \quad \text{and} \quad 11^x = 21 \mod 71. \tag{2}$$

There is no need to construct a fast algorithm, any algorithm that works is fine. ⌟

1.5 problem:

⌜Looking ahead, we need some ideas from the theory of matrices. I am sure you have all meet matrices before, they are simply square arrays of numbers. For now, write code that takes two 3×3 matrices matrices and evaluates their product. ⌟

1.6 problem:

⌜Solve the above problem by creating a function that takes two matrices and returns (if possible) their product. ⌟