Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

February 8, 2019

Cryptography & Encryption:6G7Z1011 : Mathematical Structures and a First Look at Diffie

1 Cryptography & Encryption:6G7Z1011 : Mathematical Structures and a First Look at Diffie

1.0.1 ✒:

We do some calculations with groups. Recall that the permutation group S_n has $n!$ elements (for example S_{10} has $10 \times 9 \times 8 \cdots \times 1$ elements) then you realise how fast S_n grows as a function of n.

1.1 problem:

⌜This was a homework question, but it is important so we look at it here. Let p denote a *p*lain text message then $A(p)$ is to be read A acts on p, and

$$e = A(p) \tag{1}$$

is the resulting encrypted message. One of the easiest examples of this is letting A be a matrix. If we consider the 2×2 case we have

$$\overbrace{\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}}^{e} = \overbrace{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}}^{A} \overbrace{\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}}^{p} \tag{2}$$

The important point to note is that if we wish to use A as an encryption technique we need to ensure A^{-1} the inverse of A exists. In the following p and e are real vectors of length 2 and any matrix is 2×2.

1. Write a Java method that takes two arguments: a matrix A and a plain message p, and returns the encrypted message e.
2. Write a Java method that takes one argument: a matrix A and returns, if it exists, A^{-1}.

⌟

1.2 problem:

⌜ Prove directly by hand calculation and by writing Java code that the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3}$$

form a group of order four. It is abelian. ⌟

1.3 problem:

⌜Prove by writing Java code that S_3 is a group, you need to think how best to represent S_3 in a Java class.

⌟

1.4 problem:

⌜ Prove directly by hand calculation and by writing Java code that the matrices

$$\begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \end{array} \tag{4}$$

form a group. Note : $i^2 = -1$, so you need to be able to multiple complex numbers together in your calculation. The matrices form a group of order eight, it is non-abelian. ⌟

1.5 problem:

⌜This is a bit of a challenge, can you describe the multiplication table of the permutation group S_4, note it has 24 elements.

⌟

1.6 problem:

⌜A subset S of a group G is termed a *subgroup* of G is S is itself a subgroup. Find an example of a subgroups in each of the following groups:

1. S_3

2. S_4

⌟

1.7 problem:mod functions

⌜ Consider the function $y = 627^x \mod 941$ on the x range $[0, 941]$. Sketch — if you can — what you think the function looks like. Save the function points to a file and plot it in Excel, Matlab (software of your choice). What do you deduce?

⌟

1.8 problem:groups

⌜Read the definition of a group. Determine if the following are groups; if they are a group state if they are abelian and what the unit element 1 is.

1. The set of real numbers under addition.

2. The set of all natural numbers $\{1, 2, 3 \ldots\}$ under addition.

3. The set of all 2×2 matrices under addition.

4. The set of all 2×2 matrices under multiplication.

⌟

1.9 problem:finite fields

⌜The condition of being a field is more restrictive than being a group. We will show in a later lecture that for p prime and n a positive integer there is one and only field of size p^n. An example will illustrate, let $p = 3$ and $n = 2$. Recall a field has both addition and multiplication. Let

$$F = \mathbb{Z}(3) \times \mathbb{Z}(3); \tag{5}$$

that is each element (x, y) in F is such that $x, y \in \mathbb{Z}(3)$. Define addition in the obvious way

$$(x_1, y_1) +_F (x_2, y_2) = (x_1 +_{\mathbb{Z}(3)} x_2, y_1 +_{\mathbb{Z}(3)} y_2), \tag{6}$$

and multiplication in the (much less obvious way)

$$(x_1, y_1) \times_F (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \mod 3. \tag{7}$$

Prove this is a field of size nine, do it on paper and as a Java class. ⌟

1.10 problem:Diffie

⌜ We implement Diffie with some real data. We work on the Java Implementation of the Diffie-Hellman protocol. We will use small prime numbers — if a question asks you to verify something you are free to use a brute force attack. And you will need to be able to write a fast-powering algorithm.

1. Let $p = 941$ (prove 941 is prime), we let $g = 237$.
2. Suppose Alice chooses a secret key $a = 347$ what is A?
3. Suppose Bob chooses a secret key $b = 781$ what is B?
4. What is the value of A'?
5. What is the value of B'?

Of course A' and B' should agree, what is their shared value? ⌟