Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

February 15, 2019

Cryptography & Encryption:6G7Z1011 : Coding Diffie

1 Cryptography & Encryption:6G7Z1011 : Coding Diffie

1.1 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.

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? ⌟

1.2 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?
⌟

1.3 problem:

⌜Start your assignment. ⌟