Nolan Pofi

Hw3 pt. A

My program encrypts the original message to get the cipher text (0010, 0000, 1100, 1110, 0100, 139680). It then takes that and decrypts it back to the original message of 10011100000100001100. My program begins by establishing variables with the values given from the assignment such as p, q, a, b, x0, and m. It then calculates variables needed for encryption such as n and h.

It then passes it to an encryption function which returns the cipher text. It then encrypts the message by breaking it into t parts with h bit lengths where t = 5 and h = 4 for this assignment. Then for each part it xors it with the last h bits of an x value which is calculated by taking the mod by n of the previously used x value squared x_new = (x)^2 mod n. Next it prints out the cipher text to show that it is what the program generates.

Then it calls the decrypt function on the cipher text which will return the original message. The decryption function first calculates d1 and d2 where d1 = ((p+1)/4)^(t+1)mod (p-1) and d2 is the same but the p is replaced with q. It then proceeds to calculate variables u and v where u = (x_t+1)^d1 mod p and v is the same but substituted p for q and d1 for d2. Then using those variables it calculates the given x0 using (v*a*p)+(u*b*q) mod n. It then decrypts the ciphertext blocks the same way it encrypted them by xor each with the same last h bits of x where it is calculated the same way as the encryption so that at each step it is the exact same numbers as xor a value with the same value twice nullifies. This gives the original cipher text which is then printed to show that it does generate it back through the algorithm.