Homework # 3

1. [25pnts] The global public elements are q=257; $E_{257}(0,-4)$ which is equivalent to the curve $y^2 = x^3 - 4$; G=(2,2). Bob's private key is N_B=101. Alice wants to send a message encoded in the elliptic point P_m=(112,26); Alice chooses a random integer k=41.

a. [15pnts] What is the ciphertext?

b. Show how description works

2. [20pnts] Compute the Jacobi symbols (denoted by J(x,y)) and indicate which rules you applied explicitly (show your work):

a. J(700,1617)

b. J(100,173)

c. J(1000,173)

d. J(1000,171)

3. [25pnts] Encrypt & decrypt the message M = {NETSEC} with BG (Blum & Goldwasser) where p = 499, q = 547; and let random quadratic residue for encryption is x_0 = 159201. Show your work and include a readme file for your code.

4. [30pnts] Consider textbook RSA N=173x7=1211, e=7.

a. Encrypt the message M = {NETSEC} and show its correct decryption.

b. Semantically secure RSA: using your simplified DES to create Hash values, and random numbers,

b1. encrypt the message M = {NETSEC} twice

b2. Decrypt each ciphertext.

Show your work. Include your hash values, random variables etc.