# Homework 3. Programming Part a.

# Due on November 1, 2018

3.Prog.a. Impelment Blum Goldwasser Probabilistic Encryption Algorithm with the following setup parameters:

p=499, q=547, a=-57, b=52, X0 =159201.

message m to be encrypted is in binary: 10011100000100001100

1. What is the ciphertext?

2. Verify your answer by showing that D(C(m))=m.