CPSC 418/MATH 318 Practice Problems

El Gamal Encryption

1. Suppose Alice employs the El Gamal encryption scheme with $p = 59$, $g = 2$ and private key $x = 17$.
   (a) Verify that 59 is a safe prime.
   (b) Verify that 2 is a primitive root of 59.
   (c) Use the binary exponentiation algorithm to compute Alice's public key quantity y.
   (d) Use the binary exponentiation algorithm to encrypt the message $M = 28$ with Alice's public key and the random number $k = 10$.
   (e) Use the binary exponentiation algorithm to decrypt the ciphertext $(C_1, C_2) = (11, 23)$ with Alice's private key.

2. Suppose that when performing El Gamal encryption, an encrypter deploys a poorly designed random number generator that uses the same seed and hence generates the same random number k every time it is run. Show how an attacker Eve can detect this and then mount a known plaintext attack on El Gamal under these assumption.

   Specifically, suppose Eve has a triple (M, C_1, C_2) where (C_1, C_2) is the encryption of M under Alice's public key. Now Eve intercepts another pair (C_1', C_2') that is the encryption of some unknown plaintext M' under Alice's public key. Explain how Eve can ascertain whether the same k was used in both encryptions and, if yes, how she can find M' without knowledge of Alice's private key.

3. Suppose you intercept an El Gamal ciphertext (C_1, C_2) encrypted under some public key (p, g, y) such that $gC_1 \equiv 1 \pmod{p}$.
   (a) Find the random number k used in this encryption.
   (b) Find the corresponding plaintext M without knowledge of the private key.