

## CPSC 418/MATH 318 Practice Problems

### El Gamal Signatures

1. Suppose Alice employs the El Gamal encryption scheme with  $p = 59$ ,  $g = 2$  and private key  $x = 17$ . On the practice problem set on El Gamal encryption, you verified that 59 is a strong prime and 2 is a primitive root of 59. Recall also that you computed Alice's public key to be  $y = 33$ .
  - (a) Compute Alice's signature to a message  $M$  using the random number  $k = 11$ . Assume that  $H(M\|r) = 23$ .
  - (b) Verify the signature generated in part (a).
2. This problem deals with a careless El Gamal signer.
  - (a) Suppose a signer chooses their random value  $k$  in the El Gamal signature scheme carelessly and obtains an  $r$  value of 1. Explain how this immediately reveals the signer's private key  $x$ .
  - (b) If  $k$  is chosen according to specifications, is 1 a possible value for  $r$ ? Why or why not?