Homework 28, due November 8

(1) (Page 252, problem 1) Show that if someone discovers the value of k used in the ElGamal signature scheme, then x can be determined if $\gcd(r, p-1)$ is small.
(2) (Page 253, problem 6) Alice wants to sign a document using the ElGamal signature scheme. Suppose her random number generator is broken, so she uses $k = x$ in the signature scheme. How will Eve notice this and how can Eve determine the values of k and x (and thus break the system)?
(3) (Page 255, problem 1) Suppose we use the ElGamal signature scheme with $p = 65539, \alpha = 2, \beta = 33384$. We send two signed messages (m, r, s):

$$(809, 18357, 1042) \text{ and } (22505, 18357, 26272).$$

   (a) Show that the same value of k was used for each signature.
   (b) Use this fact to find the value of k and to find the value of x such that $\beta = \alpha^x \pmod{p}$.