Homework 20, due November 13

- (1) Let h be a hash function whose input is a string of letters, spaces, and punctuation, and whose output is an integer (mod 100). Use the 100 character alphabet (ASCII 32) used earlier. The function h adds together the numerical representation of each character in the string and outputs the result (mod 100). For example, the string "Hello." would have output $h(Hello.) = 40 + 69 + 76 + 76 + 79 + 14 \pmod{100} = 54$. Use a generalized birthday attack to find two messages with the same hash, one of which you could convince someone to sign (for example, "Go BYU") and one which they would refuse to sign (for example, "I will pay you ten dollars"). Explain how you could forge a signature on the "evil" message by getting someone to sign the "good" message. Choose an RSA public and private key and sign the "good" message. Verify your signature.
- (2) Now choose an ElGamal public and private key and sign the "good" message. Verify your signature.
- (3) (Page 253, problem 5) The ElGamal signature scheme is weak to an existential forgery attack, as follows: Choose u, v such that gcd(v, p-1) = 1. Compute $r \equiv \beta^v \alpha^u \pmod{p}$ and $s \equiv -rv^{-1} \pmod{p-1}$.
 - (a) Prove that the pair (r, s) is a valid signature for the message $m = su \pmod{p-1}$. Of course, it is likely that m is not a meaningful message.
 - (b) Suppose a good hash function h is used, so that we sign h(m) instead of m (thus, we need h(m) = su). Explain how this protects against existential forgery; that is, explain why it is now hard to produce a forged, signed message (meaningless or not) by this procedure.
- (4) (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) = hi; (22505, 18357, 26272) = bye.

Show that the same value of k was used for each signature, and use this to find k and to find a such that $\beta \equiv \alpha^a \pmod{p}$.