Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
Due: 12/5/17

COSC/MATH - 314

Assignment 10

Problem 1: Let p be a prime that has 1024 bits and let a be a primitive root of p.
Let $h(x) = a^x$ (mod p). We analyze if h is a good hash function.

(a.) Is $h(x)$ preimage resistant? Say YES or NO and justify your claim.

(b.) Is $h(x)$ weakly collision resistant? Say YES or NO and justify your claim.

Problem 2: In a family of five, what is the probability that no two people are born in the same month? Explain how you have computed the probability.

Problem 3: Bob is using the El Gamal signature scheme. His public key is $(p, \alpha, \beta) = (97, 23, 15)$ and his secret key is $a = 67$.

(a.) Calculate Bob's signature for message $m = 17$ with ephemeral random $k = 31$.

(b.) You receive allegedly from Bob the signed message $(m_1, r_1, s_1) = (22, 37, 33)$ and $m_2, r_2, s_2 = (82, 13, 65)$. Verify is these messages originate from Bob.