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.

Solution:

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

Solution: h is **not** strongly collision-free because we can easily find $x_i, x_j \ni h(x_i) = h(x_j)$ if we know a message x_j. This can be accomplished by using Fermat's Little Theorem. Since $p\chi\alpha, \alpha^{p-q} \equiv 1$ (mod p). So,

$$h(x_i) \equiv \alpha^{x_i} \equiv \alpha^{x_i} \cdot \alpha^{p-1} \equiv \alpha^{x_i+p-1} \text{ (mod p)}$$

If we let $x_j = x_i + p - 1$, we get $h(x_i) = h(x_j)$ for $x_i \neq x_j$.

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.

Solution: $P(E) = (1 - \frac{1}{12})(1 - \frac{2}{12})(1 - \frac{3}{12})(1 - \frac{4}{12}) \approx 38.2\%$. Furthermore, there are 12 options for the month of birth for the first person. We want the next person to have a different month of birth so there are 11 possibilities for that person. 10 possibilities for the third person. 9 for the fourth. 8 for the fifth.

So, $(12 \cdot 11 \cdot 10 \cdot 9 \cdot 8) = 95040$. $12^5 = 248832$, ways to choose five peoples months of birth. $\frac{95040}{248832} = 55/144 = 38.2\%$.

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.