

SOEN 321

Prob 1. Bob is a paranoid cryptographer who does not trust dedicated hash functions such as SHA1 and SHA-2. Bob decided to build his own hash function based on some ideas from number theory. More precisely, Bob decided to use the following hash function: $H(m) = m^2 \bmod n$, $n = p \times q$, where p and q are two large distinct primes. Does this hash function satisfy the one-wayness property? What about collision resistance? Explain.

Sol. Since p and q are secret, then finding the square root mod n is a hard problem. Thus this hash function satisfies the one-wayness property. On the other hand, H does not satisfy the weak/strong collision resistance property because for any m , $-m$ would also have the same hash value, i.e., $H(m) = H(-m)$.

Prob. 2 Consider a (4,3) Shamir secret sharing scheme with $p=17$. Show how the secret can be recovered from the following shares: (1,10), (2,16), and (3,2).

Sol.

Form 3 equations in 3 unknowns.

$$10 = a_0 + a_1 + a_2 \bmod 17$$

$$16 = a_0 + 2a_1 + 4a_2 \bmod 17$$

$$2 = a_0 + 3a_1 + 9a_2 \bmod 17$$

$$\Rightarrow a_0=1, a_1=2 \text{ and } a_2=7. \text{ Thus the secret } = a_0=1$$