CIS4731 Assignment 1

Q1: The meaningful English word found in part 1 = ravishingly

Q2:

$$h(M) = (\Sigma_{i=1}^{t} a_i) \mod n$$

where $0 \leq a_i < n$, t can be any positive integer, and n is a pre-defined positive integer.

a) Does this hash function satisfy any of the requirements for a crypto-hash function listed below? Explain your answer:

a)

- **variable input size:** t can be any positive integer, so the input size is variable.
- **fixed output size:** output size is fixed because of the mod n upper bound.
- efficiency (time-space complexity): Because we are using a loop for summation, it is O(t) or linear which is fairly efficient.
- **first and second pre-image resistance:** This hash function offers preimage resistance because the digest cannot just be simply guessed when given the messaged to be hashed. The hash function does not offer second preimage resistance because it possible to find a second input that has the same digest as a given input.
- **strong collision resistance:** The hash function does offer strong collision resistance it is hard to find two inputs that hash to the same output.
- **pseudo-randomness (unpredictability of the output):** As long as the function distributes the value of the hash into a range in a even fashion so that all hash values re not placed into a small range area, we consider it pseudo random.

b)

Repeat part (a) for the following hash function:

$$h_2(M) = (\Sigma_{i=1}^{t} a_i^2) \mod n$$

- **variable input size:** t can be any positive integer, so the input size is variable.
- **fixed output size**: output size is fixed because of the mod n upper bound.
- **efficiency (time-space complexity):** Because we are using a loop for summation and squaring t, it is O(t) or linear which is fairly efficient.
- **first and second pre-image resistance:** This hash function offers preimage resistance because the digest cannot just be simply guessed when given the

messaged to be hashed. The hash function does not offer second preimage resistance because it is possible to find a second input that has the same digest as a given input.

- **strong collision resistance:** The hash function does offer strong collision resistance it is hard to find two inputs that hash to the same output.
- **pseudo-randomness (unpredictability of the output**): As long as the function distributes the value of the hash into a range in a even fashion so that all hash values re not placed into a small range area, we consider it pseudo random.

c) Calculate the hash function of part (b) for M = (189, 632, 900, 722, 349) and n = 989.

- (189^2 + 632^2 + 900^2 + 722^2 + 349^2) mod 989 ->
- 1888230 mod 989 ->
- **229**

Q3:

a) If we know that the following ciphertext is the result of encrypting a single meaningful English word with some key, find the key and the word:

Word: internationalization

Key: 121 and 89