q1. Ravishingly

q2. a) Analysis of the first hash function $h(M) = (\sum_{i=1}^{t} a_1) mod\ n$

1. Variable input Size: Yes, the function can take a sequence M of variable length t.
2. Fixed Output Size: Yes, the Output is an integer modulo n, so it has a fixed size.
3. Efficiency (Time-Space Complexity): Yes, the function is efficient with $O(t)$ time complexity and constant space complexity.
4. First and Second Pre-Image Resistance: No, it's easy to find another sequence M'such that $h(M) = h(M')$ by just adding or subtracting multiples of n to any a_i.
5. Strong Collision Resistant: No, for the same reason as above, it's easy to find two different sequences M and M' such that $h(M) = h(M')$.
6. Pseudo-randomness (Unpredictability of the Output): No, the output is directly related to the sum of the elements in M, making it predictable.

b) Analysis of the second hash function $h_2(M) = \sum_{i=1}^{t} a_i^2)\ mod\ n$.

1. Variable Input Size: Yes, the function can take a sequence M of variable length t.
2. Fixed Output Size: Yes, the output is an integer modulo n, so it has a fixed size.
3. Efficiency (Time-Space Complexity): Yes, the function is efficient with $O(t)$ time complexity and constant space complexity.
4. First and Second Pre-image Resistance: no, it's still easy to find another sequence M'such that $h_2(M) = h_2(M')$ by manipulating the squares of a_i.
5. Strong Collision Resistance: no, for the same reason as above, it's easy to find two different sequences M and M' such that $h_2(M) = h_2(M')$.
6. Pseudo-randomness (Unpredictability of the Output): No, the output is directly related to the sum of the squares of the elements in M, making it predictable.

c) Calculate the hash function of part(b) for $M = (189, 632, 900, 722, 349)$ and $n = 989$ to calculate $h_2(M)$, we first have to find the sum of the squares of the elements in M

$$\sum_{i=1}^{t} a_i^2 = 189^2 + 632^2 + 900^2 + 722^2 + 349^2$$

Then we take this sum modulo n

$$h2(M) = \left(\sum_{i=1}^{t} a_i^2\right) mod\ 989 = 229$$

So, the hash value is 229.

q3. 0x79 internationalization