Hashing

1. Find examples when it is better to have the following combinations of services (if any):
    a. Confidentiality without authentication
    b. Authentication without confidentiality
    c. Authentication without integrity
    d. Integrity without authentication
2. What is the difference between weak and strong collision resistance?
3. What characteristics are needed in a secure hash function?
4. In what ways can a hash value be secured so as to provide message authentication?
5. What is the differences between MAC, HMAC and One way hash functions
6. Consider the following hash function. Messages are in the form of a sequence of decimal numbers, M = (a_1, a_2,..., a_n). The hash value h is calculated as $h = \sum_{i=1}^{n} a_i \bmod n$, for some predefined value n.
    a. Does this hash function satisfy any of the requirements for a hash function? Explain your answer.
    b. Repeat for the hash function $h_2 = \sum_{i=1}^{n} a_i^{\,2} \bmod n$
    c. Calculate the hash function of part (b) for M = (189, 632, 900, 722, 349) and n = 989.
7. What should B do to confirm the source and integrity (if possible) of the message M in the following exchanges:
    a. $A \to B : M + E\left(k_{AB}, H\left(M\right)\right)$
    b. $A \to B : M + E_{Pub}\left(k_A^{Private}, H\left(M\right)\right)$
    c. $A \to B : M + H\left(S + M\right)$
8. For the three exchanges in problem 8, Discuss the advantages and disadvantages of these three arrangements for providing authentication using hash functions.