Question 2:

UNIVERSITÄT BERN

A) Consider the following *(non modular)* hash function. Messages are in the form of a sequence of numbers in $Z_n, M = (a_1, a_2, .., a_t)$. The hash value is calculated as $\sum_{i=1}^{t} a_i$ for some predefined value n.

- Does this hash function satisfy any of the requirements for a hash function (provided table)?

B) Repeat part (a) for the hash function h=$(\sum_{i=1}^{t}(a_i)^2) mod n$.

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

Explain your answers for all subquestions.

Requirement
Variable input size
Fixed output size
Efficiency
Preimage resistant (one-way property)
Second preimage resistant (weak collision resistant)
Collision resistant (strong collision resistant)
Pseudorandomness

Question 3:

A) State the value of the padding field in SHA-512 if the length of the message is:

- 5000 bits
- 5001 bits
- 5002 bits

B) State the value of the length field in SHA-512 if the length of the message is:

- 5000 bits
- 5001 bits
- 5002 bits

For both subquestions justify your answer.

Question 4:

Explain the differences in the algorithms of SHA-3 and MD5. Which one is used today? Why?