CS 463/563: Cryptography for Cybersecurity
Spring 2024
Homework # 11
Points: 20

This homework relates to **hash functions** for block ciphers (*sec 11.3.2*)

- Block size = **8 bits**
- Hash size = **8 bits**
- Encryption function:
  - ✓ Divide the key into two halves: **LK and RK**
  - ✓ Divide the plaintext into two halves: **LT and RT**
  - ✓ Then ciphertext = **LC || RC** where **LC = LK XOR RT**; and **RC = RK XOR LT**; where LC, RC, LT, and RT are each 4 bits; Plaintext and ciphertext are each 8 bits.
- **g(H) = an 8-bit** string that is equal to the complement of bits in H
  ***For example**, if H=A3 (Hexa) = 10100011 (binary); then g(H)= 01011100*
- $\mathbf{H_0}$ = Initial hash = **F4**

Given a message **m: DAB9** (in Hexa)

Question 1. [Points 7] Determine the hash (in Hexa) of the **message M** using **Martyas-Meyer-Oseas** hash function (*Fig. 11.7*).

Question 2. [Points 6] Determine the hash (in Hexa) of the **message M** using **Davis-Meyer** hash function (*Fig. 11.6*)

Question 3. [Points 7] Determine the hash (in Hexa) of the **message M** using **Migayuchi-Preneel** hash function (*Fig. 11.6*)

What to submit? Submit a pdf file with your answers via Canvas. Show your work