CS 161- Homework#3

Student: Ninh DO
SID: 25949105

Problem 1

(a) TRUE
(b) TRUE
(c) FALSE
(d) TRUE

Problem 2

(a) MAC, integrity and authentication. MAC is mainly to enhance authentication for hashing.
The scheme uses hash function and users sends {M, T}, where M is message ‘filename’, T is tag ‘hash’, T = F(K,M). K is secret key + hash function -> MAC. MAC ensures integrity by checking ‘hash’ at the server to make sure the message is untampered. 'key’ is known only to server, so nobody can interfere. ‘key’ is used to authenticate the sender.

(b) Secret ‘key’ needed to make ‘hash’ unique and nobody can guess. If the server does not have a secret ‘key’, anybody can send message ‘filename’ to the server -> fail to distinguish true user.

Problem 3

Problem 4

(a) Both hospitals should follow the steps:

- Step 1. Use the same cryptographically strong hash function SHA256(name_i + key) taking the string input that is the <u>concatenation</u> of name of i-th patient and the common key that is known only to both hospitals.

  Define: m = length(key) % 128

  Define: n = length(i-th patient name) % 8

  Define: IV = first (m+n) bits of H(name_i, key)

- Step 2. Use AES-CBC with the common key and the IV derived in step 1 to encrypt the patient names.

(b) Requirement 1 is met because the hash function SHA254, IV and AES-CBC are based on patient name and the common key. So long as the patient name does not change, the schema will return the same value.
(c) Requirement 2 is met because the hash function SHA256 returns unique value for each string (name + key), so two patients do not have two identical IV's, nor two identical cypher values.
(d) Requirement 2 is met because the scheme takes into account the key length which is unknown to Eve and the value n = (the patient name length modulo 8). Eve does not know n belong to any specific person.

Problem 5

(a) S^3 = M mod n
(b) Mallory chooses S, she compute S^3 and finds M such that S^3 = M mod n. This is possible because she know S and n, she just divide S^3 by m and take the remainder as M.
(c) Mallory just multiplies S by 4, since 64*S^3 = 64M mod n → (4*S)^3 = 64M mod n
(d) No. No way to get back M from its hash value.

Problem 6

M3 = the concatenation of M1 and M2. T3 is the concatenation of T1 and T2.

Problem 7

Too much theory and few examples in lectures.