ICS 134 – Winter 2015: Homework 1

Name: **UCI ID:**

Q1	Q2	Q3	Q4	Q5	TOT
/20	/20	/20	/20	/20	/100

Due date: January 29, 2015 at noon

Submission Guidelines: Use any word processor, as long as you can covert its output into PDF. Upload your solutions (PDF only) to the class dropbox.

Warning: Homework submissions not following above guidelines will not be graded.

PROBLEM 1. Recall the four modes of operation for symmetric ciphers that we covered in class: ECB, CBC, OFB, CFB. For each mode, explain the precise consequences of a 1-bit error in a single block of ciphertext (the i-the block). Assume that there are n>i plaintext (and ciphertext) blocks total.

PROBLEM 2. One of the problems with ECB mode is that an adversary can re-arrange ciphertext blocks, delete ciphertext blocks and even duplicate (insert) them. We learned that CBC mode is designed to address this problem. However, suppose that you could not use CBC mode. Modify ECB mode such that re-arrangement, deletion and duplication (insertion) attacks are detected. RULE: You cannot use the XOR operation at all. HINT: Think about how to treat plaintext before encryption…

PROBLEM 3. In slide 11 of Lecture 3, you saw an example of a mutual authentication protocol (between Alice and Bob) that used conventional cryptography; it was assumed that Alice and Bob share K_{AB}. Design a mutual authentication protocol between Alice and Bob that uses Public Key cryptography. (Assume that Alice has a public key PK_A and secret key SK_A, and Bob has PK_B and SK_B, respectively.)

PROBLEM 4: Recall using hash functions for message authentication. In one method we need a block cipher E() and a hash function H(). Alice computes MAC(M)=E(K,H(M)) where K is a key shared by Alice and Bob and M is the plaintext message. Alice then sends [M, MAC(M)] to Bob who authenticates M by re-computing MAC(M). Another method needed only a hash function H(). Alice computes HMAC(K,M) using the HMAC definition given in class. She then sends [M, HMAC(K,M)] to Bob who authenticates M by re-computing HMAC(M). Suppose that you discover that H() is insecure – it's actually not weakly collision-resistant. Which of the two methods is more secure in light of your discovery? Explain your answer.

PROBLEM 5. As you know, every US resident has a 9-digit Social Security Number (SSN), which is unique. Let's assume that – given a very large crowd– you select people at random (but only those with blue eyes). Then, you ask each selected person for his/her SSN. You then encrypt, using AES, each person's SSN with a 256-bit key K, which you select, and keep only the first 32 bits of the result. How many blue-eyed people do you need to select in order to have ≥50% probability that at least two of them have the same 32 bits of encrypted SSN. Explain carefully…