CS 4640: Computer Security **Spring 2017**

Homework 3
Total Points 100%

This homework will contribute 5% to your total grade

Due date & time: 11:59 pm on March 2nd, 2017. Submit the homework through ICON. Your submission will be a `pdf` document with the name ⟨your-last-name⟩-⟨your-first-name⟩-homework-3.

Late Policy: You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: The submitted homework must be typed. Using Latex is recommended, but not required. **Please do not write your answers in a paper and take a picture of it.** This is not acceptable.

Papers: The homework requires you to read the following three papers based on which you will answer the following two questions.

1. *New Directions in Cryptography.* Whitfield Diffie and Martin E. Hellman. `https://www-ee.stanford.edu/~hellman/publications/24.pdf`
2. *CryptDB: Protecting Confidentiality with Encrypted Query Processing.* Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. `https://people.csail.mit.edu/nickolai/papers/popa-cryptdb.pdf`
3. *Inference Attacks on Property-Preserving Encrypted Databases.* Muhammad Naveed, Seny Kamara, and Charles V. Wright. `https://cs.brown.edu/~seny/pubs/edb.pdf`

You should read the paper 2 before paper 3. One can read paper 1 independently.

Problem 1 (60 pts) Read the article "New Directions in Cryptography" by Diffie and Hellman, and answer the following questions. [To get a good grade in this question make sure you answer is short and directly to the point. Bullet-points answers are recommended.]

- **a (15 pts)** The paper gives rationales for building encryption schemes that are secure against known plaintext attacks and chosen plaintext attacks, by discussing how such schemes remove restrictions that are placed on the ways of using them. Discuss these rationale in your own words.
- **b (15 pts)** List all the limitations and shortcomings discussed in the paper about symmetric encryption schemes.
- **c (15 pts)** List all the limitations and shortcomings discussed in the paper about symmetric message authentication schemes.

d (15 pts) The paper establishes the relationships among (1) public-key encryption, (2) public key distribution, and (3) digital signature (referred to in the paper as one-way authentication). By relationships, we mean it is possible to use one scheme to implement another. List these relationships, and explain the constructions involved to use one scheme to implement another.

Problem 2 (40 pts) Read the articles "CryptDB: Protecting Confidentiality with Encrypted Query Processing" and "Inference Attacks on Property-Preserving Encrypted Databases", and answer the following questions. [To get a good grade in this question make sure you answer is short and directly to the point. Bullet-points answers are recommended.]

a (20 pts) Does the "*CryptDB*" system IND-CPA secure? **Informally** present your arguments. **I am not looking for a proof**.

b (5 pts) What is the requirement for the attack against deterministic encryption (DTE) (shown in paper 3) to work?

c (15 pts) Is it always the case that the attack against the order-preserving encryption (OPE) shown in paper 3 work? If it does not always work, give a circumstance where the attack may not work?