

## Assignment #1

Due: Tuesday, September 13th, 2005.

### Problem 1 (40 pts) Cryptography:

Read the article “New Directions in Cryptography” by Diffie and Hellman, and answer the following problems.

- a 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 List all the limitations and shortcoming discussed in the paper about symmetric encryption schemes and symmetric message authentication schemes.
- c 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 using one scheme to implement another scheme. Question asked in class was if any public key encryption scheme be used as a digital signature scheme. Please discuss with example, why or why not.

### Problem 2 ( 30 pts) Information Security, Basic Concepts:

- a Chapter 4, Problem 3.

A noted computer security expert has said that without integrity, no system can provide confidentiality.

- a. Do you agree? Justify your answer.
- b. Can a system provide integrity without confidentiality? Again, justify your answer.

- b Please refer to the article given in IEEE Security and Privacy Magazine

(May/June2004): **The Security and Privacy of Smart Vehicles**

<http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=1306972>

Discuss the main security requirements (confidentiality, integrity, availability) in the context of the application domain outlined in the paper.

### Problem 2 ( 30 pts) Data Quality: The CS department of a university has decided to start a data quality campaign. The campaign will mainly regard the improvement of the quality of data available through the CS web site and the improvement of the databases owned by each CS professor and storing students attending to their courses in the current academic year.

- a On the CS web site a list of available courses for graduated students must be published. Each course should consists of: (i) a name, (ii) the instructor’s name and surname, (iii) a schedule, and, if present, (iv) the prerequisites. Please discuss the different types of incompleteness that can occur on publishing the list of courses’ page.

ID-CourseA	Name	Surname	BirthDate
1	Mike	Collins	07/20/1982
2	Anne	Herbert	07/17/1983
3	Julianne	Merrals	07/17/1983
4	Robert	Archer	NULL
5	Mark	Taylor	09/30/1984
6	Bridget	Abbott	09/30/1983
7	John	Miller	04/13/1984
8	Carl	Adams	02/02/1981
9	John	Smith	09/30/1984
10	Edward	Monroe	01/02/1981
11	Anthony	White	NULL
12	Marianne	Collins	10/15/2004

Figure 1: Students of Course A

- b** In the figures 1 and 2, two tables listing the students of course A and course B are shown. It is of interest to perform a semantic accuracy check by cross-matching the two tables. Please apply a record matching algorithm based on a blocking strategy on the Surname field (which means comparing only records that have the same value on the surname field, see also Winkler 2004). Please show the results of the different steps of the algorithm, namely: (i) preprocessing, (ii) blocking on surname , (iii) decision on the records. For the decision on the records, use the decision rule stating that:

*if (R1.Surname = R2.Surname) and (R1.BirthDate) = (R2.BirthDate) than (R1,R2) is a match, else if (R1.Surname = R2.Surname) than (R1,R2) is a possible match, else (R1,R2) is a Non-Match.*

ID	Name	BirthDate
Course B		
1	Bridget Abbott	09/30/1983
2	Mark Taylor	09/30/1984
3	Jude Merrals	07/17/1983
4	John Smith	09/30/1984
5	Anne Herbert	07/17/1983
6	Mike Collins	07/20/1982
7	Carl Adams	02/20/1982
8	John Miller	NULL
9	Monica Collins	NULL
10	Edward Monroe	NULL
11	Anthony Moore	NULL

Figure 2: Students of Course B