

Homework 4 ICS 247 Security Algorithms

Due: Wednesday, March 5, 2003, in class

Please answer the following questions, each of which is worth 10 points.

1. Design a secure public encryption scheme such that

$$E_B(E_A(M)) = E_A(E_B(M)),$$

where E_X denotes encryption using X 's public key.

2. Design a version of a protocol solving Yao's Millionaire problem that can answer the question of whether or not $i < j$ (as opposed to the $i \leq j$ version done in class).

3. Formulate an encryption scheme and an operator $*$ such that

$$E(M_1) * E(M_2) = E(M_1 \cdot M_2),$$

where \cdot denotes modular multiplication.

4. Formulate an encryption scheme and an operator $*$ such that

$$E(M_1) * E(M_2) = E(M_1 + M_2),$$

where $+$ denotes modular addition.

5. Formulate an encryption scheme and operators \oplus and $*$ such that

$$E(M_1) \oplus E(M_2) = E(M_1 + M_2),$$

where $+$ denotes modular addition, and

$$E(M) * c = E(cM),$$

for any constant c .