T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 3
Tue 4.2.2003 12–14 T3 or Wed 5.2.2003 18–20 T1

Question 1 is from Kaufman, Perlman and Speciner, *Network Security: Private Communication in a Public World*, second edition, chapter 4.

1. Consider the following alternative version of CBC-mode. To encrypt a message, use the algorithm for CBC decryption. To decrypt a message, use the algorithm for CBC encryption. Would this work? How is the security of this modification related to normal CBC-mode?

2. Why is it so important that the IV used in CBC-mode is chosen at random? Hint: consider the case where several plaintexts are encrypted using the same key, but different IVs.

   (Many popular protocols such as SSH2 uses a predictable IV in CBC-mode.)

3. A bank uses CBC-mode to encrypt transactions, but does not use any other integrity protection. Assume that the plaintext message has the form

   $$\cdots \mid \text{From account n:o} \mid \text{Message} \mid \text{To account n:o} \mid \text{Amount} \mid \cdots \; ,$$

   where | denotes the block boundaries. For simplicity, we assume that each field is one block long. The interpretation of the message is that amount euros should be paid from the first account to the second account. Suppose that you know which account the transaction is paid to. How can you change the ciphertext so that the amount will be paid to your account instead?

4. Present a known-plaintext attack on 3EDE-DES that uses 2^{112} time and 2^{56} memory.

5. Why should the key used for CBC-MAC be different from the key used in the encryption mode?