T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 9
Tue 8.4.2003 12–14 T3 and Wed 9.4.2003 18–20 T1

1. Are there any truly provably secure encryption methods ?

2. What is the main difference between a "one-way function" such as the RSA problem and a "one-way function" such as SHA-1 ?

3. Discuss the security assumptions of each one of the following cryptographic algorithms:

   - RSA Signature Algorithm (say - PKCS #1 v2.1)
   - Naor-Reingold Number-Theoretic PRF
   - Advanced Encryption Standard.
   - A "provably secure" mode of operation for AES.
   - Secure Socket Layer 3.0

4. Mount a known-plaintext (distinguishing) attack against CBC mode with random IV's. What is the appropriate oracle model ? How would you use the birthday paradox in this case ?