T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 1
Tue 21.1.2003 12–14 T3 or Wed 22.1.2003 18–20 T1

Questions 2–7 are from Kaufman, Perlman and Speciner, *Network Security: Private Communication in a Public World*, second edition, chapter 2.

1. Connect the words.

Cryptology	Cells of (unknown) ancient organisms.
Cryptography	Study of both using and breaking ciphers.
Cryptanalysis	A secret message.
Cryptogram	Breaking secret messages.
Cryptospore	Encrypting messages.

2. What does the dedication "Si spy net work, big fedjaw iog link kyxogy" to Kaufman, Perlman and Speciner mean? (Hint: it is a simple substitution cipher.)

3. A simple scheme to prevent messages from being modified by an attacker is to append to each message M a hash of M. What is wrong with this scheme?

4. Three users, A, B and C, want to use secret key cryptography to identify each other. Each user has a secret key K_A, K_B and K_C, respectively. They use a challenge-response scheme, where a user proves its identity by responding to the challenge with a function of its secret key and the challenge. Why is this scheme insecure?

5. For performance reason, it is common to sign a short digest of the message rather than the message itself. Why it it so important that it is difficult to find two messages with the same digest?

6. What is wrong with the following identification protocol? In the protocol, K_{AB} is a secret key known only by Alice and Bob. (Hint: assume that Alice can open two connections to Bob.)

   - Alice picks a random challenge r_A and sends it to Bob.
   - Bob encrypts r_A with K_{AB} and sends the result to Alice.
   - Bob picks a random challenge r_B and sends it to Alice.
   - Alice encrypts R_b with K_{AB} and sends the result to Bob.

7. Suppose that the work load of legitimate users of a cryptographic scheme grows linearly with the key length. Suppose further that the only way to break the key is a brute-force attack trying all possible keys. If the computational resources of both the legitimate users and potential adversaries doubles due to advances in computer technology, does this work to the advantage of the legitimate users, the adversaries, or does it not make any difference?

8. In 1650 Pierre Fermat conjectured that every number of type $F(n) = 2^{2^n} + 1$ where $n = 0, 1, 2, 3, \ldots$, is a prime number. These numbers are now called Fermat numbers. Prove or disprove his conjecture.