T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 2
Tue 28.1.2003 12–14 T3 and Wed 29.1.2003 18–20 T1

Questions 1–3 are from Kaufman, Perlman and Speciner, *Network Security: Private Communication in a Public World*, second edition, chapter 3.7.

1. Come up with as efficient an encoding as you can to specify a completely general one-to-one mapping (permutation) between 64-bit input values and 64-bit output values. How many such permutations are possible ?

2. Token cards display a number that changes periodically, perhaps every minute. Each device has a unique secret key. A human can prove possession of a particular such device by entering the displayed number into a computer system. The computer system knows the secret keys of each authorized device. How would you design such a device. Only an overview of the key ideas is needed.

3. How many DES keys, on the average, encrypt a particular plaintext block to a particulate ciphertext block. In other words, given 64-bit values P and C, how many keys K (of the 2^{56} possibilities) can be expected to satisfy $DES(K, P) = C$.

4. Describe an efficient chosen-plaintext method of distinguishing a 2-round Feistel cipher from a random permutation.

   A general 2-round Feistel cipher can be described as follows. We split the n-bit plaintext block into two halves $P = (L_0, R_0)$. Now we set $L_1 = L_0 \oplus f_1(R_0)$ and $R_1 = R_0 \oplus f_2(L_1)$, where f_1 and f_2 are unknown $n/2$-bit permutations ("round functions"). The ciphertext block is $C = (L_1, R_1)$.

5. Early versions of the Secure Shell (SSH) protocol employed the RC4 stream cipher initialized with the same key for both directions, (i.e. server $\rightarrow$ client and client $\rightarrow$ server). What is wrong with this idea ? (hint: Eve now has access to two ciphertext streams encrypted with the same keystream.)

6. Early versions of the WAP WTLS (Wireless Transport Layer Security) protocol used simple XOR checksums (exclusive-or of every message word) in conjunction with stream cipher encryption. How would you attack such a system (goal of attack: to modify messages without detection).