T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 1
Thursday 5.2.2004 14.15, room T3.
Markku-Juhani O. Saarinen `<mjos@tcs.hut.fi>`

1. How many different 8-bit block ciphers there can be ? Here we consider ciphers to be different if for some key the same plaintext will produce a different ciphertext. (In other words, how many permutations of 256 elements exist?)

2. One of the very first versions of SSH used stream ciphers in a way that the communication in both directions (from user to host and from host to user) was keyed with the same key. Hence the stream that was xor'ed with the plaintext to produce the ciphertext was the same. What problems can you see in this ?

3. Consider a 2-round Feistel cipher: Let (L_0, R_0) be the message to be encrypted and (L_2, R_2) is the ciphertext.

$$\begin{aligned} L_1 &= R_0 \\ R_1 &= L_0 \oplus f_1(R_0) \\ L_2 &= R_1 \\ R_2 &= L_1 \oplus f_2(R_1) \end{aligned}$$

   Can you see a chosen-plaintext attack that can distinguish such a cipher from a random permutation ? How about 3-round Feistel ciphers ?