T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 3
Thursday 12.2.2004 14.15, room T3.
Markku-Juhani O. Saarinen `<mjos@tcs.hut.fi>`

1. If you flip one bit in CBC-encrypted ciphertext, how much and which part of the corresponding plaintext is affected ?

2. Consider a variant of CBC which uses a constant IV (say, IV $= 0$). Since the IV is constant, it is not necessary to include it with the message; such a mode can be used to construct permutations on strings of length nm, where m is the block length. How can you distinguish such a permutation from a random permutation in a chosen-plaintext attack ?

3. Present a time / memory tradeoff known plaintext attack against an "EEEE" DES mode; a mode which uses 4 independent keys (each 56 bits; 224 total) to encrypt a 64-bit block by applying DES 4 times. An attack is considered effective if $\max(time, memory) < 2^{224}$.