T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 2
Tue 11.2.2003 12–14 T3 and Wed 12.2.2003 18–20 T1

1. Imagine that we would be able to make a table of every 160-bit value of $H(x)$ for every possible 160-bit input x. How many of the 2^{160} possible output values can be expected to be used ?

2. The Davies-Meyer mode for block ciphers works as follows. Use a block cipher $E(K, P)$; K is the key and P is the plaintext. Start with some initial value X_0 and update as $X_{i+1} = E(M_i, X_i) \oplus X_i$. Final value X_n is the hash.

   We ignore the final padding of message with its length and let the user choose X_0.Is there some easy way of breaking this construction ? (i.e. of finding collisions for messages with length greater than zero)

3. Devise a method for finding collisions, which doesn't require too much memory. (i.e. what sort of algorithm is needed to find $H(x) = H(y)$, where $x \neq y$)

4. Devise a method for producing secure hashes of large messages with a property that when 1 random bit is changed, only $O(\log n)$ effort is required to update the hash – rather than $O(n)$. Here n is the length of message (number of message blocks). We assume the existence of a pseudorandom permutation $H(x)$, which operates in $O(n)$ time.