T-79.159 Cryptography and Data Security **Spring 2004**
Tutorial 6
Thursday 11.3.2004 14.15, room T3.
Markku-Juhani O. Saarinen <mjos@tcs.hut.fi>

1. How secure would you expect an Elliptic Curve ElGamal cryptosystem to be with a 192-bit key ?
2. Use Pollard's ρ to factor the 11-digit number 53524124153
3. What is the Discrete Logarithm of 123 modulo p=541, where the generator g=2 ?