HW – ECDSA (Due date:1/7/2011)

- Suppose E be the elliptic curve $y^2=x^3+x+6$ over Z_{11}. The base point $B=(2,7)$ and Bob's private key is $d=7$.
- Q1: Find the corresponding public key Q
- Q2: Assume $h=H(M)=4$. Please use the random number $k=4$ to sign the message M. What is the output (r, s) of the signature?
- Q3: Verify that the signature you generated is correct.