# Cybermen Elliptic Curve Procedure

1. Use Calculator at <https://andrea.corbellini.name/ecc/interactive/modk-mul.html>
2. Use curve A = 5, B = 3  y2 = x3 + 5x + 3
3. Use Field p = 211
4. Use Base point P: x = 17, y = 123
5. Both sides select private number, compute public point Q: x = , y = , as in Crypto homework 7
6. Both sides exchange public point Q:, compute shared key, as in Crypto homework 7
7. To compute session key for AES take the x coordinate of the shared key and add x’s to the end until it is 16 bytes long
   1. Example: 192 becomes 192xxxxxxxxxxxxx  
      
   2. Instructor note: often people will hash the number and use part of the hash for the session key, but let’s keep it simple
8. Use AES.ECB\_MODE (ECB has no nonce, no tag) with the session key
9. Encode the encrypted message with base64 for text transmission