# Cybermen Elliptic Problem

The Doctor gets on Graham’s terminal on the Cybermen spaceship and immediately fires up Wireshark to see what traffic she can capture. After examining several TCP streams, she finds an interesting one.

Cybermen Master: Prepare to receive encrypted message. Use Cybermen Elliptic Curve Procedure. My public key is 17, 23.

Cyberman15: Acknowledge. My public key is 17, 88

Cybermen Master: Message follows.

5ONHPLXu8wPGNibvCq+uI9zUw+oIkBSvMHVdBwY1DOUT8KLuTg6mta0rzcedKZEGbTTkdfZgLZen\n0K2uUGkbAPGgSF2aMa4uk1z4DY08jPg=\n

Your job is to decrypt the message (duh 😊).

Hint: The Cybermen have chosen a modulus (211) and curve that results in 232 points. However, they chose a terrible base point in the Cybermen Elliptic Curve Procedure. It has a small subgroup.

Hint: Before you try to break anyone’s key, put their curve, field, and base point P into the calculator and play with N. You may find there are not many choices for the shared key.

Hint: You could just list all the possible x coordinates from the hint before. Convert the x coordinates to session keys and see if one of them decrypts the message.