# Cybermen Diffie Hellman Problem (small subgroup)

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 Diffie Hellman Procedure. My public key is 19137. Priv was 49299

Cyberman15: Acknowledge. My public key is 13135. Priv was 25643

Cybermen Master: Message follows.

I7w5ncyw96zmSAFfZJ8y+lfQGMJQI/i6YxvwFLuCMAEKVfMx8q/si9nyMNUNALhoyVbNZ+xMfYTIgmFAriSMC4gDBVKCYBBEFGnhGFQw1Bm5UYC9GFsq8qHfFzAUCsgp

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

The hints are base64 encoded. If you want to view a hint, you can use  
<https://gchq.github.io/CyberChef/#recipe=To_Base64('A-Za-z0-9%2B/%3D')>

Hint: The Cybermen have chosen a modulus (29311) and generator (3679) that results in a very small subgroup.   
VGhlIEN5YmVybWVuIGhhdmUgY2hvc2VuIGEgbW9kdWx1cyAoMjkzMTEpIGFuZCBnZW5lcmF0b3IgKDM2NzkpIHRoYXQgcmVzdWx0cyBpbiBhIHZlcnkgc21hbGwgc3ViZ3JvdXAuICA=

Hint: One way: use Python or a calculator that can do powers in modular arithmetic to see the possible values of gx mod p. There won't be many.  
T25lIHdheTogIHVzZSBQeXRob24gb3IgYSBjYWxjdWxhdG9yIHRoYXQgY2FuIGRvIHBvd2VycyBpbiBtb2R1bGFyIGFyaXRobWV0aWMgdG8gc2VlIHRoZSBwb3NzaWJsZSB2YWx1ZXMgb2YgZ3ggbW9kIHAuICBUaGVyZSB3b24ndCBiZSBtYW55Lg==

Hint: Convert the possible values of gx mod p to session keys and see if one of them decrypts the message.  
Q29udmVydCB0aGUgcG9zc2libGUgdmFsdWVzIG9mIGd4IG1vZCBwICB0byBzZXNzaW9uIGtleXMgYW5kIHNlZSBpZiBvbmUgb2YgdGhlbSBkZWNyeXB0cyB0aGUgbWVzc2FnZS4=

Hint: Another way: since the subgroup is so small, you should be able to crack one of the public keys easily. Just compute gx mod p until you get their public key. It may not be the exact number they used for their private key, but it will crack the decryption.  
QW5vdGhlciB3YXk6ICBzaW5jZSB0aGUgc3ViZ3JvdXAgaXMgc28gc21hbGwsIHlvdSBzaG91bGQgYmUgYWJsZSB0byBjcmFjayBvbmUgb2YgdGhlIHB1YmxpYyBrZXlzIGVhc2lseS4gIEp1c3QgY29tcHV0ZSBneCBtb2QgcCB1bnRpbCB5b3UgZ2V0IHRoZWlyIHB1YmxpYyBrZXkuICBJdCBtYXkgbm90IGJlIHRoZSBleGFjdCBudW1iZXIgdGhleSB1c2VkIGZvciB0aGVpciBwcml2YXRlIGtleSwgYnV0IGl0IHdpbGwgY3JhY2sgdGhlIGRlY3J5cHRpb24u

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

I7w5ncyw96zmSAFfZJ8y+lfQGMJQI/i6YxvwFLuCMAEKVfMx8q/si9nyMNUNALhoyVbNZ+xMfYTIgmFAriSMC4gDBVKCYBBEFGnhGFQw1Bm5UYC9GFsq8qHfFzAUCsgp

A screenshot of a computer

Description automatically generated