# 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.

Cyberman15: Acknowledge. My public key is 13135.

Cybermen Master: Message follows.

I7w5ncyw96zmSAFfZJ8y+lfQGMJQI/i6YxvwFLuCMAEKVfMx8q/si9nyMNUNALhoyVbNZ+xMfYTIgmFAriSMC4gDBVKCYBBEFGnhGFQw1Bm5UYC9GFsq8qHfFzAUCsgp

The Doctor says, "Hmm, that modulus is only 32 bits long and is crackable. I think it would take a few hours to crack on our laptop, but we don't have time for that. Let me see if I can make them use something that is easier to crack."

She sends:  
Cyberman15: Unable to decrypt message. Please resend message with p = 41495592889 (unchanged from procedure) but use generator g = 2679865019.  
My public key is

Cybermen Master: Ack

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:   
VGhlIEN5YmVybWVuIGhhdmUgY2hvc2VuIGEgbW9kdWx1cyAoMjkzMTEpIGFuZCBnZW5lcmF0b3IgKDM2NzkpIHRoYXQgcmVzdWx0cyBpbiBhIHZlcnkgc21hbGwgc3ViZ3JvdXAuICA=

Hint:   
T25lIHdheTogIHVzZSBQeXRob24gb3IgYSBjYWxjdWxhdG9yIHRoYXQgY2FuIGRvIHBvd2VycyBpbiBtb2R1bGFyIGFyaXRobWV0aWMgdG8gc2VlIHRoZSBwb3NzaWJsZSB2YWx1ZXMgb2YgZ3ggbW9kIHAuICBUaGVyZSB3b24ndCBiZSBtYW55Lg==

Hint:   
Q29udmVydCB0aGUgcG9zc2libGUgdmFsdWVzIG9mIGd4IG1vZCBwICB0byBzZXNzaW9uIGtleXMgYW5kIHNlZSBpZiBvbmUgb2YgdGhlbSBkZWNyeXB0cyB0aGUgbWVzc2FnZS4=

Hint:   
QW5vdGhlciB3YXk6ICBzaW5jZSB0aGUgc3ViZ3JvdXAgaXMgc28gc21hbGwsIHlvdSBzaG91bGQgYmUgYWJsZSB0byBjcmFjayBvbmUgb2YgdGhlIHB1YmxpYyBrZXlzIGVhc2lseS4gIEp1c3QgY29tcHV0ZSBneCBtb2QgcCB1bnRpbCB5b3UgZ2V0IHRoZWlyIHB1YmxpYyBrZXkuICBJdCBtYXkgbm90IGJlIHRoZSBleGFjdCBudW1iZXIgdGhleSB1c2VkIGZvciB0aGVpciBwcml2YXRlIGtleSwgYnV0IGl0IHdpbGwgY3JhY2sgdGhlIGRlY3J5cHRpb24u