# Cybermen Diffie-Hellman Encryption Procedure

1. Use modulus p = 41495592889. This should be large enough to prevent brute force attacks.
2. Use generator g = 2. In the slides, g is called α.
3. Each side selects a private key between 2 and p - 2.
4. Each side computes a public key using pow(g, private key, p)
5. Share the public keys with each other.
6. Each side computes the Diffie-Hellman key using   
   DH key = pow(other's pub key, your priv key, p)
7. Both sides should now have the same DH key.
8. The DH key will be too short for AES-128, which needs a key length of 16. To compute session key for AES take the DH key and add x’s to the end until it is 16 bytes long
   1. Example: 192 becomes 192xxxxxxxxxxxxx  
      
   2. Instructor’s note: often people will use hashes or a Key Derivation Function to create the session key, but let’s keep it simple.
9. Use AES.ECB\_MODE (ECB has no nonce, no tag) with the session key.
10. Encode the encrypted message with base64 for text transmission.