Ciphers and Number Theory 8

1. Show that 6 is a primitive root in $\mathbb{Z}_{13}$.

2. Alice and Bob use Diffie-Hellman to calculate a secret key with $p = 13$ and $g = 6$. Given that Alice chooses exponent $a = 4$ and Bob chooses exponent $b = 3$, explain what information is exchanged betweeen them and determine the final key.

3. It is proposed to apply Diffie-Hellman with $p = 13$ and $g = 8$. Why is this not a good idea?

4. Take $p = 47$ and $g = 10$ (a primitive root in $\mathbb{Z}_{47}$). Alice chooses exponent $a = 5$ and Bob chooses exponent $b = 11$, and Bob wishes to send the message $c = 17$. Using the above data, give Alice's public key for ElGamal encryption, and also Bob's encrypted message. Show that Alice can decrypt this message.

5. Return to the examples on Sheet 7 and use the Chinese Remainder Theorem to speed up the decryption process.