

## Cryptography Assignment 4

1. Show how a “man in the middle” attack can break the Diffie-Hellman key exchange allowing Eve to read and manipulate messages. Here Eve pretends to be Alice to Bob and vice versa.
2. Let  $p = 37$ .
  - (a) Show that 3 is not a primitive root of  $p$  and 5 is a primitive root.
  - (b) Use the Pohlig-Hellman algorithm to find the  $x$  such that  $5^x \equiv 28 \pmod{37}$ .
3. Let  $p$  and  $q$  be primes such that  $p = 2q + 1$ .
  - (a) Show that  $p \equiv 5 \pmod{6}$ .
  - (b) Show that for all positive integers  $x, y, z$  relatively prime to  $p$ ,  $x^q + y^q \neq z^q$ .  
(Special case of Fermat’s last theorem)

Item (b) was first proved by Sophie Germain in 1825 and because of this such  $q$  are called Sophie Germain primes.