1. Consider Diffie-Hellman Key Exchange where Alice and Bob have chosen prime value 17 and primitive root 5.
If Alice's secret key is 4 and Bob's secret key is 6, determine the secret key they exchanged. (5 points)

> From Alice, $\alpha = 4 \overset{R}{\leftarrow} Z_{17}, u \leftarrow g^{\alpha} = 5^4 = 625$
>
> From Bob, $\beta = 6 \overset{R}{\leftarrow} Z_{17}, v \leftarrow g^{\beta} = 5^6 = 15625$
>
> Secret key from Alice: $w \leftarrow v^{\alpha} = 15625^4 = 59,604,644,775,390,625$
>
> Secret key from Bob: $w \leftarrow u^{\beta} = 625^6 = 59,604,644,775,390,625$

2. Using the RSA cryptosystem, encrypt the message x = 3, assuming the two primes chosen to generate the keys are p = 13 and q = 7.
You should choose a value e < 10. Show your calculations and assumptions. (5 points)

> Assume $e = 5$, here we have $gcd(e, p-1) = 1, gcd(e, q-1) = 1$ and $p\neq p $
>
> $n \leftarrow pq = 91$
>
> $d \leftarrow e^{-1} \bmod (p-1)(q-1) = 5^{-1} \bmod 72 = 29$
>
> $pk \leftarrow (91, 5), sk \leftarrow (91, 29)$
>
> $F(pk, x) := 3^5 \bmod 91 = 61$
>
> Check: $I(sk, y) := 61^{29} \bmod 91 = 3$