1. Fix RSA parameters $p = 307$, $q = 311$, $n = p \cdot q$, public key pk $= (247, n)$, and secret key sk $= (55303, n)$. Use square-and-multiply to sign the message $m \equiv 2 \pmod{n}$.

Need to compute sig $= m^d \pmod{n} = 2^{55303} \pmod{95477}$

In binary, 55303 is 1101100000000111

I did the calculations using sagemath, and got sig $= \boxed{81901}$.

To verify, I compute $sig^e \pmod{n} = 81901^{247} \pmod{95477}$ and got 2, as expected.

2. Suppose that you see in the public database that a message $m \equiv 2 \pmod{110107021}$ has been signed as

$$(\text{sig}, \text{pk}) = (33554432, (8806881, 110107021)).$$

(a) Without computing $\varphi(110107021)$, sign the message

$$m \equiv 6172 \pmod{110107021}$$

as if you are the owner this RSA key. (You are advised to use a computer for this exercise, but it is possible to do by hand).

$e = 8806881$

$n = 110107021 = pq$

want m^d, where $d = e^{-1} \pmod{\varphi(n)}$ not this, since can't compute $\varphi(n)$

alt: want sig s.t. $6172 \equiv \text{sig}^{8806881} \pmod{n}$

33554432.factor() $= 2^{25}$: Use this fact

$\Longrightarrow$ $d = 25$

$\text{sig}' = 6172^{25} \pmod{110107021}$

$\Longrightarrow$ $(\text{sig}', \text{pk}) = (27417578, (8806881, 110117021))$

3. This question is about ElGamal signatures. Our public setup parameters will be $p = 37$ and $g = 2$.

   (a) You observe two parties claiming the identity with public key $g^a = 23$. In order to check which party is honest (if any), you ask both parties to sign the message $m \equiv 1 \pmod{36}$. You receive the signatures

$$(r_a, sig_a) = (25, 13)$$

   from party A and

$$(r_b, sig_b) = (30, 6)$$

   from party B. Check which of these parties is honest.

$g^m \pmod{p} = 2.$

Party A: $pk^{r_a} \cdot r_a^{sig_a} \pmod{p}$

$= 23^{25} \cdot 25^{13} \pmod{37}$

$= 2$

Party B: $pk^{r_b} \cdot r_b^{sig_b} \pmod{p}$

$= 23^{30} \cdot 30^{6} \pmod{37}$

$= 11.$

Thus $\boxed{\text{party A}}$ is honest.

(b) An honest party with public key 23 signs message $m_1 = 14 \pmod{36}$ with the signature

$$(r_1, sig_1) = (19, 19)$$

and $m_2 = 4 \pmod{36}$ with the signature

$$(r_2, sig_2) = (19, 29).$$

Sign a message $m_3 = 25 \pmod{36}$ as if you are the person with public key 23.

Note $r_1 = r_2$, meaning the nonce k was repeated. We compute it as

$$k \equiv \frac{m_1 - m_2}{sig_1 - sig_2} \pmod{p-1}$$

$$\equiv \frac{14-4}{19-29} \pmod{36}$$

$$\equiv \boxed{35}.$$

Then we can find the secret key a:

$$sig_1 = k^{-1}(m_1 - ar) \pmod{p-1}$$

$$\Longrightarrow a = -(k \cdot sig_1 - m_1)\, r^{-1} \pmod{p-1}$$

$$= -(35 \cdot 19 - 14) \cdot 19^{-1} \pmod{36}$$

$$= \boxed{15}.$$

Now we use it to sign our message:

$$sig_3 = k^{-1}(m_3 - ar) \pmod{p-1}$$

$$= 35(25 - 15 \cdot 19) \pmod{36}$$

$$= 8$$

should choose a new nonce

We can verify as follows:

$$pk^r \cdot r^{sig} \pmod{p} = 23^{19} \cdot 19^8 \pmod{37}$$

$$= 20 = 2^{25} \pmod{37} = g^m$$

4. You should use SageMath for this question.

(a) The command for '$n \pmod p$' in SageMath is '$n \% p$'. By checking all the possible values of $2^a \pmod{31}$, show that 2 does not generate $\mathbb{F}_{31}^*$ as a multiplicative group.

It only generates the numbers 1, 2, 4, 8, 16.

✓

(b) Find a generator of $\mathbb{F}_{31}^*$ as a multiplicative group.

(c)* How many possible choices of generator are there for $\mathbb{F}_{31}^*$?

I found, through brute force computation, that the generators are: 3, 11, 12, 13, 17, 21, 22, and 24.

✓

5. By implementing Pohlig-Hellman in SageMath, compute a such that

$$11^a \equiv 8080 \pmod{12289}.$$

skipping this one

6. You should use SageMath for this question.

(a) Let n be the numbers in your UoB username (for example, my UoB username is ul19594, so for me $n = 19594$), and using the SageMath command

```
.next_prime()
```

let p be the smallest prime number $> n$. Find a generator g of $\mathbb{F}_p^*$, using SageMath commands. (It is sufficient to write down a generator together with the command that you used to find it).

n= 23068
p= 23071

g = 3

command: order = Mod(3, p).multiplicative_order()

(b) Using the SageMath command

```
.random_element()
```

choose a random element h in $\mathbb{F}_p^*$, and let that be Alice's public key g^a, where g is as in part (a). Use Pohlig-Hellman (aided by SageMath) to find a.

h= 21414