E1

a) Alice will exchange the public key with Bob, that being $3 = 2^8 \% 11 = A$

b) Bob will do the same thing with his equation, he will send $6 = 2^9 \% 11 = B$

c) The key K is 4, we know this because Alice calculates $4 = B^8 \% 11 = K$ and bob calculates $4 = A^9 \% 11 = K$

d) A MITM would only observe p, g, A, B the private keys would stay hidden

e) They can't calculate K without a and b, neither of which were ever sent

f) Mathematically it can be brute forced but in most cases it is effectively impossible

E2

a) φ/Φ represents a euler function

b) In this case Φ(n) = 72 and 1 % 72 = 1, d*e is 505, her number is incorrect

c) Alice would send n = 91 = P*Q in addition to e = 5

d) Alice will keep 7 and 13

e) He will send 82

f) Alice can decrypt by taking $(c^d)\ mod\ n$

g) An attacker would still need the Φ(n)

h) The attacker can't really do anything without the private key

E3

a) Yes this is correct, if we perform the encryption with the calculation $20^7 \% 33$ we get 26

```
e = 7
n = 33
m = 20
c = m ** e % n
print(c)
```

b) In all honesty I am struggling with understanding this part, I would appreciate any additional resources that might help with my comprehension

c) She could change her private key regularly