7^(-1) mod 33 means the multiplicative inverse of 7 in mod 33
by definition, it is an integer x, so that x * 7 mod 33 = 1 mod 33
19 * 7 mod 33 = 133 mod 33 = 1 mod 33
Hence, 19 is the multiplicative inverse of 7 in mod 33

If you want to know how to calculate, then you need to know
the Extended Euclidean Algorithm, but it's out of the scope of this course,
we are more interested in using the algorithm, so you can use Wolfram Alpha

How to find 7^(-1) mod 33, use Extended Euclidean Algorithm
or you can use Wolfram Alpha

23^(-1) mod 551 = 24
Check again: 23 * 24 mod 551 = 1 mod 551

To find the private key, we apply the following equation:
d * e mod ϕ(n) = 1
Hence, d = e^(-1) mod ϕ(n), it means d is the multiplicative inverse of e mod ϕ(n)
d = 59^(-1) mod 504 and using Wolfram Alpha, d = 299

Check again:
299 * 59 mod 504 = 1 (true)

d * e mod ϕ(n) = 1 mod ϕ(n)

IN RSA, the private key is the multiplicative inverse of e mod ϕ(n)
It means d * e mod ϕ(n) = 1 mod ϕ(n), hence d = e^(-1) mod ϕ(n)

Question 4

To break RSA, we need to know the public key, because this is public, so we can get it easily
The public key has 2 numbers: (n, e)

We can factorise n, to find p and q (there are algorithms to factorise a number)
(or you can go to wolfram alpha, and type factorize [the number you want])

From the key generation formula, you know n is the product of two prime numbers, n = p * q
Hence, we try to find either p or q. If we can find q, then q = n / p

If we can find p and q, then we can find ϕ(n) because ϕ(n) = (p - 1) * (q - 1)

If we can find ϕ(n), then can we find d because d = e^(-1) mod ϕ(n),

If we can find d, then we can decrypt C to get the value of M

n = 481, how can I find q or p

I will creat a program, and set p = 2, 3, 5, 7 … (prime numbers)
and try to divide n by p, if the result is an integer, then I have found out either p or q

481 / 2 =
481 / 3 =
481 / 5 =

We divide by prime numbers because of the

or I can go to wolfram alpha and type **factorise 481**