$c \cdot d \equiv e \cdot m \cdot d \pmod{n}$

$n \cdot M = ed - 1 \Rightarrow n \mid ed - 1 \Rightarrow ed \equiv 1 \pmod{n}$

$\Rightarrow e \cdot m \cdot d \equiv m \pmod{n} \Rightarrow c \cdot d \equiv m \pmod{n}$

Try to break this scheme!

We have public key (n, e) and ciphertext c.
What do we need to compute the plaintext message from n, e, c?

→ We need a number d s.t. $ed \equiv 1 \pmod{n}$,

~~$n = (ed-1)/M$~~ i.e. $n \mid ed - 1 \Leftrightarrow \exists k$:

$n \cdot k = e \cdot d - 1 \Leftrightarrow 1 = e \cdot d - n \cdot k$

compute $\gcd(e, n)$: $1 = e \cdot a + n \cdot b$

$a \to d$, $b \to k = -b$

$\Rightarrow e \cdot d \equiv 1 \pmod{n}$

$\Rightarrow c \cdot d \equiv e \cdot m \cdot d \equiv m \pmod{n}$

$e \cdot d = 1$, m ← plaintext □