In each of the following examples, Alice and Bob wish to send messages to one another and eve wishes to intercept the message. RSA is either used incorrectly (yields an incorrect result), is used correctly but can be broken, or is both correct and can not be broken. Select the option that best applies and explain. Assume that p, q are prime and Bob publishes the public key $(N = pq, e)$

(a) Eve, Alice, and Bob share a menu. Bob asks Alice what dish she wants, and Alice responds with the name of the dish using standard RSA encryption.

> **Solution:** *Broken*. Since there are a finite number of options, Eve can just guess-and-check. Eve knows the public key that Bob will release in order to receive Alice's message, so now Eve can just encrypt all menu items using e and see which one matches Alice's encrypted message, which she can publicly see.

(b) Eve is able to extort extra details from Alice and Bob. She now also knows the value of $(p-1)(q-1) \pmod p$

> **Solution:** *Correct*. Eve's goal is to compute $(p-1)(q-1)$ so that she is able to find $d = e^{-1} \mod (p-1)(q-1)$.
>
> Given $(p-1)(q-1) \equiv pq - p - q + 1 \equiv -q + 1 \pmod p$, Eve can find $q \pmod p$. But this simply isn't enough information since rewriting $q = kp + m$ where m is known introduces another variable k. Using the only other information we have about p and q, $N = pq = kp^2 + mp$.
>
> Now, to solve for k, Eve would have to be able to efficiently factor $p(q-m)$, which we know is a hard, otherwise she can also efficiently factor pq.

(c) Bob selects e where e is coprime to N but not coprime to $(p-1)(q-1)$.

> **Solution:** *Incorrect*. RSA works only if e is coprime to $(p-1)(q-1)$ so that there exists $d = e^{-1} \pmod{(p-1)(q-1)}$.
>
> It is possible for e to be coprime with N but not with $(p-1)(q-1)$. For instance, if $p = 5$ and $q = 7$, choose $e = 4$. Now, there is no multiplicative inverse such that $4d \equiv 1 \pmod{4 \cdot 6}$.