Cryptography 2nd Homework

1. Solve the following system of congruences:

$$\begin{aligned} 13x &\equiv 4 \pmod{99} \\ 15x &\equiv 56 \pmod{101} \end{aligned}$$

2. For $n = pq$, where p and q are distinct odd primes, define

$$\lambda(n) = \frac{(p-1)(q-1)}{gcd(p-1, q-1)}.$$

Suppose that we modify the RSA Cryptosystem be requiring that $ed \equiv 1 \pmod{\lambda(n)}$.

(a) Prove that encryption and decryption are still inverse operations in this modified cryptosystem.

(b) If $p = 37$, $q = 79$, and $e = 7$, compute d in this modified cryptosystem, as well as in the original RSA Cryptosystem.