Ryan Pollack

1. We know P and Q are two prime numbers and P·Q = N.
The prime numbers up to 54 are:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53
Either P or Q must be one of those.
If we look the next highest prime, being 59, we would see the 2nd number couldn't be above 48:
N = 2881 / 59 ≈ 48.8
So, if both P and Q are prime numbers and one of the primes is over 54 (aka 59, 61, 67, ...), the other must be under 48.8 and thus under 48 (aka 47, 43, 41). Therefore, at least one of P and Q is under 54.

2. Since one of the values must be under 48.8, we can take each prime under it and divide by the product of P·Q as 2881 so:
~Under 48.8~
2,281 / 47 ≈ 61.29 X not a prime
2,881 / 43 = 67 ✓ a prime
43 and 67 are both primes and their product is 2,881, therefore P = 43 and Q = 67.

3. (P − 1) = (43 − 1) = 42   42 · 66 = 2,772
(Q − 1) = (67 − 1) = 66   (P−1)(Q−1)
We already know E = 1,109 is always a prime number. So,
GCD = (E, (P−1)(Q−1)) = GCD(1,109, 2,772) = 1
Therefore, E and (P−1)(Q−1) are relatively prime because the greatest integer that divides them both is 1.

4. D is a modular inverse of E so:

$\therefore D \equiv E^{-1} \pmod{(P-1)(Q-1)}$

$D \equiv E^{-1} \pmod{(42 \cdot 68)}$

$D \equiv E^{-1} \pmod{2,772}$

$D \equiv 1,109^{-1} \pmod{2,772}$

$D \approx .0000159$

5. We can decode using $M \equiv C^{D} \pmod{N}$. Breaking down into each block, we know N is 2,881, C is each individual block (which must be less than N) and D is .0000159. So, doing each block individually:
(which is probably wrong)

1. $1,567^{.0000159} \pmod{2,881} \equiv$
2. $214^{.0000159} \pmod{2,881} \equiv$
3. $1023^{.0000159} \pmod{2,881} \equiv$
4. $398^{.0000159} \pmod{2,881} \equiv$
5. $581^{.0000159} \pmod{2,881} \equiv$
6. $1,427^{.0000159} \pmod{2,881} \equiv$
7. $1,623^{.0000159} \pmod{2,881} \equiv$
8. $2,679^{.0000159} \pmod{2,881} \equiv$
9. $895^{.0000159} \pmod{2,881} \equiv$
10. $948^{.0000159} \pmod{2,881} \equiv$
11. $951^{.0000159} \pmod{2,881} \equiv$

All these become individual then put together and encrypt

Bonus 1. So we know $P \cdot Q = N$, then we can write:

$$\phi(N) \rightarrow \phi(P \cdot Q) = (PQ - 1) - (P - 1) - (Q - 1)$$
$$\phi(P \cdot Q) = PQ - 1 - P + 1 - Q + 1$$
$$\phi(P \cdot Q) = PQ - P - Q - 1$$
$$\phi(P \cdot Q) = P(Q-1) - (Q-1)$$
$$\phi(P \cdot Q) = (Q-1) \cdot (P-1)$$
$$\phi(N) = (P-1)(Q-1)$$

Bonus 2. We know $N = P^2$, so

$$\phi(N) \rightarrow \phi(P^2)$$

We can write out a set from 1 to P^2 where:

$$\{0, 1, 2, \ldots, p, (p+1), \ldots (p^2-1), p^2\}$$

Now we can search for which numbers aren't relatively prime to p^2. The numbers not relatively prime are the multiples of p, being $0, p, 2p$, etc. It's every 'p^{th}' number, so it is:

$$\phi(p^2) = p^2 - p$$