Theory: \( C \equiv P^e \mod p \)

1) Here \( P \) denotes the number blocks of the plain text, for example 2200, 0819, etc. in the above example. Then we obtain \( C \) by the above formula, where \( C \) denotes the corresponding blocks of ciphertext numbers.

For \( P = 2200 \), we have \( C = 602 \), etc.

2) To decrypt the ciphertext, we need to recover \( P \) from \( C \). The following steps are used. The decryption key is an integer \( d \) such that \( de \equiv 1 \mod (p-1) \). Since \( (e, p-1) = 1 \), we have integers \( d, k \) such that

\[
de + k(p-1) = 1,\text{ hence } de \equiv 1 \mod (p-1).
\]

3) Take a ciphertext block \( C \). Then we get,

\[
C \equiv P^e \mod p
\]

\[
\Rightarrow C^d \equiv P^{de} \mod p \equiv P \mod p, \text{ as } de + k(p-1) = 1,
\]

\[
\Rightarrow C^d \equiv P \equiv (p^{k(p-1)}) \mod p; \text{ suppose } p \nmid p
\]

\[
\Rightarrow C^d \equiv P \mod p, \text{ as by } \exists \overline{1} \text{ with } P \equiv 1 \mod p.
\]

If \( p \nmid P \), then \( P = 0 \), as \( 0 \leq P < p \), we have \( C = 0 \), since \( C \equiv P^e \mod p \), so \( C \equiv 0 \mod p \).
As $0 < c < p$, we conclude that
\[ C^d \equiv 0 \mod p \implies C^d \equiv 1 \mod p \] in this case as well.

**Summary:** For given prime $p$ and number $e$ relatively prime to $p-1$, choose $d$ such that $ed \equiv 1 \mod (p-1)$. This is possible as $(e, p-1) = 1$.

**Coding:** $C = P \mod p$,

**Decoding:** $P \equiv C^d \mod p$.

In all cases $P$ and $C$ are chosen between 0 and $(p-1)$ inclusive, namely the possible remainders when dividing by $p$.

If $e = 3$, encrypt the message GOOD MORNING.

Note $25 < p < 2525$, for $p=101$.

Hence $m = 1$, $2m = 2$.

The numerical equivalents for GOOD MORNING, in blocks of 2 = $2m$ digits are:

06 14 14 03 12 1417 13 08 12 06.
Raise each of these 2 digit numbers to the 3\textsuperscript{rd} power, since \( e = 3 \) and reducing modulo 101 gives 14 17 17 27 11 17 65 76 07 76 14.

Eq: What is the plain text message that corresponds to the ciphertext 01 09 00 12 12 09 24 10 that is produced using modular exponentiation with modulus \( p = 29 \) and encryption exponent \( e = 5 \)?

By: \( p = 29, \ e = 5 \).

Inverse of \( e = 5 \) modulo \( p - 1 = 28 \) is 17, since 
\[5 \times 17 = 105 \quad \text{and} \quad 105 \equiv 1 \pmod{28}, \]
\[28 \times 4 = 104 = 105 - 1.\]

Raise each block to 17\textsuperscript{th} power and reduce modulo 29. We then get 01 04 00 12 12 04 20 15

Plain text: BEAM ME UP.