Extra 1 Given key $(e, n) = (13, 2537)$, encrypt "PUBLIC KEY CRYPTROGRAPHY"

Convert to plaintext, p, using table

$p = 1520\ 0111\ 0802\ 1004\ 2402\ 1724\ 1519\ 1406\ 1700\ 1507\ 24$

We want to produce a ciphertext, c, where $c = p^e (modn)$

$c = c_1c_2c_3c_4c_5c_6c_7c_8c_9c_{10}c_{11}$

$c_1 = 1520^{13} \text{ mod } 2537 = 0095$

$c_2 = 0111^{13} \text{ mod } 2537 = 1648$

$c_3 = 0802^{13} \text{ mod } 2537 = 1410$

$c_4 = 1004^{13} \text{ mod } 2537 = 1299$

$c_5 = 2402^{13} \text{ mod } 2537 = 0811$

$c_6 = 1724^{13} \text{ mod } 2537 = 2333$

$c_7 = 1519^{13} \text{ mod } 2537 = 2132$

$c_8 = 1406^{13} \text{ mod } 2537 = 0370$

$c_9 = 1700^{13} \text{ mod } 2537 = 1185$

$c_{10} = 1507^{13} \text{ mod } 2537 = 1957$

$c_{11} = 24^{13} \text{ mod } 2537 = 2130$

So ciphertext is 0095 1648 1410 1299 0811 2333 2132 0370 1185 1957 2130

Extra 2 Given ciphertext $c = 2206\ 0755\ 0436\ 1165\ 1737$

And key $(e, n) = (13, 2747)$

Decrypt the message. We want plaintext, p

We know $c^d = (p^e)^d = p^{ed} = p^{1+\phi(n)t} \pmod n$ for some t

So $c^d = p * p^{\phi(n)t} \pmod n$

We know by a previous theorem that $p^{\phi(n)t} = 1$

So $c^d = p \pmod n$

Find d

We know by Bezout's theorem that given relatively prime numbers $e, \phi(n)$,

Then there exists d, f such that $ed + \phi(n)f = 1$

Find $\phi(n)$

Given $n = 2747$, $\phi(2747) = \phi(41)\phi(67) = (41 - 1)(67 - 1) = 2640$

Find d, f such that $13d + 2640f = 1$

Using Euclidean Algorithm

2640 = 13(203) + 1

13 = 1(13) + 0

So gcd(2640,13) = 1 (true)

1 = 2640 + 13(-203)

We want d positive

$d_0 = -203, f_0 = 1$

$d = d_0 + \frac{f}{gcd(e,\phi(n))} * t$ for some t

$f = f_0 - \frac{d}{gcd(e,\phi(n))} * t$ for some t

Let $t = 1$, then $d = -203 + (2640) = 2437, f = 1 - (13) = -12$

Verifying, $13(2437) + 2640(-12)$ is true

So $d = 2437$ works

So for $c = 2206$, $p = 2206^{2437} = 617 \pmod n$

$c = 0755, p = 0755^{2437} = 0404$ (mod n)

$c = 0436, p = 0436^{2437} = 1908$ (mod n)

$c = 1165, p = 1165^{2437} = 1306$ (mod n)

$c = 1737, p = 1737^{2437} = 1823$ (mod n)

So plaintext message is 0617 0404 1908 1306 1823

Using the table to convert back to letters, this is GREETINGSX