Hmw 5

1).

a. $p = 3,\ q = 11,\ e = 7,\ m = 5$

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$

$\gcd(20, 7) = 1$

$d \times e \bmod \phi(n) = 1$

$7d \bmod 20 = 1$

$d = 3$

public key = $\{7, 33\}$

private key = $\{3, 33\}$

so,

encryption:

$c = m^e \bmod n$

$= 5^7 \bmod 33$

$= 14$

Decryption:

$= c^d \bmod n$

$= 14^3 \bmod 33$

$= [(5^4 \bmod 33) \cdot (5^2 \bmod 33) \cdot (5^1 \bmod 33)] \bmod 33$

$= 3875 \bmod 33.$

b). $p = 5,\ q = 11,\ e = 7,\ m = 5$

$n = p \times q = 5 \times 11 = 55$

$\phi(n) = (p-1) \cdot (q-1) = 4 \times 10 = 40$

$\gcd(40, 3) = 1$

$3d \bmod 41 = 1$

$d = 27$

public key = $\{3, 55\}$

private key = $\{27, 55\}$

encryption = $9^3 \bmod 55 = 14$

Decryption = $14^{27} \bmod 55$

c.) $p = 7,\ q = 11,\ e = 17,\ m = 18$

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1) \cdot (q-1) = 60$

$\gcd(60, 17) = 1$

$17d \bmod 60 = 1$

$d = 53$

public key = $\{17, 77\}$

private key = $\{53, 77\}$

encryption = $8^{17} \bmod 77$

$= 57$

Decryption = $57^{53} \bmod 77$

$= 8$

d. $p = 11,\ q = 13,\ e = 11,\ m = 7$

$n = 143$

$\phi(n) = 120$

$\gcd(143, 120) = 1$

$11 \bmod 120 = 1$

$d = 11$

public key $= \{11, 143\}$

private key $= \{11, 143\}$

encryption $= 7^{11} \bmod 143$

$= 106$

Decryption $= 106^{11} \bmod 143$

$= 7$

e). $p = 17,\ q = 3,\ e = 7,\ m = 2$

$n = 527$

$\phi(n) = 480$

$\gcd(527, 480) = 1$

$7d \bmod 480 = 1$

$d = 343$

public key $= \{7, 527\}$

private key $= \{343, 527\}$

encryption $= 2^7 \bmod 527$

$= 128$

Decryption $= 128^{343} \bmod 527$

$= 2$

43, 61

2623, 2111

2)

a) we need to figure out the private key to see the text.

b). Yes that formula will work. $d * e \bmod \phi(n) = 1$

C) $p = 43$, $q = 61$

$n = 2623$

$\phi(n) = \phi(p) * \phi(q)$

$\phi(n) = \phi(43) * \phi(61)$

$\phi(p) = p - 1$

$\phi(n) = 42 * 60$

$\phi(n) = 2520$

now, we calculate d.

$d \cdot 2111 \bmod 2520 = 1$

$d = 191$ to satisfy this equation

So,

$m = c^d \bmod n$

$m = 1141^{191} \bmod 2623$

$= 1088$. Yes it does!!

$\cdot 125 \% 1 \ 325$

1055
47 $\boxed{47^{-1} \bmod 1055}$

3). $A = 791291$, $B = 402$
$A^{-1} \bmod B$
$= 791291^{-1} \bmod 402$
$791291x = 1 \bmod 402$

$791291 = 1968 \times 402 + 155$
$402 = 2 \times 155 + 92$
$155 = 1 \times 92 + 63$
$92 = 1 \times 63 + 29$
$63 = 2 \times 29 + 5$
$29 = 5 \times 5 + 4$
$5 = 1 \times 4 + 1$
$4 = 1 \times 4 + 0.$
$\gcd(791291, 402) = 1$
Now euclidean algo
$1 = 5 - 1 \times 4 = 5 - 1(29 - 5 \times 5)$
$= 6 \times 5 - 29$
$= 6 \times [63 - 2 \times 29] - 29$
$= 6 \times 63 - 13 \times 29$
$= 6 \times 63 - 13[92 - 1 \times 63]$
$= 19 \times 63 - 13 \times 92$
$= 19[155 - 1 \times 921] - 13 \times 92$
$= 19 \times 155 - 32 \times 92$
$= 19 \times 155 - 32[402 - 2 \times 155]$
$= 83 \times 155 - 32 \times 402$
$= 83[791291 - 1968 \times 402] - 32 \times 402$
83 is the inverse.

b. $A = 65532$, $B = 10240$

$65532 = 6 \times 10240 + 4092$

$10240 = 2 \times 4092 + 2056$

$4092 = 1 \times 2056 + 2036$

$2056 = 1 \times 2036 + 20$

$2036 = 101 \times 20 + 16$

$20 = 1 \times 16 + 4$

$16 = 4 \times 4 + 0$

$gcd = 4$.