EE2302 Foundations of Information and Data Engineering

Assignment 6 (Solution)

1.

87	37		
1	0	87	a
0	1	37	b
1	-2	13	$c = a - 2b$
-2	5	11	$d = b - 2c = -2a + 5b$
3	-7	2	$e = c - d = 3a - 7b$
-17	40	1	$f = d - 5e = -17a + 40b$

$x = (3)(87)(-17) + (5)(37)(40) = 2963$.

2.

$M_1 = 12 \times 13 = 156,\ \ \alpha_1 \equiv 156^{-1}\ (\text{mod } 7) = 4$ (steps of finding inverses are omitted.)
$M_2 = 7 \times 13 = 91,\ \ \alpha_2 \equiv 91^{-1}\ (\text{mod } 12) = 7$
$M_3 = 7 \times 12 = 84,\ \ \alpha_3 \equiv 84^{-1}\ (\text{mod } 13) = 11$
$M = 7 \times 12 \times 13 = 1092$
$x = 5(156)(4) + 2(91)(7) + 8(84)(11)\ \ (\text{mod } 1092) = 866$

3.

a) HELLO = ”8 5 12 12 15”

b) $\mathrm{E}(H) = 8^3 \bmod 55 = 17$,
$\mathrm{E}(E) = 5^3 \bmod 55 = 15$,
$\mathrm{E}(L) = 12^3 \bmod 55 = 23$,
$\mathrm{E}(O) = 15^3 \bmod 55 = 20.$
The encrypted message is “QOWWT”.

c) N = 55. Factorize it, so p = 11 and q = 5.
$\phi(N) = (p-1)(q-1) = 40$
Since $3d \equiv 1 \bmod 40$, we can obtain $d = 27$. (steps omitted.)

Decrypt the ciphertext as follows:
$8^{27} \bmod 55 = 2,$
$5^{27} \bmod 55 = 25,$
$15^{27} \bmod 55 = 5.$
The message is “BYE”.