EE2302 Foundations of Information 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	$f = d - 5e = -17a + 40b$

$x = (3)(87)(-17) + (4)(37)(40) \ (\text{mod } 37 \times 87) = 1483.$

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) $c = m^e \text{mod } N = 16^3 \text{mod } 55$

$16^2 \equiv 36 \text{ mod } 55$

$16^2 \times 16 \ \text{ mod } 55 \ = 36 \ \times 16 \text{ mod } 55 = 26 \ mod \ 55.$

(b) $N = p \times q \qquad 55 = 5 \times 11.$

$\phi(N) = (p-1)(q-1) = 4 \times 10 = 40.$

$ed \equiv 1 \text{ mod } 40$

$3d \equiv 1 \text{ mod } 40 \ \ \Rightarrow \ d = -13 = 27.$

$m = c^d \text{ mod } n = 21^{27} \ mod \ 55 \ = \ 21^{16} \times 21^8 \times 21^2 \times 21 \ mod \ 55$

$= \ 1 \times 1 \times 1 \times 21 \ mod \ 55 \ = 21 \ mod \ 55$

$(\ 21^2 \equiv 1 \ mod \ 55\ , \ 21^4 \ \equiv 1 \ mod \ 55, 21^8 \equiv 1 \ mod \ 55\ , 21^{16} \equiv 1 \ mod \ 55\ )$

4.

a) a and m are co-primes, so that a^{-1} exists.

b) $\phi(26) = 12$

c) There are 12 possible values for a and 26 possible values for b. Therefore, the number of possible keys is $12 \times 26 = 312$.

d) For $a = 15$, it can be shown that $a^{-1} \equiv 7 \mod 26$.

$$15x + 6 = 21 \ (\text{mod } 26)$$

$$x = 7(21 - 6) \ \ (\text{mod } 26)$$

$$= 105 \text{ mod } 26$$

$$= 1$$